BITCOIN E ALTCOINS
FÁCIL, PRÁTICO E COMPLETO



- O que são?
- Para que servem?
- Quais são as vantagens?
- Quem pode participar?
- Como participar?
- Como investir ou aplicar?
- Como se ganha dinheiro com isso?
- Quais são os custos e os riscos?
- É legal ou ilícito?
- É seguro?
- Possui sigilo?
- Onde são aceitas?
- Como se usam?
- Como se conseguem ou se ganham?
- Onde se compram?
- Onde se vendem ou trocam?
- Quanto valem?
- Onde se guardam?
- Como se transportam?
- Como são feitas?
- Como posso fabricar também?
- Quais equipamentos são utilizados?
- Como adquirir os equipamentos?



Adriano Caravina

- Históricos e antecedentes;
- Explanações sociológicas e culturais;
- Terminologias e nomenclaturas;
- Conceitos e definições;
- Traduções e linguagem popular;
- Tutoriais passo a passo;
- Procedimentos diversos;
- Informática e tecnologia;
- Hardware e software;
- Noções de economia e investimentos;
- Investimentos por e no estrangeiro;
- Combinações e comparações;
- Dicas e sugestões;
- Faucets, pools e miners;
- Projeção do futuro;
- Natureza jurídica e questões legais;
- Despesas, taxas e tributos;
- Legislação nacional e estrangeira;
- Comentários jurídicos;
- Questões criminais e tributárias;
- Comentário público;
- Links e sites diversos;
- Glossário.

SUMÁRIO

1) PREFÁCIO
2) CONCEITO DE MOEDA
3) FUNÇÕES DA MOEDA
4) REQUISITOS DE VIABILIDADE DA MOEDA
5) HISTÓRIA E ORIGEM DA MOEDA
6) OSCILAÇÕES MOMENTÂNEAS DA MOEDA
7) HISTÓRIA E ORIGEM DOS BANCOS
8) CONTROLE ESTATAL DA MOEDA
9) SISTEMA FINANCEIRO
10) LASTRO EM OURO
11) DA MOEDA MUNDIAL CONTEMPORÂNEA
12) QUESTÃO MILITAR E GUERRA
13) VALOR DO OURO
14) INVESTIMENTOS EM OURO
15) INVESTIMENTOS NA BOLSA DE VALORES
16) TRIBUTAÇÃO SOBRE OURO, AÇÕES E RENDA VARIÁVEL
17) MEIOS E ENCARGOS DE ENVIAR OU CARREGAR DINHEIRO AO EXTERIOR
18) ABRIR UMA CONTA BANCÁRIA OU EMPRESA NO EXTERIOR (*OFFSHORE*)
19) MICRONAÇÕES E LOCAIS SEM JURISDIÇÃO
20) ESPÉCIES E TIPOS DE SOCIEDADES E DE ATIVIDADE EMPRESARIAL
21) INVESTIMENTOS ESTRANGEIROS NO BRASIL
22) OBTENÇÃO DE DOCUMENTOS PESSOAIS E ABERTURA DE EMPRESA NO BRASIL
23) FORMAS DE PAGAMENTOS ATUAIS
24) A FICÇÃO SE TORNOU REALIDADE
25) OUTROS MEIOS DE PAGAMENTO ELETRÔNICO OU DIGITAL
26) MOEDA DIGITAL OU ELETRÔNICA
27) SEGURANÇA DIGITAL
28) *HASH*
29) ALGORITMO DE *HASH*
30) CERTIFICADOS DIGITAIS

31) LADO NEGRO DAS MOEDAS VIRTUAIS
32) DOS RISCOS E PERIGOS DAS MOEDAS VIRTUAIS
33) CUIDADOS EM COMPRAS E PAGAMENTOS PELA INTERNET
34) ESPLANAÇÃO SOBRE PIRÂMIDES FINANCEIRAS
35) DAS MANIFESTAÇÕES ESTATAIS SOBRE AS CRIPTOMOEDAS
36) DA REGULAMENTAÇÃO DAS MOEDAS VIRTUAIS
37) POSIÇÃO DO BRASIL SOBRE AS MOEDAS VIRTUAIS
38) NATUREZA JURÍDICA DA BITCOIN NO BRASIL
39) POR QUE A BITCOIN SERIA UMA COMÓDITE?
40) POR QUE A BITCOIN É UMA MOEDA?
41) DO ASPECTO CRIMINAL NO BRASIL
42) GÊNESE E PRIMÓRDIO DO BITCOIN
43) QUEM CRIOU O BITCOIN?
44) SOFTWARES LIVRE E *OPEN SOURCE*
45) QUEM CONTROLA OU ESTÁ POR TRÁS DO BITCOIN?
46) BITCOIN
47) *PEER-TO-PEER* (P2P)
48) COMO A BITCOIN É FEITA?
49) MÉTODOS DE CONSENSO
50) *FORK*
51) INSUMOS NA GERAÇÃO DE BITCOINS
52) *BLOCKCHAIN*
53) VALOR DA BITCOIN E DAS ALTCOINS
54) *BITCOINERS* - LOCAIS ONDE ACEITAM BITCOINS
55) UNIDADES DA BITCOIN (SATOSHIS)
56) ONDE SE GUARDAM AS BITCOINS E ALTCOINS?
57) COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?
58) SIGILO DOS PAGAMENTOS ELETRÔNICOS
59) POSSIBILIDADE DE PENHORA E DE DEPÓSITO JUDICIAL DE BITCOINS
60) ONDE E COMO COMPRAR BITCOINS E ALTCOINS
61) COMO GANHAR BITCOINS E ALTCOINS?
62) LISTA DE FAUCETS
63) O QUE É MINERAÇÃO DE BITCOIN?
64) COMO MINERAR BITCOINS E ALTCOINS
65) LISTA DE ALTCOINS: CONSENSO E *HASH*
66) MINERAÇÃO NA NUVEM

67) MINERAÇÃO EM PISCINA (*POOL*)
68) EQUIPAMENTOS DE MINERAÇÃO
69) INTRODUÇÃO ÀS ALTCOINS
70) LISTA DE ALTCOINS: ANÚNCIOS
71) ESPLANAÇÕES SOBRE ALGUMAS ALTCOINS
72) QUAIS SÃO AS ALTCOINS PROMISSORAS?
73) CRIE SUA PRÓPRIA MOEDA VIRTUAL
74) CONSIDERAÇÕES SOBRE *START-UP* OU PROJETO DE *SOFTWARE*
75) DO ASPECTO RELIGIOSO
76) DÚVIDAS, INFORMAÇÕES E ATUALIZAÇÕES
77) GLOSSÁRIO

PREFÁCIO

A introdução de um livro, além de ser uma prévia sucinta da obra, tal como um *trailer* de um filme, ainda ajuda, em pouquíssimo tempo, saber os objetivos, ênfase, técnica, estilo e didática do autor.

A presente obra possui o objetivo principal de desvendar, elucidar, esclarecer e popularizar o enigmático Bitcoin, as demais moedas virtuais (altcoins - *alternate cryptocurrencies*) existentes e as novas moedas e formas de pagamentos que ainda estão por vir. Em suma, o livro objetiva atingir principalmente quem não sabe, não entende, está interessado ou tem curiosidade. Se quer saber, é porque está interessado ou, no mínimo, curioso. Se alguém está interessado é porque não sabe e quer saber. E, alguém que já sabe ou entende do tema abordado no livro, dificilmente irá adquiri-lo; muito menos lê-lo. Melhor ainda, quem já entende ou já sabe, não precisa de introduções ou preliminares.

O presente trabalho se desvencilha dos enfoques míopes, superficiais, isolados, restritivos, infantis, ingênuos, fantasiosos, delirantes, utópicos, surreais, mirabolantes... dos adolescentes e demais entusiastas das criptomoedas que aparenta viver dentro de uma bolha ou uma redoma de vidro isolados de tudo e de todos; enfim alheios de tudo o mais que existe e acontece no mundo. Desse modo, a análise, prisma, visão e apresentação das moedas digitais são feitas através de uma interpretação adulta, séria, lógica, racional, crível, realista, viável, possível, capitalista e interligada com as outras ciências. Por outras palavras, não cometemos, o erro de querer nerdenizar (tratar todos como se fossem geeks ou aficcionados em informática e tecnologia) os leitores ou de impor ao resto do mundo o linguajar, os dogmas, as filosofias e o estilo de vida de um pequeno grupo de pessoas que vive como que num mundo paralelo, numa realidade alternativa ou em outra dimensão, como, por exemplo, no filme “Tomorrowland - Um Lugar Onde Nada é Impossível”. Diante disso ao invés de utilizarmos alguma língua alienígena como Klingon ou Na'vi, optamos pela linguajem popular.

Exemplificando, os membros da comunidade Linux (um sistema operacional) cometem o erro, absurdo e suicida, de não compartilharem o

conhecimento, prática e expetiência que possuem. Ou seja, raramente um membro dá suporte, auxílio, ajuda, orientação ou explicação para os iniciantes e leigos. Muito mais difícil ainda é algum membro ensinar. Diante desse egoísmo e visão narcisista, as pessoas que estavam interessadas em se familiarizarem com o Linux, desanimam e desistem ante a oposição, resistência e até deboche daqueles que dominam o assunto. Como consequência disso, o Linux não se populariza e cada vez menos pessoas ingressam na comunidade. E quanto menos popular é e menos usuários possui, cada vez menos investimentos, aplicações e desenvolvimentos o Linux recebe. A mesma atitude infantil ocorre em relação às criptomoedas. Os que já fazem parte da comunidade ou já entendem, costumam dificultar, complicar ou até mesmo desanimar quem está querendo ingressar no meio. O jargão comum é alguma frase como: “Você está muito atrasado! Isso surgiu em 2009! Nem perca seu tempo com isso! Esquece!”.

Já, pelo contrário, quando se trata de algum jogo, os adeptos criam verdadeiras comunidades solidárias (inclusive sites para ensinar contendo manuais, tutoriais e dicas para os iniciantes e troca de experiência entre os mais experientes) para divulgação, promoção e captação de novos participantes para tornar o jogo cada vez mais popular e garantir que não seja descontinuado (encerrado). Por que não fazem o mesmo em relação às moedas criptográficas? Porque pensam que quanto menos pessoas participarem, mais ricos esse grupinho será. Ledo engano, pois se não tornar uma febre e viralizar estará sujeito ao fracasso, tal como muitas altcoins fracassaram.

Ainda mais. Não se consegue convencer as pessoas comuns aderirem às moedas digitais com os argumentos de que elas são legais, bacanas, novidade, bonitas, divertidas, coloridas, modernas, ecologicamente corretas, última moda, etc. É necessário demonstrar-lhes a utilidade prática, a importância, o valor, o ganho monetário, etc. Dessa forma, adentramos nas mentes das pessoas normais e através de seus próprios pensamentos, raciocínios, lógicas, convicções, valores, preceitos e princípios lhes demonstramos que os métodos convencionais, por mais antigos, tradicionais, sólidos, estáveis, eficientes que eram (não são mais), estão cada vez mais definhando, esfacelando e desintegrando-se. Já os meios virtuais, por outro lado, já são realidade e é apenas uma questão de tempo para que não existam

mais dinheiro físico, cheque, agências bancárias, caixas eletrônicos, sistemas de pagamentos tradicionais, etc.

Além de apresentarmos exemplos, fatos, antecedentes e históricos evolutivos, também demonstramos o que é iminente, o que está por vir e a projeção do que ainda se espera.

Tendo em vista esse objetivo, o texto foi elaborado da forma mais didática possível para democratizar e popularizar o entendimento e o acesso às moedas eletrônicas.

Exemplificando, aos verdadeiros entendidos da área, nem precisaríamos ensinar ou explicar absolutamente nada; vez que já sabem, ou deveriam saber, tudo ou praticamente tudo a respeito. Por isso que se diz "entendidos da área". Já aos que não são entendidos da área específica, mas possuem, ao menos, algum entendimento avançado de informática, bastaríamos dizer que o Bitcoin é um protocolo de rede P2P (*peer-to-peer*) para fins de emissão de moeda, realização de transações (pagamentos e recebimentos) e dos respectivos registros contábeis. Por sua vez, a respectiva moeda do protocolo Bitcoin é a bitcoin; que consiste numa moeda digital criptográfica que utiliza do algoritmo de *hash* SHA-256. Em relação às demais moedas digitais, bastaríamos dizer que são variações do protocolo Bitcoin com utilização de diferentes algoritmos de hashes, de métodos de criptografia e/ou de emissão das respectivas moedas.

A presente obra, portanto, não é dedicada especialmente às pessoas do meio Bitcoin e nem voltada exclusivamente a quem é da área de informática. Mas, pelo contrário, considera, dentro do possível, todos os graus de conhecimentos sobre os assuntos principal, base e correlacionados.

Pretendemos, desse modo, no critério faixa etária nos dirigirmos desde as crianças que tenham gosto, interesse, disciplina ou paciência para leitura até os outrora chamados de idosos (“melhor idade”). E, em todas as idades, reduzimos ao máximo possível o conhecimento básico inicial para facilitar e ampliar a assimilação do tema. Mas não nos restringimos a isso. Durante a elaboração da obra nos vislumbramos como dando uma palestra à uma plateia mista, eclética, ecumênica ou variada. Desse modo, a mesma

informação é repassada de diferentes formas para poder atingir e ser compreendida pelos mais diversos destinatários. Dentro desse contexto, também abordamos assuntos, temas e questões correlatas, relacionadas, inter-relacionadas, paralelas, reflexas e conexas.

Ressalta-se, assim, que o foco é o Bitcoin e, em segundo plano, as demais moedas virtuais. Mas há parênteses ou pequenas dispersões do foco para facilitar a compreensão (entendimentos necessários para poder compreender a exposição). Assim, as demais informações, por serem periféricas aos temas central e secundário, são abordadas sem muita profundidade, servindo apenas de introdução ou noção geral para melhor compreensão dos focos principais. Deste modo, há temas versando históricos, antecedentes e cronologia até chegar ao tópico central; inclusive comparativos históricos, passados e contemporâneos, com as questões relacionadas com os temas principais. Em reforço há pinceladas com o objetivo de fornecer verbetes e demais referências de como conseguir se aprofundar mais nos temas. Não tem como deixar de falar também sobre tecnologia, informática (*hardware* e *software*) e nem sobre investimentos, aplicações e rendimentos financeiros, nacionais e internacionais (afinal tem que demonstrar que as moedas virtuais são um bom negócio); bem como sobre a análise, mesmo que superficial, sobre abrir empresa (dentro e fora do país) e passar uma temporada ou, até mesmo, residir definitivamente no exterior.

Ilustrando melhor, não se trata de dispersão (perder o foco), não ter sequência cronológica de desenvolvimento ou faltar coerência lógica. O desenvolvimento do trabalho não é nada confuso. É semelhante a caminhar sem ficar somente olhando fixamente para frente, mas, também, dando olhadas rápidas para os lados. Também se assemelha ao invés de dirigir numa rodovia reta de forma estática, contínua, constante e ininterrupta, contemplar a paisagem paralela e fazer pequenos desvios e paradas para descansar a mente do estresse da visão da rodovia reta e descontrair com outras atividades rápidas. Por outras palavras, a mente humana é rebelde à repetição, mesmice, monotonia ou estímulo unilateral. É sabido que nossa mente se estressa fácil com a concentração ou a fixação em algo após certo tempo e, por causa disso, é recomendável periódicas interrupções com rápidas distrações para evitar o tédio ou a fadiga mental. Tal estratégia pedagógica é comum em aulas de cursos preparatórios para concursos

públicos e vestibulares, onde o professor constantemente faz rápidas interrupções para falar algo engraçado, fofocar, contar algo pessoal, dizer algo curioso ou interessante, dar uma dica fora do tema da aula, fazer um "gancho" com outro assunto ou matéria, etc.

Se fosse um diálogo, em tempo real, com uma ou poucas pessoas, seria possível facilmente constatar imediatamente a assimilação do(s) interlocutor(es) e prosseguir a explanação evitando-se repetições e divagações desnecessárias; bem como responder de plano às eventuais dúvidas, indagações, questionamentos, crítica e pedidos de esclarecimentos. Mas não é o caso.

Há de se ter em mente que cada pessoa tem sua forma e velocidade de raciocínio e de assimilação de informações; assim enquanto uns são mais rápidos na compreensão, outros exigem maiores e mais detalhadas explanações. Além do que nem todos possuem a base de conhecimento necessária para podermos partir de determinado ponto em comum.

Ainda mais, quando o tema é muito recente, ainda é controverso, envolve uma nova visão ou interpretação, existe certa rejeição sumária pré-concebida, envolve tabus, atrita com mitos, confronta com o "conhecimento popular" ou conflita com os costumes ou a tradição, necessário se faz uma exposição mais aprimorada e exaustiva da fundamentação (com argumentos extras aos convencionais); o que, em tese, não seria necessário se versasse questão consolidada ou pacífica. Por exemplo, até hoje existem pessoas que duvidam que o ser humano foi à Lua ou até mesmo ao espaço, que a Terra é redonda, que a Terra gira em torno do Sol, que houve o holocausto pelos nazistas, que existe inteligência artificial, que veículos inteligentes podem andar totalmente sozinhos, que praticamente ninguém tem privacidade, etc.

Outro detalhe é que nosso idioma (Português Brasileiro) ao mesmo tempo em que possui palavras para tudo, essas mesmas palavras possuem diferentes significados; com o que, algumas vezes se faz necessário repetir a mesma frase, duas ou três vezes, com outras palavras para ser mais claro e evitar interpretações equivocadas.

Ressalta-se, ainda, que a obra está dividida em tópicos, muito bem identificados e delineados, facilitando ao leitor “pular”, ou apenas “correr os olhos”, no que já sabe ou interprete como “perfumaria”; bem como possui grifos nas palavras chaves (verbetes) ou de maior importância (não só evidenciado temas; mas, inclusive, resumindo o texto) e os devidos destaques estéticos nas transcrições e citações para facilitar e agilizar a leitura dinâmica e, até mesmo, para “pular” ou localizar certos trechos, pontos ou temas. Além do que, por ser uma obra eletrônica, é possível ao leitor efetuar busca por palavras chaves.

Apesar de a Internet estar infestada de várias páginas e postagens sobre a questão, muitas pessoas sequer sabem pesquisar, não possuem uma boa conexão de Internet ou não possuem tempo para fazerem elas mesmas as pesquisas. Além disso, a enorme maioria dos textos (que em grande parte está em inglês) foram, e são, redigidos por pessoas que não sabem do que estão falando; e, das poucas que realmente sabem, na grande maioria das vezes quando não lhes falta didática (falam de modo que somente outro entendido ou do meio compreenda), pecam pela superficialidade (explanações sucintas que mais dúvidas despertam do que elucidam) e pelas informações retalhadas, esparsas, dispersas, confusas, contraditórias e, até mesmo, desatualizadas.

Assim é somente uma minoria que possui compreensão considerável sobre o assunto; sendo que esse grupo é composto, em sua maioria, basicamente de profissionais avançados de Informática e, claro, de adolescentes e jovens que cresceram “brincando” por anos com computadores.

Ressalta-se que, conforme veremos, o assunto não é nenhuma novidade (vez que existe há vários anos), mas, apesar disso, várias pessoas sequer ouviram falar disso.

Um dos maiores problemas recorrentes que a indústria tecnológica possui, é constantemente ser incompreendida, dando margem à suposições, mitos, equívocos e confusões baseadas em uma falta geral de conhecimento, com o que, além de perpetuar a relutância, resistência e ignorância a seu respeito, seus benefícios e usos, também dificulta o esclarecimento e põe em

risco à própria sobrevivência da mesma. Não é a melhor tecnologia ou o melhor produto que sempre prevalece, mas, muitas vezes, é simplesmente a mais popular que vence; e, para agradar à multidão, precisa antes ser conhecida, compreendida, acessível, proveitosa e prazerosa. Portanto, a própria indústria tecnológica é a principal culpada pela ignorância das pessoas a respeito de seus produtos e serviços por não se empenhar em esclarecer os pretensos clientes ou consumidores. Suspeita-se que além da impaciência para ensinarem aos leigos, os gênios tecnológicos devem presumir que todos devem ter a mesma facilidade do que eles para entenderem a tecnologia. Ledo engano!

As tentativas de divulgar o Bitcoin foram frustradas em razão de terem, na grande maioria, se restringido a divulgarem dentro do grupo de pessoas que entendem e, quando divulgado fora deste meio, foram por pessoas totalmente desqualificadas. Pior ainda, muitas pessoas que entendem não quiseram propagar o conhecimento para não atrapalharem seus investimentos (cartel de mineração) e para poderem continuar comprando moedas virtuais a preços baixos. Explica-se. Tal como um pequeno grupo de pessoas que sabe da existência de uma mina de ouro num local público, eles tornam isso um segredo e prosseguem as extrações de ouro até quanto puderem. Mas, por serem leigos em economia e sociologia, ignoraram que é justamente a adesão em massa (multidão ou popularidade) que dá vida, valor, vigor e prosperidade para as moedas e as comódites que não possuam valor intrínseco (em si mesmas ou por si mesmas). Isso mesmo, os “sabidões” não sabem de tudo e, assim, os “espertalhões” “cavam a própria cova” ao laborarem na estratégia de formarem uma “panelinha” (grupo seleto, fechado e secreto) em volta das criptomoedas.

Qualquer pessoa que possui algum entendimento sobre o tema, que tenha procurado aprender sozinho sobre o assunto ou que já tentou explicar isso para alguém, sabe muito bem a enorme quantidade de pessoas que não sabem absolutamente nada disso e como é demasiadamente difícil fazê-las entender.

Diante disso, pede-se desculpas, compreensão e paciência antecipadas às pessoas com algum conhecimento em informática e sobre o assunto aqui tratado. Para esses o presente trabalho vai, ao menos em alguns momentos, vai dar a impressão de repetitivo, de lento como um veículo atolado que não

sai do lugar e de, até mesmo, infantil por explicar o que é simples e óbvio para uns, mas não é para muitos. Como “termômetro” (para ter uma noção melhor do nível de entendimento das pessoas) fiz a experiência de tentar explicar de forma oral (pessoal e presencialmente) este assunto com pessoas dos mais diversos níveis de classe social, estudo, cultura, conhecimento e inteligência e, até mesmo, pessoas de formação universitária (saúde, exatas, humanas, etc.) demonstraram desconhecimento e muita dificuldade de compreender sem a explicação de conceitos prévios, básicos e essenciais.

Realmente, enquanto que não é nada fácil ensinar algo que se tem como simples para alguém que sequer entende os preceitos e premissas necessárias, em contraposição, quem tem algum conhecimento sobre a questão fica entediado, impaciente e irritado com a “lenga lenga”, “enrolação” ou demora para chegar ao que lhe interessa.

Sim, colocamos nomenclaturas, terminologias, conceitos, definições e explicações dos termos mais comumente utilizados na área ou na questão.

Sem prejuízo disso, o presente livro também possui muitas informações preciosas para aqueles que possuem entendimento inicial, intermediário e, até mesmo, avançado sobre a questão. O glossário possui informações complementares, de reforço e de revisão, que não podem ser dispensadas nem por quem conseguir assimilar ou ter uma boa noção lendo o restante da obra.

Recomenda-se não pular capítulos ou escolher somente alguns para ler. Primeiro, porque os assuntos estão interligados, interconectados ou entrelaçados, de modo que não é possível compreender um sem entender o outro. Desse modo, por exemplo, fazendo uma analogia com a Bíblia, se uma pessoa só ler os evangelhos (Novo Testamento), não irá compreender o que significa cordeiro, expiação, lei e determinados rituais; vez que tais conceitos estão no Antigo Testamento. Em segundo, porque o desenvolvimento das explicações seguiu esse roteiro e, assim, nos primeiros capítulos estão as premissas, pressupostos e bases para compreender o que consta dos capítulos seguintes.

O presente trabalho, tendo em vista o manuseio da presente obra em monitores e telas, para ser tornar mais fácil e prática a leitura, não seguiu os padrões da ABNT (Associação Brasileira de Normas Técnicas) e nem o formato convencional herdado dos livros impressos.

Ante o fato da obra ser destinada a qualquer pessoa (e não apenas às pessoas do meio ou entendidas da questão), não foi redigida no padrão estético ou conforme a formatação de trabalho científico ou acadêmico.

Pelo fato do tema envolver colaboradores anônimos ou com pseudônimos, bem como trabalho coletivo democrático na Internet, não há muitas citações, referências ou atribuições de créditos e, inclusive, constam muitas expressões, jargões, clichês e até mesmo frases similares, semelhantes e, até mesmo, idênticas em todos os trabalhos que abordam a questão. Para sermos mais claros, seria semelhante se estivéssemos pregando sobre a doutrina (cartilha) de uma religião ou igreja ou se estivéssemos vendendo os produtos de uma franquia. Desse modo, não se limite ao que é semelhante aos demais, mas se apegue nos diferenciais.

Os padrões sugeridos pela ABNT não são nada didáticos, práticos, ágeis ou eficazes; mas, pelo contrário, dificultam e cansam a leitura e, até mesmo, confundem o leitor.

Dispensamos as páginas e partes em branco para agilizar a leitura, bem como para economizar papel em eventual impressão.

Poupei o leitor de ter que ficar indo e voltando, com a interrupção da leitura para conferir citações, transcrições, referências, fontes, notas de rodapés, apêndices e anexos; o que é demasiadamente difícil de fazer num livro digital, fora que é bem irritante.

Foram citados vários links da Internet como forma de material de apoio ou informação complementar.

No mundo contemporâneo a velocidade das informações, dos acontecimentos e das mudanças é muito rápida, com o que as coisas mudam não só constantemente, mas de forma muito dinâmica. Pior ainda quando se

trata de questões de informática (que mudam com muita frequência), de sites da Internet (que somem do dia para a noite) e de legislação (que possui prazo de validade semelhante ao leite de saquinho). E, em razão disso, o que ouvimos, vemos, lemos, aprendemos, falamos, escrevemos ou ensinamos hoje, por mais atualizados que esteja, irá com o passar do tempo, constantemente, sendo desatualizado e/ou mudado. Além disso, pelo fato das coisas atualmente mudarem muito rápido, é difícil para um livro permanecer totalmente atualizado por muito tempo.

Diante disso, os endereços dos links ficaram expostos (visíveis) de propósito para agilizar o conhecimento dos destinos dos mesmos, tornando desnecessário colocar o cursor em cima para saber o endereço e, principalmente, levando em consideração que os links podem se "quebrarem" (ficarem desatualizados), com o que a visualização completa do link possibilita poder localizar manualmente o que se quer no site linkado ao seguir a sequência de cliques ou pastas constantes na sequência do link quebrado ou mediante a opção de pesquisa no próprio site e, até mesmo, no Google (ou outro site de buscas/pesquisas) se o próprio site linkado mudou de endereço ou de nome.

Também ensinamos os canais de atualização para poder se manter atualizado com as novidades sobre as moedas virtuais.

De igual forma, através dos conceitos, nomenclaturas, terminologias e nomes é possível a realização de pesquisas rápidas na Internet para conferir se há novidades ou se houveram mudanças; bem como para se aprofundar melhor no tema.

Da mesma forma, foram indicados os verbetes, números, nomes, institutos e fontes das informações jurídicas para a conferência de eventuais alterações.

Apesar da obra procurar ser a mais completa possível, infelizmente isso é, humana e fisicamente, impossível. Explica-se. Ao terminar de escrever o livro, novos temas, questões, fatos, novidades e alterações surgem e, em razão disso, o trabalho pronto é revisto para alcançar tais pontos. Depois é realizada nova revisão para conferir as informações, links, programas e

legislações para verificar se não houve mudanças. Segue-se nova pesquisa para ver se há alguma novidade a ser acrescida. Entretanto, todo esse zelo, diligência e precaução não conseguem impedir a possibilidade de assim que der a obra por concluída, revisada, atualizada e pronta para disponibilização, surgir um novo site, uma nova empresa, um novo programa, uma nova alteração, etc.

Detalhe, se nunca pararmos de ficar revisando e procurando eventuais atualizações de um manuscrito, nunca iremos publicá-lo. Desse modo, dentre as opções de disponibilizar uma obra com probabilidade, remota e eventual, de algum item faltante ou desatualizado e de nunca conseguir concluir e disponibilizar a obra pelo fanatismo, psicose e zelo extremista de perfeição, o melhor para todos é impor um limite de revisões e atualizações para poder conseguir disponibilizar o livro. Depois de disponibilizado, após um merecido descanso, com a ajuda dos comentários (*feedback*) dos leitores e com o estímulo da aceitação do mesmo, procede-se à uma eventual revisão, atualização e até ampliação, se assim for necessário.

Desse modo, contamos com os *feedbacks* (retornos), avaliações, comentários, solidariedade, informes de erros ou de imprecisões, críticas, sugestões, ideias, auxílios, atualizações e demais colaborações dos leitores e entusiastas das criptomoedas através do e-mail (bitcoinealtcoins@gmail.com), do grupo (https://www.facebook.com/groups/1311019482290913/) e da página institucional (https://www.facebook.com/Bitcoin-e-altcoins-972584846175010/) no Facebook.

Nesse tipo de tema não é possível como no Direito poder dizer que a obra está atualizada até a data “x”, vez que envolve acontecimentos no mundo inteiro (e não só no próprio país quando se trata de Direito) e a velocidade com que estas informações chegam até ao Brasil variam muito dependendo da fonte (localidade) e do grau de sigilo da mesma. Presuma ou tenha como referência a data da publicação.

Em suma, a presente obra constituiu uma tarefa herculana de transferir conhecimento, amplo, completo e atualizado e, ainda, de tornar este atualizado pelo maior tempo possível.

Dentro dessas premissas procuramos sermos o mais breve possível para evitar de ser enfadonho, entediante, prolixo, cansativo e irritante.

Boa leitura, bom aprendizado e bons investimentos.

CONCEITO DE MOEDA

O senso comum descreve aquilo que as pessoas percebem no seu dia-a-dia, com interpretação muitas vezes individualista, tendenciosa, sem técnica, sem base científica, com visão míope, desprovida de informações corretas e totalmente distorcida da realidade. Desse modo, o pensamento popular (e equivocado) é de que moedas são as peças metálicas, geralmente redondas, de valor igual ou inferior à unidade monetária e que são fundamentais para realização de operações de baixo valor ou de valores não inteiros; ou seja, para troco.

A palavra dinheiro vem do latim "denarius", nome dado a uma antiga moeda romana. Essa palavra foi usada para denominar uma moeda de prata e cobre que circulava em Castilha, na Espanha. Depois foi utilizada para todas as moedas e todo o tipo de dinheiro.

A palavra moeda deriva do latim (língua oficial do Império Romano) *moneta*. Na Roma (Itália) antiga, contudo, o termo “monetor” ou “moneta” significava conselheiro, no sentido de uma pessoa que aconselha e previne. De acordo com alguns historiadores, o significado dessa palavra remonta a um acontecimento chave da história romana. Em 390 a.C., durante uma invasão gaulesa, os grasnos de um bando de gansos residentes num templo da deusa Juno, no Monte Capitólio, alertaram os Romanos para um ataque eminente, salvando-os da derrota. Em agradecimento, os Romanos construíram um novo templo dedicado a Juno Moneta, a deusa que previne e aconselha. A primeira casa da moeda romana foi construída em 289 a.C., nesse templo ou muito perto dele, tendo começado por aí a se produzir moedas (*denarius*) em bronze e, mais tarde, em prata. Na face de muitas dessas moedas era cunhada a efígie de Juno Moneta. Daí terem surgido termos como “moeda” e “casa da moeda”.

Todo dinheiro é moeda, mas nem toda moeda é dinheiro. Logo, dinheiro é um tipo de moeda.

Enquanto o dinheiro é constituído pelas notas (geralmente em papel) e moedas metálicas, a definição de moeda é mais abrangente; já que engloba não só o dinheiro, mas todos os meios através dos quais são efetuadas as

transações monetárias e comerciais. Assim, **dinheiro** é qualquer objeto ou registro verificável que seja geralmente aceito em troca de bens e serviços em um país ou contexto socioeconômico. Dinheiro é qualquer coisa, fato ou circunstância que faz alguém trabalhar para outra pessoa. O dinheiro, portanto, nada mais é que um meio de pagamento inventado para facilitar a obtenção de bens e serviços; bem como o seu acúmulo, pois é muito mais fácil guardar dinheiro do que animais, objetos, temperos, metais, etc.

- https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html;
- https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.pt.html.

O conceito de **moeda**, entretanto, é econômico, descrevendo um bem qualquer que serve para intermediar trocas, tem aceitação geral, permite avaliar outros produtos e possui certos atributos físicos específicos. Note-se, portanto, que moeda é um bem qualquer, tanto que as primeiras moedas foram mercadorias (gado, sal, fumo, escravos, conchas, mel, peixes secos, arroz, rum, peles de animais, etc.).

Desse modo, a moeda é o dinheiro sob qualquer forma quando usado ou em circulação (passa adiante de mão em mão) como meio de troca. É todo o ativo que constitua forma imediata de solver (quitar, extinguir ou pagar) débitos, com aceitabilidade geral e disponibilidade imediata, e que confere ao seu titular um direito de saque sobre o produto social. São os papéis-moedas (cédulas ou notas) e as moedas metálicas admitidas em circulação. Em geral, a moeda é emitida e controlada pelo governo de um país, que é o único que pode fixar e controlar o seu valor dentro do respectivo território.

Em síntese, o **conceito abstrato de moeda** é aquilo que é aceito em troca de bens e serviços. Porém não é aceito como um objeto a ser consumido, mas como uma valorização e representação de poder aquisitivo a ser usado, constante, periódica e continuamente, em novos e sucessivos processos de compra de bens ou pagamento de serviços; ou seja, para circular representando crédito em si e com poder de solver débitos.

> "No mundo moderno, a moeda de um país, no seu sentido mais amplo, tem três atributos básicos: é unidade de conta ou padrão de valor, ao qual são referenciados os preços de todos os bens e serviços; é também meio de troca, servindo para a aquisição de bens e serviços e pagamentos de salários ou de dívidas, preenchendo a função de meio de pagamento; e, finalmente, constitui-se também em reserva de valor, podendo ser guardada como parte da riqueza ou poupança das pessoas." (Luiz Aranha Corrêa do Lago, A moeda metálica em perspectiva histórica, 1ª parte, PUC - Rio, p. 8/9; *in* http://www.econ.puc-rio.br/pdf/td481.pdf).

Assim, o dinheiro é mundialmente conhecido como meio de pagamento de bens, serviços e dívidas. Além disso, serve para mensurar o valor de bens, serviços e de riqueza. Entretanto, nem sempre uma única moeda serve de referência para uma mesma localidade; ou seja, no mesmo local podem coexistir mais de uma moeda em vigência. Por exemplo, no Paraguai apesar de a moeda oficial ser o Guarani (₲), concomitantemente, o dólar norteamericano (US$), o euro (€) e o real (R$) são moedas rotineiramente utilizadas no dia a dia do comércio local.

O dinheiro sempre foi criado pela sociedade (agrupamento, comunidade ou coletividade de pessoas num determinado território) como um sistema democrático de valorização do trabalho e dos bens até que o governo resolveu assumir essa função e passar a regulamentar. Assim, a moeda nacional ou oficial é criação do Estado (definição institucional), mas necessita da aceitação da comunidade (em especial do comércio) para tornar-se dinheiro (aceitação mercantil). Portanto existe confronto e consenso entre o Estado e o mercado a respeito do que vai constituir o dinheiro. Consenso em tempos de calmaria e confronto em circunstâncias de caos, calamidades, hiperinflação, guerra, etc. quando há migração massiva para moedas estrangeiras (por exemplo, dólar ou euro) ou outra coisa (ouro, por exemplo) que seja eleita pela sociedade para essa função.

Em conclusão, o dinheiro não consiste em moedas e notas de banco. O dinheiro é alguma coisa que as pessoas estiverem dispostas a usar para representar de forma sistemática o valor de outras coisas, com o objetivo de trocar bens e serviços. O dinheiro permite às pessoas compararem rápida e

facilmente o valor de diferentes bens para trocarem, facilmente, uma coisa por outra e para armazenarem riqueza de forma conveniente. Assim, em resumo, o dinheiro é um meio de troca universal que permite que as pessoas convertam quase tudo em quase qualquer outra coisa.

> "Uma moeda (qualquer moeda, digital ou de latão) só tem valor se as pessoas confiarem nela. Se todo mundo acredita que um pedaço de papel azul estampado com um peixe da família dos serranídeos vale R$ 100, então vale." (Revista Super Interessante, Edição 297, novembro de 2011: http://super.abril.com.br/tecnologia/o-dinheiro-do-futuro).

Por outras palavras, o dinheiro apesar de ser um meio de troca, não existe por assim dizer; o que existe é valor associado ao mesmo. O dinheiro é essencialmente um símbolo; uma abstração. No dinheiro físico cada unidade (moeda ou cédula) representa um valor, que pode ser utilizado em troca de um bem ou serviço. Se antigamente cada papel-moeda representava a porção do seu valor em ouro (lastro em ouro ou sistema de Bretton Woods), hoje apenas existe confiança que será aceite universalmente e que pode trocá-lo em qualquer lugar. É a confiança no valor da moeda que possibilita a sua circulação. Esse valor é que o dinheiro é e o que possibilita sua utilização como intermediário de trocas. O valor facial, impresso ou nominal não se altera apesar de o dinheiro poder perder valor pela inflação.

Desse modo, a moeda é um instrumento que facilita as trocas e a reserva de valores e, como tal, triunfou plenamente no domínio das relações mercantis (comerciais). Era usada não apenas no comércio, mas também na coleta de impostos (tributos), no pagamento total ou parcial de rendas e naturalmente para amealhar (economizar). A moeda, portanto, é a expressão concreta do dinheiro. Dispõe de uma representação material, com valor econômico, que é utilizada como instrumento de troca, possuindo como tal um poder aquisitivo (poder de compra) servindo para determinar, de uma forma prática, o preço das coisas. A moeda presta, assim, um importante serviço como unidade de medida comum em que se expressam todos os valores. Sem ela, para fixar o preço de uma mercadoria seria necessário comparar o seu valor com todas as restantes.

Em apertada síntese, segundo a teoria econômica, que foi construída com base em duas hipóteses, vindas desde Adam Smith:

1) O dinheiro é um valor neutro; ou seja, apenas um meio de facilitar trocas e sua origem ou propósito não afeta os investimentos, as transações em si nem as relações entre as pessoas que o utilizam.

2) O dinheiro pode até ter nomes diferentes, mas foi criado em vários lugares sempre para atender os mesmos objetivos.

Em arremate, segundo o economista belga Bernard Lietaer (ex-diretor do Banco Central da Bélgica e um dos arquitetos do regime que criou o Euro): "o dinheiro é um acordo, geralmente inconsciente, feito por uma comunidade, para ser usado como meio de troca. O dólar como moeda global foi um acerto que se deu no final de 1945, depois da Segunda Guerra Mundial. Porém, quando um contrato não funciona é preciso fazer o distrato. Se a sociedade começa a questionar a eficiência do atual modelo financeiro, temos de pensar em criar outros meios de troca entre a comunidade que evitem colapsos. As moedas complementares são possibilidades, funcionando paralelamente às já em circulação, como o dólar, que jamais poderiam ser eliminadas totalmente" (trecho da palestra "O futuro do dinheiro", em 06/11/2007 no Banco Real, no evento "Encontros de Sustentabilidade").

FUNÇÕES DA MOEDA

As principais **funções da moeda são:**

I) **Intermediária de trocas.** É a evolução do escambo (troca direta de um bem por outro), consistente numa operação de economia monetária, com melhor especialização e divisão social do trabalho, transações realizadas com menores tempo e esforço e melhor planejamento de bens e serviços. Enfim, é um instrumento intermediário de aceitação geral, que permite ao seu detentor a possibilidade de solver débitos, de efetuar pagamentos e o direito de exigir da sociedade quaisquer bens correspondentes ao valor facial indicado. A introdução do dinheiro permitiu desdobrar a troca direta em duas fases distintas: 1) Troca de bens ou serviços produzidos por um indivíduo, por dinheiro (operação de venda); e, 2) Troca de dinheiro por bens ou serviços produzidos por um indivíduo, (operação de compra). Assim, troca-se um bem por uma determinada quantidade de dinheiro (venda) e troca-se uma determinada quantidade de dinheiro por um bem (compra).

II) **Poder ou função liberatória.** Mediante a garantida concedida pelo Estado à moeda, ela possui a condição e o poder de liquidar débitos e saldar dívidas (inclusive para com o próprio Estado).

III) **Medida de valor.** Como unidade padronizada de medida de valor ou conta, constitui um denominador comum de valores, racionaliza informações econômicas e configura um sistema agregado de contabilidade social, produção, investimento, consumo e poupança. Quando o valor de um bem é frequentemente usado para comparar ou medir o valor de outros bens, ou quando o valor é utilizado para especificar débitos, então esse bem funciona como unidade de conta. Como denominador comum de valores, permite contabilizar ou exprimir numericamente os ativos e os passivos (os haveres e as dívidas). É o padrão de avaliação de todos os bens e serviços colocados no mercado. Em resumo, faz o papel de um denominador comum, ao qual todos os valores da economia estão vinculados, indexados e atrelados. Esta função do dinheiro suscita a distinção entre preço absoluto e preço relativo. O preço absoluto é a quantidade de moeda necessária para se obter uma unidade de um bem; ou seja, é o valor expresso em moeda. Já o

preço relativo exige que se considerem dois preços, na medida em que é a comparação de preços; ou seja, é a quantidade de unidades do bem 2 a pagar por cada unidade do bem 1.

IV) **Padrão de pagamentos.** Possibilita realizar pagamentos ao longo do tempo, permite crédito e adiantamento e viabiliza fluxos de produção e de renda.

V) **Reserva de valor.** A moeda possui a capacidade de reter em si um valor patrimonial, sendo considerada um ativo monetário de liquidez por excelência e de aceitação consensual praticamente unânime. É essa função que dá ao dinheiro a característica de ser poupado, guardado ou recuperado e ser preferencialmente usado como meio de troca; vez que, permite que sejam feitas comparações entre o mesmo bem não só em diferentes lugares, mas também em diferentes momentos no tempo; ou seja, o dinheiro dá a quem o possui a alternativa de consumir determinado bem no presente ou no futuro, a oportunidade de poupar (acumular riqueza para ser usada no futuro), como também a possibilidade de distribuir os pagamentos ao longo do tempo. Os indivíduos, seja por motivo de transação, segurança ou especulação, preferem acumular dinheiro, à semelhança dos que o guardavam num cofre ou numa botija, para exercer, no futuro, os direitos que a sua posse permita. A maioria dos bens não perecíveis tem essa característica. Assim, esta função é compartilhada com outros ativos como o ouro, as ações, as obras de arte, imóveis, etc. A grande diferença entre o dinheiro e as restantes reservas de valor reside no elevado grau de liquidez do dinheiro, enquanto que os outros ativos têm de ser transformados em moeda antes de serem trocados por outro bem.

VI) **Instrumento de poder.** Como instrumento de poder econômico, conduz ao poder político, permitindo a manipulação na relação Estado-Sociedade.

REQUISITOS DE VIABILIDADE DA MOEDA

Confiram-se, ainda, os principais **requisitos essenciais de viabilidade da moeda:**

- **Indestrutibilidade** – a moeda deve ser suficientemente durável, no sentido de que não se destrua ou se deteriore, à medida em que é manuseada na intermediação de trocas, pois caso contrário ela perderia o seu valor. Além do que inviabilizaria o acúmulo de riqueza (poupança), vez que ao tentar guardar para o futuro, elas se deteriorariam (estragariam).

- **Inalterabilidade** – ser impossível ou extremamente difícil de sofrer alterações, adulterações ou manipulações para evitar deterioração e fraudes.

- **Homogeneidade** – duas unidades monetárias distintas, mas de igual valor devem ser rigorosamente iguais; ou seja, medida (peso, pureza, valor, etc.) padronizada e reprodutível. Como consequência direta disso, a moeda é fungível; ou seja, permite a reposição (ressarcimento) do mesmo valor através de outras unidades, como, por exemplo, num empréstimo (não são as mesmas unidades que são devolvidas ou utilizadas no pagamento).

- **Divisibilidade** – a moeda deve possuir múltiplos e submúltiplos em quantidade tal que as transações de grande e pequeno porte possam realizar-se sem dificuldades. Por outras palavras, deve-se permitir o fracionamento do valor para pagamentos pequenos e para fins de troco. Essa característica qualquer pessoa percebe com o fato de existirem cédulas e moedas metálicas de diversos valores para facilitar os pagamentos e respectivos trocos. Se a moeda de determinado páis tivesse uma única cédula e nenhuma moeda, como se faria para dar troco? Se cortassem a cédula, ela perderia o valor. A única solução popular ou do comércio seria a criação de títulos de créditos para fins de troco.

- **Transferibilidade** – a moeda deve ser de fácil transferência entre seus possuidores.

- **Portabilidade** – deve possuir facilidade de manuseio e transporte.

- **Segurança -** dificuldade de ser duplicada e proteção contra fraudes e falsidades.

- **Aceitabilidade** – é a probabilidade de algo ser aceito por outros indivíduos em troca de um determinado preço. Quando um objeto é mais prontamente aceito por outras pessoas na economia, é mais provável que cada indivíduo irá deseja-lo aceitá-lo como sendo um meio de troca. A implicação disto é que a aceitabilidade pode ter uma natureza auto-reforçante.

- **Estabilidade** – a moeda não pode ter muitas ou altas oscilações de preço.

Em resumo, a moeda deve ser fácil de carregar, transportar e transferir para facilitar as trocas entre diferentes pessoas e locais.

HISTÓRIA E ORIGEM DA MOEDA

Primeiramente é necessário antes saber e entender o passado para compreender o presente e poder antever o futuro. Desse modo conhecer a história e o porquê de as coisas serem atualmente assim, nos possibilita antever, vislumbrar, presumir e prever o que está por vir; vez que conhecendo padrões, tendências, históricos de comportamentos e de reações e demais informações relacionadas ao objeto de estudo (perfil, personalidade, habilidades, recursos, potenciais, limites, fraquezas, vícios, qualidades, méritos, vitórias, conquistas, falhas, fracassos, erros e o aprendizado com eles, experiências de sucesso, práticas, modo de pensar, modo de agir, instintos, reações mecânicas ou subconscientes, ideais, espiritualidade, crenças, mitos, tradições, costumes, desejos, aspirações, objetivos, necessidades, motivações, preferências, etc.), podemos apurar os possíveis eventos futuros e suas respectivas probabilidades de ocorrer.

A **numismática** é a ciência que estuda, identifica e analisa cronologicamente e geograficamente a história da moeda e o seu contesto histórico.

Economia é a ciência que estuda as formas de comportamento humano resultantes da relação existente entre as ilimitadas necessidades a satisfazer e os recursos que, embora escassos, se prestam a usos alternativos.

A moeda ou o dinheiro como conhecemos atualmente, é o resultado de uma longa evolução. Desse modo, em resumo, **a moeda apareceu sob diferentes formas ao longo da história**:

- **Escambo** – Trocas diretas e simples de bens;
- **Moeda-Mercadoria** – Uma mercadoria é escolhida por se adaptar as necessidades gerais;
- **Moeda metálica** – Inicialmente produzida por algum material de valor intrínseco e, depois, com metais simples com valores nominais;
- **Papel-moeda conversível** – Moeda feita em papel, mas com a possibilidade de seu valor poder ser conversível em metais (exemplo, lastro em ouro);

- **Moeda fiduciária** – De curso forçado e poder liberatório garantido pela estrutura jurídica, sem lastro e dependente da confiança pública;

- **Moeda bancária ou escritural** – Sem existência física real correspondendo a lançamentos contábeis de débitos e créditos;

- **E-cash ou moeda eletrônica** – Movimentação de recursos fora da rede de compensação estabelecida pelos bancos.

A história da moeda está intimamente ligada às trocas comerciais, especialmente na passagem de uma economia baseada na troca direta para a troca indireta ou monetária (utilização de um bem intermediário).

Em apertada síntese, a moeda surgiu através de convenção social em diversas civilizações e com vários formatos (conchas, gado, sal, cobre, prata, ouro, etc.); tendo sido depois inicialmente padronizada mundialmente (em razão dos intercâmbios dos comerciantes) em pequenos pedaços (para facilitar o transporte e manuseio) de metal (com materiais, formatos, tamanhos e pesos variados), estilizadas (inseridos inscrições, gravuras, desenhos, figuras, símbolos ou brasões) e cunhadas (fabricadas ou moldadas) pelo governo (que passou a controlar e manipular). Posteriormente foram inventados o cheque e a cédula (moeda de papel), em substituição às tradicionais moedas metálicas, para tornar mais fácil ainda o manuseio, transporte, guarda e, até mesmo, a fabricação. Continuando o desenvolvimento, a evolução, a eficiência e a praticidade dos negócios, surgiram os cartões de crédito e de débito e, depois, as transferências eletrônicas de créditos, que continuam a ser aperfeiçoadas cada vez mais.

> **Convenção social** é o padrão de comportamento, embora não escrito, criado e aceito pela sociedade em geral para a conveniência. São regras de condutas oriundas dos costumes de uma determinada sociedade. É um hábito arraigado (enraizado) que leva até mesmo a desaprovação de quem não o pratica.

Na sua origem, a moeda não é senão uma mercadoria reconhecida como equivalente geral e, ao mesmo tempo, utilizada como intermediária nas trocas. E, por também ser uma mercadoria, é exposta a oscilações; podendo o seu valor subir ou baixar segundo a sua situação no mercado.

Nos primórdios da civilização não havia moeda e, assim, praticava-se o **escambo**; ou seja, simples troca direta de mercadoria por mercadoria, de mercadoria por serviço e/ou de serviço por mercadoria, sem qualquer equivalência de valor e, muito menos, troco ante a indivisibilidade dos objetos nas trocas diretas.

Assim, quem pescasse mais peixe do que o necessário para si e seu grupo trocava este excesso com o de outra pessoa que, por exemplo, tivesse plantado e colhido mais milho do que fosse precisar. Esta elementar forma de comércio foi dominante no início da civilização, podendo ser encontrada, ainda hoje, entre povos de economia primitiva, em regiões onde, pelo difícil acesso, há escassez de meio circulante, e até em situações especiais, em que as pessoas envolvidas permutam objetos sem a preocupação de sua equivalência de valor. Este é o caso, por exemplo, da criança que troca com o colega um brinquedo caro por outro de menor valor, que deseja muito.

De modo similar, o "**Timedollar**" é uma iniciativa de intercâmbio comunitário, em que o tempo é o meio de troca. Quando alguém ajuda o outro, recebe um crédito de uma hora e o beneficiário passa a ter um débito, que pode desaparecer se também fizer algo para os demais. Esse mecanismo cria uma moeda baseada em um acordo e, por isso, não surge inflação nem juros, já que uma hora sempre representa 60 minutos. Mas, e quanto às velocidade e qualidade do trabalho? Primeiramente, nenhum trabalho é idêntico ao de outro; e, em segundo, se a pessoa vai ganhar por hora, não importando a quantidade e nem a qualidade, fatalmente irá "enrolar" para poder gastar mais tempo.

As mercadorias utilizadas para escambo geralmente se apresentam em estado natural, variando conforme as condições de meio ambiente e as atividades desenvolvidas pelo grupo, correspondendo a necessidades fundamentais de seus membros.

Nesta forma de troca, no entanto, ocorrem dificuldades, por não haver uma medida comum de valor entre os elementos a serem permutados.

Pelo fato de o escambo não considerar o tempo, o trabalho, a dificuldade e o custo despendidos (gastos) na obtenção, produção ou criação da coisa

negociada (mercadoria, objeto, animal, alimento, etc.), não levar em conta a escassez ou abundância do bem e, ainda, dificultar o manuseio, transporte e, principalmente, o acúmulo de moeda (por envolver produtos perecíveis ou deterioráveis), as pessoas passaram a buscar e testar outras formas de valorizar e pagar pelas coisas e pelo trabalho. Assim, primeiramente, começaram a estipular graduações de valores para os bens, mas isso só funcionava dentro da mesma comunidade ou localidade, vez que algo escasso ou de difícil obtenção ou produção num local pode ser abundante e de fácil obtenção ou produção em outra localidade. Ainda mais, surgiu outro problema, como mensurar (avaliar ou quantificar) devidamente a correlação de troca entre os bens?

Outra falha intrínseca do escambo era a necessidade e pressa de encontrar algum interessado no bem (exemplo, banana) que queria usar como moeda (pagamento) e que, ainda, tivesse sobrando exatamente o bem (exemplo, leite) que queria adquirir; ou seja, o escambo exige a correlação recíproca inversa de necessidade x disponibilidade.

Por outras palavras, o escambo exige uma dupla coincidência de desejos ou necessidades coincidentes inversas; vez que, por exemplo, quem pescasse demais e quisesse adquirir trigo, teria que encontrar alguém que tivesse trigo em excesso e quisesse, justamente, adquirir peixes.

Muitas comunidades (famílias, aldeias, povoados, tribos, vilas, cidades, etc.) ante seus recursos naturais, condições climáticas e geológicas, habilidades e dons dos seus cidadãos e outros motivos diversos, acabam produzindo em abundancia determinados bens em detrimento da escassez e, até mesmo, da inexistência de outros; em contrapartida, povos próximos e, principalmente, distantes, por circunstâncias, condições e fatores diferentes podiam ter em abundância/excesso justamente o que eles precisavam e, ainda, coincidentemente podiam necessitar daquilo que eles tinham de sobra. Entretanto, na maioria das vezes, podia ocorrer desses outros povos também terem em excesso as mesmas coisas ou terem escassez de bens diferentes dos que os primeiros tinham em excesso; numa dessas situações a negociação não se concretizava e a moeda acaba se deteriorando (estragando e sendo perdida) se fosse perecível.

Em razão da falta de repasse dos excedentes passaram a investir na produção de outros bens que eram escassos naquele momento (mudança do tipo de cultivo na lavoura e dos animais na criação) e a procurarem formas de conservar por mais tempo os alimentos e os estocavam (para consumo próprio ou oportunidade futura de negociação); mas isso não resolvia satisfatoriamente o problema de falta de interessados no que tinham em excesso; salvo em casos de secas, incêndios, pragas, infestações, geadas, enchentes e outras calamidades que destruíam os alimentos e/ou as criações de outra(s) comunidade(s) e, assim, provocava a demanda (necessidade, procura, interesse, etc.). Ainda tinha a despesa, tempo e trabalho dispendido com o método e local de armazenamento; bem como a proteção do mesmo contra ladrões, pragas e efeitos da natureza.

Um problema na mudança do plantio e/ou da criação era saber se iria dar resultados e quanto conseguiriam produzir, se é que conseguiriam. Se acabassem produzindo demais gerariam outros bens em excesso. E se os outros povos ou até mesmo os vizinhos também resolvessem produzir na mesma época esses produtos? Em ambos os casos o comércio enfraqueceria e aumentaria o problema. Como conseguir prever o que se terá grande escassez ou procura no futuro para poder começar agora a plantar, criar ou extrair?

Exemplificando, se um produtor tivesse vários porcos, poderia trocar, um ou alguns, por sacos de cereais. Mas, e quando quem queria ou necessitasse de suínos, não tinham grãos, mas apenas vinho para efetivar a troca? A solução inicial foi encontrar uma terceira pessoa para fazer uma ponte de ligação. Assim, continuando o exemplo, quem tivesse cereais e quisesse vinho conseguia integrar e concretizar os interesses das três pessoas. Portanto o terceiro trocava seu cereal pelo porco do primeiro e, depois, trocava esse porco pelo vinho do segundo.

Após constatarem a necessidade costumeira dessa terceira pessoa nos negócios, alguns comerciantes se especializaram nesse tipo de serviço de intermediação.

Surgiu, assim, o **câmbio** (troca de bens diferentes compensando a diferença de valores), a *exchange* (intermediário ou facilitador nas

negociações) e, como aperfeiçoamento contínuo do processo negocial, a moeda; ou seja, um objeto que serve de elemento intermediário e compensador na efetivação do processo de troca.

O ***exchanger*** **(cambista)** é a pessoa ou empresa que, em troca de uma taxa (*fee*), faz intercâmbios de dinheiro, cartões de crédito e uma variedade de outros bens e valores para o tipo de moeda solicitada por um indivíduo ou empresa. Cada casa de câmbio é uma propriedade de negócios independente e possui suas próprias políticas, regimento interno, regras, procedimentos, taxas, métodos e sistemas de financiamento, para atender à procura do mercado.

Além disso, no escambo a simples troca de um bem por outro provocava constante sentimento de injustiça e, longas e acaloradas, discussões; vez que começaram a perceber, considerar e comparar o trabalho, o tempo, a dificuldade, o perigo e o custo/investimento envolvidos na obtenção dos bens e, assim, cada um ao seu modo começou a criar, de forma subjetiva ou em conformidade com sua região, uma escala hierárquica valorativa de bens. Mas como em cada localidade tais circunstâncias envolvidas na valoração do bem são diferentes (por exemplo, o que é difícil de obter num lugar é extremamente fácil em outro), surgiam as discussões durante as negociações, pois cada parte insistia que seu bem (mercadoria ou serviço) valia mais que o da outra parte.

Exemplificando, já que tudo valia a mesma coisa, por que alguém se daria ao trabalho de transformar o milho ou o trigo em farinha ou a cevada em cerveja se não iria ganhar nada a mais por isso? Ou, então, numa negociação de gado não importar se o animal era novo, velho, gordo, magro, doente, macho, fêmea ou prenha.

Valor econômico adicionado, valor adicionado ou valor agregado é, assim, o valor adicional que adquirem os bens e serviços ao serem transformados durante o processo produtivo.

Portanto, ante os inconvenientes acima, as comunidades passaram a escolher um único bem como referencial de troca, que tivesse valor e fosse aceito por todos como tal. Foi a substituição do escambo (troca direta de um

bem [produto ou serviço] por outro) pela moeda mercadoria (troca indireta através de algo com valor intrínseco).

A partir desse instante, o procedimento rudimentar e primitivo da troca que tinha como base o câmbio direto de bens, passa a ter mais um componente, agora em duas fases. Primeiro, faz-se um serviço ou vende-se algo para obter um bem intermediário (moeda) e, depois, usa-se esta moeda-objeto para adquirir um objeto ou serviço específico desejado.

Entretanto, mesmo trazendo maior mobilidade para o empreendimento de transações comerciais, a moeda não é usada em todas as economias do mundo. Diversas sociedades e regiões preservam o uso da troca em sua economia. De forma geral, os produtores inseridos neste tipo de economia utilizam dos excedentes de sua produção para estabelecerem alguma forma de escambo. Ao longo do tempo, a diversificação dos produtos dificultou a realização desse tipo de troca natural. A prática do escambo existe até hoje no Zimbábue e entre ribeirinhos da Amazônia.

Em tese (na teoria), para que uma mercadoria possa ser utilizada como moeda, ela deve ter durabilidade (não ser perecível), ter divisibilidade (comportar divisão), ter homogeneidade (ser igual às outras unidades) e ter facilidade de manejo e transporte. Mas, na prática, muitos bens foram usados como moeda apesar de serem indivisíveis, de difícil manejo ou transporte, perecíveis, deterioráveis e terem risco de pragas, doenças e de morte.

Algumas mercadorias pela extrema utilidade passaram a ser mais procuradas do que outras; e, sendo aceitas por um grande número de pessoas, assumiram a função de moeda, circulando como elemento trocado por outros produtos e servindo para avaliar-lhes o valor. Eram as moedas–mercadorias.

Várias coisas serviram de moeda durante a história. Numa tentativa de estabelecer um certo padrão monetário, os comerciantes costumavam utilizar algum tipo de mercadoria de grande procura ou valorização pela maioria das pessoas. Basicamente foram alimentos (grãos, sementes, mudas, etc.), bebidas alcóolicas (vinho, rum, cerveja, aguardente, etc.), animais, temperos (sal, condimentos em pó e, inclusive, ervas, chás e raízes), tecidos

(peles/couro, lã, seda, algodão, linho, etc.), vestimentas (casacos, sandálias, botas, chapéus, luvas, etc.), armas (funda, estilingue, facas, lanças, espadas, arco e flecha, escudo, etc.), utensílios (anzóis, cordas, cestos, etc.), ferramentas (martelos, arados, pás, facões, serras, etc.), metais e, inclusive, escravos; ou seja, na enorme maioria dos casos foram bens tidos não só como úteis ou necessários, mas valiosos ante sua essencialidade (necessidade fundamental ou preeminente). Confiram-se alguns exemplos: açúcar (Barbados), algodão (Barbados), amendoim (Nigéria), amêndoa (Sudão), animais (em todo o mundo antigo), arroz (Índia, China e Japão), bacalhau (Islândia), botas (China), búzios (Europa, África, Ásia, China e na península Arábica), cacau (México e índios centro-americanos), cruz de Katanga (regiões da África), dentes de animais (Oceania), espetos (Grécia Antiga), esteiras (Ilhas Carolinas), fitas de aro amarradas umas às outras formando uma lâmina (oeste da África), mogno (Honduras), pedras rai de yap (ilhas da Micronésia), peixes (Alasca), peles (Sibéria e América), pérolas (África), sal (Roma e Etiópia), seda (China), tartarugas (Marianas), telas e tecidos (Europa, África e China), etc.

Na antiga Babilônia, era usada a cevada e, ainda hoje, entre tribos de índios centro-americanos são usados os grãos de cacau, em contrapartida de primitivas tribos africanas que continuam usando as conchas. Na Grécia Antiga foi utilizado o boi (que era chamado pekus); já entre os romanos e os etíopes foi o sal (usado como pagamento e na conservação de alimentos). Na Rússia medieval, peles de esquilo eram trocadas por bens. Ainda são usadas em partes da Finlândia.

Da antiguidade até o ano 410, no Egito a moeda era o cobre; na Índia eram os animais domésticos, o arroz e metais, e, na China eram, conchas, seda, sal e cereais.

Na Idade Média (de 410 a 1453), na Alemanha a moeda era o gado, cereais e mel; na Rússia era o gado e a prata; e, no Japão era cobre, perola e arroz.

Na Idade Moderna (1453 a 1789), nos Estados Unidos a moeda era o fumo (tabaco), cereais, madeira e gado; na França eram metais preciosos e cereais; e, no Japão era o arroz.

No Brasil, entre outras, circularam o cauri (trazido pelos escravos africanos), o pau-brasil, o açúcar, o cacau, o tabaco e o pano, trocado no Maranhão, no século XVII, devido à quase inexistência de numerário, sendo comercializado sob a forma de novelos, meadas e tecidos. Em 1874, foi proibida no Brasil, a circulação dos gêneros alimentícios utilizados como moeda.

Os búzios foram usados como dinheiro durante cerca de 4.000 anos por toda a África, Ásia Meridional, Ásia Oriental e Oceania. Até o início do século XX ainda era possível pagar impostos em búzios, no Uganda britânico.

As **mercadorias mais cotadas no câmbio** foram o sal (em razão de ter sido adotado pelos romanos que possuíram vasto território), pedaços de metal (pela durabilidade, resistência e conversão em utensílios, ferramentas e armas), as conchas (normalmente em países com grande extensão marítima) e o gado (por sua alta versatilidade: locomoção própria, reprodução, meio de transporte, força bruta para trabalhos, carne, leite, queijo, manteiga, couro, esterco, ossos e chifres para fabricar instrumentos e armas, etc.).

Até hoje empregamos palavras como pecúnia (dinheiro) e pecúlio (dinheiro acumulado) derivadas da palavra latina *pecus* (gado). A palavra capital (patrimônio) vem do latim *capita* (cabeça). Da mesma forma, a palavra salário (remuneração, normalmente em dinheiro, devida como contraprestação pelo empregador em face do serviço do empregado) tem como origem a utilização do sal, em Roma, para o pagamento de serviços prestados. Desse modo, a palavra salário deriva do latim *salarium*, que provém de sal (*salis* em latim e, *hals* em grego).

A atual moeda indiana "rúpia" vem do termo em sânscrito (a linguagem da antiga Índia) "rupa", que significa "gado". Já "libra" vem da medida de peso usada para medir a quantidade de metal utilizada nos pagamentos.

Resumindo, as moedas-mercadorias variaram enormemente de região para região e, de época para época, mas sempre possuíram os requisitos de raridade ou escassez (o que lhes dava valor) e de desejo ou necessidade

comum das pessoas em geral (implicando em ampla aceitabilidade como meio de troca ou pagamento e, com isso, podia ser facilmente convertida em qualquer outro bem ou serviço).

Em razão da falta de homogeneidade; dos resultados da ação do tempo (depreciação, deterioração, perecimento, envelhecimento, apodrecimento, doença e até a morte); da impossibilidade de divisão; da dificuldade de manuseio, transporte e estocagem (não permitindo o acúmulo de riquezas ou reserva de valores); dos constantes e repentinos períodos de escassez e de excesso, que provocavam frequentes e bruscas oscilações de seu valor ante a lei da procura e da oferta (ausência de estabilidade ou valor constante); da justaposição do valor de uso (como bem de consumo) e de troca (estabelecido no mercado); dos valores de uso e de troca torná-la muito semelhante ao escambo e suas limitações intrínsecas; de não cumprir satisfatoriamente o requisito da aceitação geral exigida nos instrumentos monetários, as moedas-mercadorias (alimentos, animais, temperos, condimentos, etc.) eram prejudicadas na sua função como instrumento de troca ou meio de pagamento e, assim, com o passar do tempo, elas foram se tornando cada vez mais inconvenientes, ineficientes, inviáveis, insatisfatórias, incômodas, inadequadas, inconfiáveis e imprestáveis às transações comerciais; com isso, gradualmente foram sendo substituídas e descartadas (abandonado o uso).

Tal processo evolutivo se deve à necessidade constante de se aperfeiçoar as trocas de mercadorias ou os meios de pagamentos, visando a rapidez, a praticidade, a agilidade, a eficiência, a segurança, etc.

Por motivos semelhantes, logo quando se descobriu o metal, passou-se a utilizá-lo na fabricação de utensílios, ferramentas e armas que, anteriormente, eram feitos de pedra, osso, chifre, madeira ou barro, que não possuíam a mesma rigidez, resistência, durabilidade e eficiência. Ainda mais, os metais possuem o grande trunfo de poderem ser reciclados (reaproveitados, refeitos, convertidos, remodelados ou reconstruídos) infinitamente em qualquer outro objeto. Em consequência disso tais objetos metálicos foram muito desejados e supervalorizados e, em pouco tempo, o próprio metal foi valorizado e, com isso, acabou substituindo rapidamente as moedas mercadorias.

Numa etapa transitória entre a apreciação cada vez maior dos utensílios de metal e a valorização do próprio metal, houve a fabricação e o uso (como moeda) de réplicas em miniaturas dos objetos metálicos mais visados. Exemplos, miniaturas de facas e chaves no Oriente e do talento, miniatura de pele de animal feita de cobre ou bronze, que circulou na Grécia e em Chipre.

Portanto, por apresentar vantagens como a possibilidade de entesouramento, divisibilidade, raridade, facilidade de transporte e beleza, o metal foi eleito como principal padrão de valor e, assim, passou a ser trocado, no início, no estado natural e, depois, em vários formatos: objetos, utensílios, adornos (anéis, colares, braceletes, pulseiras...), moedas, barras, pepitas, grãos, pó, etc.

As primeiras formas de dinheiro conhecidas são os lingotes (ou barras de metal), que eram usados na Babilônia há uns 5.000 anos.

Como a produção de metais exigia, o conhecimento dos raros locais onde podia ser encontrado e o domínio das técnicas de extração e de fundição, o que não estava ao alcance de todos, os metais foram, fácil e rapidamente, mais valorizados do que qualquer outro bem ou serviço.

Os metais (cobre, ferro, bronze, prata e ouro), com o passar do tempo, foram as mercadorias intermediárias que se ajustaram mais às necessidades de meio de troca, principalmente devido as características essenciais que se exigem dos instrumentos monetários (indestrutibilidade, homogeneidade, divisibilidade, transferibilidade, facilidade de manuseio, transporte e acúmulo) e ao fato de que o seu valor de uso não compete com o seu valor de troca.

Esparta recorreu inicialmente ao ferro. Egito, Roma, Europa Central e China usaram o cobre, bronze e, depois, principalmente a prata e o ouro. Enfim, por causa das possíveis aplicações industriais e comerciais, pela raridade, pela durabilidade, pela beleza, pela homogeneidade, pela divisibilidade, pelos valores místicos, pela ostentação envolvida e pela ampla e universal aceitabilidade, a prata e o ouro se destacaram e consolidaram como metais preferidos e de notório valor monetário. Portanto,

com o passar do tempo, gradativamente, os metais preciosos (ouro e prata) foram sendo os preferidos ante o brilho e a beleza; sendo que o ouro tem a grande vantagem de ser o único metal que naturalmente não enferruja e, a prata, apesar de oxidar, basta polir que o brilho volta.

Em resumo, os primeiros metais utilizados como moeda foram o cobre, o bronze e, notadamente, o ferro. Por serem, ainda, muito abundantes, não conseguiam cumprir uma função essencial da moeda que é servir como reserva de valor. Dessa maneira, os metais não nobres foram sendo substituídos pelo ouro e pela prata, metais raros e de aceitação histórica e mundial.

A prata era geralmente empregada na cunhagem de moedas de valor mais baixo do que as de ouro; apesar de que houve um processo evolutivo para chegar nessa conclusão óbvia para os dias de hoje. Explica-se. Como não havia no início um padrão estabelecido ou relação fixa de valor entre os dois metais, houve muita oscilação desde a tentativa frustrada de igualá-los até inúmeras interpretações de quanto um vale do outro. A questão foi resolvida através de imposição legal (depois harmonizada por tratados internacionais) estabelecendo uma artificial ou arbitrária correspondência ou equivalência de tanto de um vale do outro (em média de 15 para 1).

O alumínio, apesar de ser o elemento metálico em maior quantidade na Terra; ou seja, é encontrado em abundância na crosta terrestre (8,1%), em razão de não ser encontrado livre ou puro, mas deve ser separado de outros minérios, como a bauxita. A bauxita contém de 35% a 55% de óxido de alumínio, este mineral é extraído da natureza e através dele se obtém a alumina (produto intermediário que leva à produção de alumínio). Quando o alumínio foi descoberto, a sua separação das rochas era extremamente difícil e cara, com o que, durante algum tempo, foi considerado um metal precioso; inclusive mais valioso do que o ouro. Com o avanço (simplificação, rapidez e barateamento) dos processos de obtenção, o preço do alumínio baixou continuamente até colapsar em 1889, devido à descoberta anterior de um método simples de extração do metal.

Alexandre, o Grande, da Macedônia, foi a primeira personalidade a ter a face registrada no denário, pequena moeda de prata usada no Império

Romano. A expressão originou a palavra “dinheiro” em português e, “dinero”, em espanhol.

Após isso, vários outros governantes passaram a inserir suas imagens nas moedas e, com o passar do tempo, graças à vaidade pessoal dos governantes e o fascínio (admiração, medo ou veneração) do povo, os governantes passaram a acreditar que era sua imagem (rosto, busto, nome, emblema, símbolo, brasão, etc.) que dava valor à moeda; quando não isso, as pessoas acreditavam que eram os símbolos, ícones ou referências religiosas ou místicas que davam o valor e poder à moeda. Crenças estas que muitos ainda têm atualmente ao criarem moedas virtuais em homenagem a celebridades e ídolos.

“Quase todas as moedas tinham como tipo no anverso o busto do imperador ou de membros de sua família. No reverso predominavam representações de divindades ou personificações de atributos ou ações dos imperadores, mas também inscrições, monumentos (templos, pontes, anfiteatros etc.), animais, corpos celestes, instrumentos de culto, além de cenas de atividades militares e civis.” (Luiz Aranha Corrêa do Lago, A moeda metálica em perspectiva histórica, 1ª parte, PUC - Rio, p. 41; *in* http://www.econ.puc-rio.br/pdf/td481.pdf).

- http://www.bbc.com/portuguese/noticias/2011/11/111121_euro_mitos_historia_mv.shtml.

Uma das explicações da origem do cifrão (confira outras infra no item thaler ou táler) é a de que surgiu no ano 711, da era cristã, quando o general Táriq-ibn-Ziyád comandou a conquista da Península Ibérica, ocupada até então pelos visigodos. A montanha rachada ao meio chamada “Colunas de Hércules” (apelido do Estreito de Gibraltar, que separa a África da Europa, em razão da mitologia grega rezar que o semideus Hércules, num de seus 12 trabalhos, rachou ao meio a montanha com apenas um golpe de maça) foi conquistada pelo general árabe Djebel-el-Táriq que, para comemorar, gravou em moedas uma linha em “S”, simbolizando o caminho sinuoso. Dois traços no meio da linha mostravam o poder e a força. O símbolo, assim gravado nas moedas, se difundiu e passou a ser reconhecido mundialmente como cifrão, representação gráfica do dinheiro.

- http://www.moedasdobrasil.com.br/cifrao.asp.

O padrão monetário bimetálico findou-se em torno de 1873, ante o desmoronamento do valor da prata, dando, assim, origem ao monometalismo ou monarquia absoluta do ouro.

As **pedras preciosas** (berilo vermelho, jeremejevite, musgravite, diamantes [em ordem crescente de raridade pela tonalidade: amarelo, marrom, incolor, azul, verde, preto, rosa, laranja, roxo e vermelho], grandidierite, poudreteita, benitoíte, tanzanita, alexandrita, painita, turmalina, aquamarine, água-marinha, esmeralda, rubi, safira, jade, etc.) e as pérolas também foram (e como os metais preciosos ainda são) utilizadas como moedas ante sua raridade, beleza, brilho, resistência e durabilidade; mas ante o inconveniente de dificultar a divisibilidade e de não poderem ser recompostas, reversíveis ou restauradas depois de fracionadas (partidas, divididas, quebradas...) ou moldadas, os metais preciosos acabaram tendo a grande preferência ante sua maleabilidade e conversibilidade.

Assim, os **metais preciosos** passaram a sobressair por terem uma aceitação mais geral e uma oferta mais limitada, o que lhes garantia um preço estável e alto. Além disso, não se desgastavam e eram facilmente reconhecidos, divisíveis e leves.

Entretanto, havia o problema da pesagem; ou seja, o metal comercializado exigia aferição de peso e avaliação de seu grau de pureza em cada troca ou negociação. Assim, em cada transação os metais deveriam ser pesados para se determinar seu valor. Em razão disso, os primeiros comerciantes viajavam carregando seus sacos de ouro e prata e algumas balanças, com as quais pesavam a quantidade necessária de metal para comprar ou vender mercadorias. Em suma, o metal era dividido e pesado quando se celebrava algum negócio.

Assim, o problema foi resolvido través da cunhagem; ou seja, era impresso na moeda o seu valor. Muitas vezes, entretanto, um soberano recontava as moedas para financiar o tesouro real. Ele recolhia as moedas em circulação e as redividia em um número maior, apoderando-se do

excedente. Esse processo gerava o que conhecemos como inflação; vez que existia um maior número de moedas para uma mesma quantidade de bens existentes.

A passagem da moeda na sua forma física original à moeda cunhada constituiu uma mudança exterior de forma, mantendo-se, porém, um comportamento idêntico na circulação.

A princípio, as peças eram fabricadas por processos manuais muito rudimentares e tinham seus bordos irregulares, não sendo, como hoje, peças absolutamente iguais umas às outras.

A primeira **moeda cunhada** foi na região da Lydia (onde atualmente fica a Turquia), no século 7 a.C., por volta de 610-560 a.C. Era feita de Electrum (liga de ouro e prata que ocorre naturalmente), do tamanho da digital de um polegar, no formato oval, com o desenho, em relevo, de uma cabeça de leão e com o emblema real garantindo a pureza e o peso do metal. Assim, os lídios inventaram a moeda moderna, com pesos, tamanhos e valores diferentes. Cada pedaço de metal tinha um valor que correspondia a um determinado produto. Entretanto, a Electrum tinha um grande problema de confiança, pois não dava para saber ou confirmar se as moedas tinham realmente a quantidade de ouro que se afirmava. Em razão disso, o rei Creso adotou a padronização do peso e determinou a fabricação das moedas apenas de prata e ouro puros, com desenhos de partes do corpo de um leão indicando seu peso e valor.

Os judeus, antes do exílio na Babilônia, usavam moedas da Pérsia e, depois, a dracma, que era uma moeda grega. As primeiras dracmas dos judeus, cunhadas por volta de 400 anos antes de Cristo, traziam a escrita “Judéia”.

Mais tarde, a moeda metálica ganhou forma definida e peso determinado, recebendo marca indicativa de valor, que também apontava o responsável por sua emissão. Essa medida agilizou as transações, dispensando a pesagem e permitindo a imediata identificação da quantidade de metal oferecida para troca.

Surgem, então, no século VII a.C., as primeiras moedas com características das atuais: são pequenas peças de metal com peso e valor definidos e com a impressão do cunho oficial; isto é, a marca de quem as emitiu e garante o seu valor.

Embora principalmente o ouro e a prata tenham sido usados para cunhar moedas, outros metais também foram utilizados. Por exemplo, a antiga Esparta cunhava moedas de ferro para desencorajar os cidadãos de se envolver no comércio exterior.

Roma teve a sua primeira moeda oficial por volta de 335 a.C. o (*aes grave* ou *aes librale*), de forma redonda com indicação de valor e cunhagem oficial. Em 268 a.C., Roma passa a emitir moedas em prata denominada denário, termo do qual se origina a palavra dinheiro. O denário serviu como base do sistema de moedas (sistema monetário) de Roma. Os primeiros *denarii*, tinham no anverso a efígie da deusa Roma (*dea roma*), símbolo do estado romano, e no reverso a efígie dos gêmeos Castor e Pólux, heróis da mitologia grega, com uma estrela sobre suas cabeças.

> A contagem dos anos antes do nascimento de Cristo, contam-se retroativamente; ou seja, vão diminuindo até o ano zero.

As moedas romanas em circulação, durante a maior parte da República e do Império Romano do Ocidente, incluíam: o áureo (*aureus*, em latim) de ouro; o denário (*denarius*) de prata; o sestércio (*sestertius*) de bronze; o dupôndio (*dupondius*) de bronze; e, o asse (as) de cobre. Durante o século III d.C., o denário foi substituído pelo denário duplo, também conhecido como antoniniano (*antoninianus*); o qual, por sua vez, foi extinto pela reforma monetária de Diocleciano, que criou denominações tais como o argento (*argenteus*, "de prata") e o *follis* (bronze prateado). Após as reformas, as moedas em circulação passaram a ser, basicamente, o soldo (*solidus*) de ouro e algumas denominações menores de bronze, até o fim do Império Romano do Ocidente. A única moeda de prata cunhada foi a Miliarense. A moeda era indexada no valor da prata em todo o período histórico romano, chegando a influenciar a moeda do Império Bizantino. O denário transparece no termo espanhol "dinero" e na unidade monetária atual dos países árabes, o "dinar". Da lira de prata deu origem ao nome da moeda

inglesa do latim libra. Até mesmo os termos "moeda" e “monetário” se referem ao Templo de Juno Moneta, perto do qual era cunhado o dinheiro da Roma antiga.

No fim do século VII uma nova moeda de prata começou a ser cunhada na Inglaterra e na França. Na Inglaterra era chamada Penny e, na França Denier, do latim *denarius*.

O primeiro **padrão monetário** a se difundir na Europa Ocidental após a queda do Império Romano do Ocidente foi estabelecido pelo Imperador Carlos Magno por volta de 800 d.C. Era baseado no *denarius*. Nem a libra, nem o soldo foram originalmente verdadeiras moedas: no Ocidente tanto o *solidus* como o *librum* eram moedas de conta, meros coletivos de *denarius*.

A moeda de meio *denarius* era chamada *obolus* (símbolo ob~) e um quarto de *denarius*, *quadrans* (símbolo q/r). Moedas baseadas no *denarius* de Carlos Magno também circulavam em Portugal com o nome de dinheiro, na França como *denier*, na Espanha como *dinero* e na Itália como *denaro*, na Alemanha como *pfennig* e na Inglaterra como *penny* (plural *pence*) ou *sterling*. Também os nomes dos seus múltiplos foram usados em outros países da Europa Ocidental: em Portugal, soldo e libra; na França, *sou* (que se escrevia *sol* até o século 18) e livre; na Itália, soldo e lira; na Espanha, *sueldo* e libra.

Apesar de o **dinheiro** ter surgido pela primeira vez no reino da Lídia, há milhares de anos, ele desapareceu com o fim do Império Romano. E quando a Idade Média chegou, com servos que cultivavam os alimentos em imensas propriedades de senhores feudais, a terra passou a ser a coisa mais valiosa. As pessoas só produziam o que precisavam e o escambo (a troca) tomou o lugar do dinheiro.

Na alta idade média, só o império bizantino cunhava moedas de ouro desde 717, o *solidus* ou *nomisma*; que era conhecida no Ocidente como *besante*. Nos países árabes, incluindo o califado de Córdoba que dominava os atuais Portugal e Espanha, o besante foi reproduzido com o nome de dinar (também do latim *denarius*), ao lado do qual circulava o dirham (do grego *drachma*) de prata e o *fuls* (de *follis*, singular de *follera*) de cobre.

Os **principais metais utilizados na cunhagem de moedas** foram o ouro e a prata. O emprego desses metais se impôs, não só pela sua raridade, beleza, imunidade à corrosão e valor econômico; mas, também, por antigos costumes religiosos. Nos primórdios da civilização, os sacerdotes da Babilônia, estudiosos de astronomia, ensinavam ao povo a existência de estreita ligação entre o ouro e o Sol, a prata e a Lua. Isso levou à crença no poder mágico desses metais e no dos objetos com eles confeccionados.

A produção de moeda com metais preciosos como matéria-prima testemunhou o rápido desenvolvimento de uma economia monetária. A organização do sistema monetário em torno de ouro, prata ou *electrum* (liga de ouro e prata), consolidou-se em duas frentes: a do ouro e prata e a da acumulação de capital, em parte concentradas nas mesmas mãos. A moeda substitui gradualmente a lógica da acumulação de riqueza em bens materiais por uma lógica baseada na obtenção do máximo lucro e de acumulação de capital.

No momento em que se converte em moeda, o ouro estabelece uma relação mais ou menos estável com a prata e mesmo com outros metais, como o cobre e o bronze. Além do ouro e da prata também circulavam moedas de cobre e de latão, destinadas a transações de baixo valor. Estabeleceram-se sistemas monometálicos puros ou sistemas bimetálicos, em que as moedas cunhadas em ambos os metais tinham valores independentes. Para que este último sistema seja eficaz é necessário que a relação entre as duas quantidades de metais disponíveis se mantenha estável. A adoção de sistemas bimetalistas exige uma equivalência entre o valor dos dois metais contidos nas diversas peças metálicas. Quando isso não acontece surgem desequilíbrios que podem dar origem a um entesouramento das melhores, só se utilizando nas transações as mais desvalorizadas. Este fenômeno está expresso na “lei” de Gresham, segundo a qual, a má moeda expulsa a boa.

No início do século 13, muitas pessoas não usavam dinheiro na Inglaterra. A grande maioria vivia no campo e trocava coisas que eles não podiam fazer eles mesmos. As únicas pessoas que regularmente manipulavam moedas de prata eram os habitantes de cidades de mercado (e havia apenas 300 delas e

algumas destas tinham menos de 500 habitantes). No entanto, ao longo do século 13, outros 1.400 mercados foram fundados na Inglaterra. Por volta de 1300, vários países começaram a cunhar moedas de grande valor de ouro, e o crédito estava disponível a partir de empresas de serviços bancários italianas, que tinham filiais em todo o continente.

As pessoas raspavam a volta das moedas para desgastar e juntar o pó do metal e fazer mais moedas com o que tiravam de outras; por causa disso foi inventada as “ranhuras” na volta das moedas para ficar evidente se houve algum tipo de fraude. Já os governantes adulteravam tanto o peso, o tamanho, a composição e a pureza do ouro das moedas. Era a desonestidade ajudando a melhorar o sistema de segurança.

A cunhagem de moedas em ouro e prata se manteve durante muitos séculos, sendo as peças garantidas por seu valor intrínseco; isto é, pelo valor comercial do metal utilizado na sua confecção. Assim, uma moeda na qual haviam sido utilizados vinte gramas de ouro, era trocada por mercadorias deste mesmo valor.

O **thaler ou táler** foi uma moeda de prata usada na Europa por quase quatrocentos anos. Tudo começou em 1518, em uma mina de prata da Boêmia que realizava cunhagem da moeda de prata. Referida mina de prata foi nomeada de St. Joachimstaler ou "O vale de São Joaquim" em razão de sua localização. A cidade de Joachimsthal pertencia ao Reino de Bohemia (na Alemanha) e ao Sacro Império Romano; atualmente se chama Jáchymov e pertence à República Checa. A moeda cunhada com a prata dessa mina foi denominada pela população local de Vale de São Joaquim (St. Joachimstaler) e posteriormente simplificada como Joachimsthaler e posteriormente simplificado para thaler. Em alemão arcaico "thal", hoje grafado "tal", significa "vale" e "thaler" quer dizer algo ou alguém do vale. Desse modo, etimologicamente, "thaler" é uma abreviação de "Joachimsthaler". Na Alemanha logo todas as cidades começaram a cunhar moeda semelhante ao thaler e utilizando-se o nome thaler. O thaler original era representado por um leão, do brasão de armas do Reino de Bohemia; bem como na versão holandesa, os daalders eram representados pelo "leeuwendaalder" (leão Thaler). O thaler foi a moeda oficial da Alemanha até 1908. Na Escandinávia, a thaler foi cunhada pelos reis suecos, que a

denominaram daler. Em 1570 essa moeda chegou a Holanda, onde foi cunhada com o desenho de um leão, com o que foi chamada Lowenthaler ou Thaler com o leão. Foi uma moeda tão popular que circulou em toda a Europa Oriental. A partir destes primeiros "thaler" desenvolveu o novo thaler; a moeda que o Sacro Império Romano tinha definido como padrão para o comércio entre as regiões da Europa. Na ortografia checa o thaler virou tolar. Na Espanha a thaler foi apelidada de talar ou tolar. Quando a Espanha controlou a América, esta moeda foi usada na América. Por causa da pronúncia, na América Tolar foi pronunciado Dólar. Aliás, o peso (moeda espanhola) foi apelidado de "dólar espanhol" na América do Norte e da abreviatura desse apelido (sobreposição das letras P e S) surgiu o cifrão ($). Outra teoria sustenta que o cifrão se originou da gravura de duas colunas (colunas de Hércules) contendo cada qual uma faixa enrolada formando um S constantes do brasão espanhol existente na moeda espanhola. No século XVII, sob domínio espanhol, a *Casa Real de la Moneda de Potosi*, na Bolívia (na época, Alto Peru), cunhava os reales de prata com o brasão espanhol contendo as Colunas de Hércules; com o tempo a gravura mudou para as colunas com uma flâmula entranhada com formato semelhante a um "S" deitado. A palavra "cifrão", derivada do árabe "cifr", significa "cifra" em português. Outra versão de sua origem é que, em meados dos anos 700, Táriq, um general árabe, para alcançar a Europa, teria partido da Arábia e passado, sucessivamente, pelo Egito, desertos do Saara e da Líbia, Tunísia, Argélia e Marrocos; cruzando o estreito das Colunas de Hércules (Gibraltar) e chegado, finalmente, à Espanha. Táriq mandou gravar em moedas uma linha sinuosa em forma de "S" (representando o caminho percorrido), cortando por duas colunas paralelas verticais (representando as Colunas de Hércules), formando o cifrão; que passou a ser reconhecido mundialmente como representação gráfica do dinheiro. Portanto, a palavra dólar significa thaler e a palavra "dólar" é o nome de mais de vinte moedas oficias (Afeganistão, Anguilla, Antígua e Barbuda, Austrália, Bahamas, Barbados, Belize, Bermuda, Bolívia, Bonaire, British, Brunei, Canadá, Cayman, Cingapura, Costa Rica, Dominica, El Salvador, Equador, Fiji, Filipinas, Granada, Guatemala, Guiana, Hong Kong, Ilhas Marshall, Ilhas Salomão, Ilhas Turks e Caicos, Ilhas Virgens Britânicas, Jamaica, Kiribati, Líbano, Libéria, Macau, Micronésia, Montserrat, Myanmar, Namíbia, Nauru, Nova Zelândia, Palau, Panamá, Paraguai, Peru, Saba, Saint Pierre e Miquelon, Santa Lúcia, São Cristóvão e Nevis, São Vicente e Granadinas, Singapura,

Suriname, Taiwan, Timor Leste, Trinidad e Tobago, Tuvalu, Uruguai, Zimbábue, etc.). Desse modo, seu nome sobreviveu em várias moedas contemporâneas, tais como o dólar ou o tólar esloveno (substituído pelo euro).

Durante muitos séculos os países cunharam em ouro suas moedas de maior valor, reservando a prata e o cobre para os valores menores. O problema das moedas de ouro era que o ouro não existia em grande quantidade e seu valor era muito alto para poder ser utilizado nos pagamentos cotidianos e por todas as pessoas. Desse modo, a prata por ser muito mais abundante e bem mais barata, foi o material mais empregado na cunhagem das moedas e, assim, disseminou e padronizou a cunhagem das moedas. E, ainda, para valores ainda menores, utilizava-se o cobre. Esses sistemas se mantiveram até o final do século 19, quando o cuproníquel e, posteriormente, outras ligas metálicas passaram a ser muito empregados, passando a moeda a circular pelo seu valor extrínseco; ou seja, pelo valor gravado em sua face, que independe do metal (ouro, prata, cobre, etc.) nela contido.

Em síntese, as dificuldades em pesar e avaliar o metal foram superadas por meio das moedas cunhadas, que possuem a esfinge (rosto, busto) do soberano garantindo o valor do metal precioso. Através disso as trocas passaram a serem feitas com maior facilidade, rapidez e praticidade. Após essa fase, com o progresso da metalurgia, as moedas metálicas passaram a ser feitas de ligas menos nobres e os governantes passaram a impor a obrigação legal de aceitação da moeda, o que facilitou a transição para a monetização de quase todas as relações econômicas.

Por outras palavras, quando o governante assume a cunhagem (emissão) da moeda, ela perde os requisitos de privada e facultativa para tornar-se pública e obrigatória; ou seja, os credores e vendedores são obrigados a aceitá-la como pagamento.

Embora, hoje, a forma circular seja adotada em quase todo o mundo, já existiram moedas ovais, quadradas, poligonais, etc. Assim elas já tiveram tamanhos ínfimos, como o *stater*, que circulou em Aradus, na Fenícia; como, também, grandes dimensões como as do *dáler*, peça de cobre na Suécia, no

século XVII. Também já foram cunhadas em diversos materiais não metálicos como madeira, couro e até porcelana. Moedas de porcelana circularam na Alemanha, quando, por causa da guerra, este país enfrentava grave crise econômica.

Uma das principais características da realidade monetária medieval era a grande diversidade de espécies de moedas em circulação (ouro, prata, cereais, etc.).

Com a disseminação do uso das moedas, para evitar o incômodo e o risco em carregá-las, desenvolveu-se uma tendência de deixá-las sob custódia de ourives e comerciantes, que as devolviam mediante a apresentação do recibo que emitiam.

Explica-se. Andar ou viajar com um saco de moedas de ouro e/ou prata era ariscado, porque as estradas e praças estavam cheias de ladrões. Então, os comerciantes depositavam suas moedas na casa de uma pessoa de confiança: o ourives; que era o encarregado de trabalhar com o ouro, outros metais nobres e joias preciosas. Esse procedimento é basicamente o mesmo das atuais casas de penhor. Em troca das moedas que lhe davam para guardar, o ourives entregava um recibo no qual prometia devolvê-las quando o dono as pedisse. Sempre que comprava mercadorias, o comerciante ia ao ourives para retirar parte de suas moedas para efetuar os pagamentos. Por sua vez, o dono da mercadoria recebia as moedas do comerciante e, também, as depositava na casa do ourives. Como os ourives ficaram cansados dos repetitivos e constantes recibos pelas mesmas moedas, tiveram a ideia de que em vez de ficarem sucessivamente guardando, entregando e guardando novamente os mesmos ouro e prata, era melhor o comprador pagar o vendedor através de um recibo de papel que representavam uma quantidade de ouro e de prata (ou seja, um certificado de titularidade ou propriedade) depositado com o ourives. Além de guardar o dinheiro, os ourives começaram a emprestá-lo a reis, governantes e outras pessoas, em troca de algum benefício ou favor. Assim, muitos ourives se tornaram os primeiros banqueiros. Durante muito tempo, os recibos dos ourives foram usados como notas, trocados pelo ouro e prata depositados nas arcas dos banqueiros. Hoje, continuamos a usar notas, mas já não as trocamos por ouro e prata,

como se fazia antes. Com elas, compramos as coisas de que precisamos ou que queremos.

OSCILAÇÕES MOMENTÂNEAS DA MOEDA

As moedas refletem a mentalidade de um povo e de sua época. Nelas podem ser observados aspectos políticos, econômicos, tecnológicos e culturais. É pelas impressões encontradas nas moedas que conhecemos, hoje, a efígie de personalidades que viveram há muitos séculos. Provavelmente, a primeira figura histórica a ter sua efígie registrada numa moeda foi Alexandre, o Grande, da Macedônia, por volta do ano 330 a.C.

Ressalta-se, ainda, que, em tempos de guerra, hiperinflação ou outras circunstâncias de escassez ou falta da moeda convencional, as pessoas a substituem por outras coisas. Senão vejamos alguns exemplos.

Na Franca, no século XIII, substituíram a moeda por fichas metálicas em que se registravam créditos e débitos.

Durante a Guerra Civil Americana, selos acondicionados em pequenos discos de papelão, zinco ou couro; recobertos por plástico ou vidro, foram usados como moeda.

Durante os eventos devastadores da Primeira Guerra Mundial e no pós-guerra, a Alemanha não tinha mais capacidade de produzir moedas de metal em grande quantidade e, assim, socorreu-se do “notgeld”, ou seja, dinheiro de emergência. Dessa forma, os valores eram impressos em qualquer coisa, tais como quaisquer pedaços de papel, cartas de baralho, retalhos ou recortes de couro, pedaços de madeira, etc.

Ainda mais, os alemães, após a Primeira Guerra Mundial, emitiram peças de porcelana como moedas, devido à falta de metais; pois os mesmos foram usados em armas, munições, veículos e construções de guerra.

Durante a Segunda Guerra Mundial o cigarro atingiu um *status* de moeda e o mercado foi quase que completamente unificado. Apenas vendas com cigarros era aceita; não havia permuta. O cigarro era o único instrumento que visava relaxar o controle emocional para o soldado em campanha. Após a Segunda Guerra Mundial, cigarros e gasolina eram usados como uma forma

de moeda-mercadoria em algumas partes da Europa, incluindo Alemanha, França e Bélgica.

Ainda durante a Segunda Guerra Mundial, as Ilhas do Canal da Mancha (território britânico) foram ocupadas pelos nazistas e os moradores do local não tiveram opção senão utilizarem do dinheiro criado pelos invasores ante a falta da moeda local.

Com o fim da Segunda Guerra Mundial, a Alemanha estava destruída e a penúria imperava por toda parte. Havia dinheiro (*Reichsmark*) suficiente, mas não se podia comprar nada com ele. A escassez era administrada com senhas de distribuição pelos países aliados. O comércio de troca fazia parte do cotidiano e o cigarro era a moeda clandestina. O dinheiro tinha que readquirir valor real e poder aquisitivo. Assim, em junho de 1948, os norte-americanos, ingleses e franceses distribuíram 10 bilhões, 701 milhões e 720 mil marcos alemães (*Deutsche Mark*), a nova moeda do pós-guerra aos alemães em substituição ao desacreditado *Reichsmark*. Estratégia semelhante foi utilizada no Brasil que, depois de oito trocas monetárias (réis, cruzeiro, cruzeiro-novo, cruzado, cruzado-novo, cruzeiro e cruzeiro real), através do Plano Real, instituiu uma nova moeda (Real) em 1994.

Na Itália, nos anos 70, a moeda foi substituída por caramelos, recebendo o nome de liras caramelo.

A Disney começou a emitir seu próprio dinheiro em 1987 para ser usado nos parques da empresa na Califórnia e na Flórida. Agora eles podem ser utilizados em todos os *resorts* (estâncias) do grupo nos Estados Unidos, em cruzeiros, lojas da Disney e em partes da ilha privada da empresa. O troco é dado em dólares americanos (US$).

De forma semelhante, a moeda (*token*) oficial no *Tomorrowland* ("Terra do Amanhã"), no parque Maeda, em Itu - SP, valeu mais que o dólar (http://www1.folha.uol.com.br/ilustrada/2015/05/1624165-moeda-oficial-no-tomorrowland-vale-mais-que-dolar-e-rende-pouco.shtml).

Quando a Transnístria declarou sua independência da Moldávia após o colapso da União das Repúblicas Soviéticas Socialistas (URSS ou, OCCC,

em russo), o governo local colou selos postais em antigas notas da URSS como solução provisória.

Após a queda do presidente Mobutu em 1997, o governo do Zaire (atual Congo) viveu um período de falta de moeda corrente enquanto novas notas eram impressas. Assim eles simplesmente recortaram das cédulas antigas o desenho do busto do ditador deposto e as continuaram usando até que as novas entrassem em circulação.

Em São Paulo, anos atrás, fichas telefônicas, chicletes, balas e passes/bilhetes de ônibus substituíam as moedas de pequeno valor.

Nas prisões e nos campos de prisioneiros de guerra modernos, os cigarros servem muitas vezes de dinheiro. Até os prisioneiros não fumadores se mostraram dispostos a aceitar cigarros como forma de pagamento e a calcular o valor dos seus bens e serviços em cigarros.

Os créditos de carbono também podem ser considerados como moeda no mercado financeiro internacional. O Mercado de Carbono surgiu a partir da criação da Convenção-Quadro das Nações Unidas sobre a Mudança Climática (UNFCCC, em inglês), durante a ECO-92, no Rio de Janeiro.

Os créditos de carbono ou Redução Certificada de Emissões (RCE) são certificados emitidos para uma pessoa ou empresa que reduziu a sua emissão de gases do efeito estufa (GEE). Por convenção, 1 tonelada de dióxido de carbono (CO_2) corresponde a um crédito de carbono. Este crédito pode ser negociado no mercado internacional. A redução da emissão de outros gases, igualmente geradores do efeito estufa, também pode ser convertida em créditos de carbono, utilizando-se o conceito de Carbono Equivalente (equivalência em dióxido de carbono). Comprar créditos de carbono no mercado corresponde aproximadamente a comprar uma permissão para emitir GEE. O preço dessa permissão, negociada no mercado, deve ser necessariamente inferior ao da multa que o emissor deveria pagar ao poder público, por emitir GEE. Para o emissor, portanto, comprar créditos de carbono no mercado significa, na prática, obter um desconto sobre a multa devida. As nações que não conseguirem (ou não desejarem) reduzir suas

emissões podem comprar os CER em países em desenvolvimento e usá-los para cumprir suas obrigações.

- http://www.brasil.gov.br/meio-ambiente/2012/04/entenda-como-funciona-o-mercado-de-credito-de-carbono.

As empresas que conseguem reduzir a emissão dos gases poluentes lucram com a venda destes créditos de carbono. Este sistema visa privilegiar as indústrias que reduzem a emissão destes gases, pois seus lucros com a venda dos créditos aumentam. Já os países mais desenvolvidos podem incentivar os países em desenvolvimento a reduzirem a emissão de gases poluentes, comprando os créditos no mercado de carbono.

Algum tempo atrás, o "Estado Islâmico" começou a emitir suas próprias moedas. Feitas em ouro, elas foram baseadas no desenho do dinar iraquiano do califado de Uthman e contendo sete hastes de trigo numa referência ao Corão (livro sagrado dos muçulmanos).

- http://www.spiegel.de/forum/wirtschaft/gold-und-silbermuenzen-islamischer-staat-fuehrt-eigene-waehrung-ein-thread-188091-5.html;

- http://opiniaoenoticia.com.br/economia/estado-islamico-estaria-emitindo-uma-moeda-propria/.

HISTÓRIA E ORIGEM DOS BANCOS

A dificuldade e o risco do transporte de metais levaram à criação de casas de custódia, que armazenavam o ouro e a prata, fornecendo em contrapartida certificados de depósitos que, por serem mais cômodos e seguros, passaram a circular no lugar dos metais monetários. Esses certificados ficaram conhecidos como moeda representativa ou moeda-papel.

O conceito do sistema bancário originou-se na Babilônia cerca de 3000 a.C. devido às atividades de templos e palácios que forneceram lugares seguros para o armazenamento de objetos de valor.

Os **primeiros bancos** oficiais surgiram na Inglaterra. A palavra inglesa "bank" deriva da palavra italiana "banco", peça de madeira que os comerciantes de valores oriundos da Itália e estabelecidos em Londres utilizavam para realizar os seus negócios no mercado público londrino.

Desse modo, o desenvolvimento de sistemas monetários demandou o surgimento de um novo tipo de moeda: a moeda-papel. A moeda-papel veio para contornar os inconvenientes da moeda metálica (por exemplos, peso e risco de roubo), embora valessem com lastro nela. Assim surgem os certificados de depósito, emitidos por casas de custódia em troca do metal precioso nela depositado. Por ser lastreada, essa moeda representativa poderia ser convertida em metal precioso a qualquer momento, e sem aviso prévio, nas casas de custódia. A moeda-papel abre espaço para o surgimento da moeda fiduciária, ou papel-moeda, modalidade de moeda não lastreada totalmente.

Desse modo, houve uma grande evolução com a passagem das moedas metálicas às notas bancárias, convertíveis em moedas em prata e ouro. Com o seu aparecimento passam a conviver na circulação duas formas de moeda intimamente interdependentes, mas distintas, em que uma delas constitui a base da criação da outra. O seu uso começou com a entrega, aos credores ou aos depositantes de promessas de pagamento, de verdadeiras notas ou ordens de pagamento. Estes instrumentos representaram um importante papel como meio de pagamento.

Na Idade Média, surgiu o costume de se guardar os valores com um ourives, pessoa que negociava objetos de ouro e prata. Este, como garantia, entregava um recibo. Com o tempo, esses recibos passaram a ser utilizados para efetuar pagamentos, circulando de mão em mão e dando origem à moeda de papel.

Ao longo dos séculos, a requisição de jazidas de ouro e de prata para a fabricação de moedas acabou se tornando cada vez mais difícil. Por isso, o papel-moeda acabou ganhando maior espaço no desenvolvimento das transações comerciais. Na Baixa Idade Média, a falta de moedas motivava os comerciantes das feiras a utilizarem letras de câmbio para o estabelecimento de alguma negociação.

Os primeiros registros da utilização do papel como moeda remontam do ano 89. As matrizes para a impressão eram confeccionadas em tabuleiros de madeira ou de bambu, sobre as quais era aplicada uma pasta especial, feita de polpa vegetal amolecida e batida. A madeira recebia tinta e os desenhos e textos gravados eram passados para o papel. Essa invenção permaneceu escondida durante séculos; sua importância pode ser exemplificada pelo fato de os chineses terem erguido um templo em homenagem ao inventor dessa técnica. A partir do ano 610 missionários cristãos espalharam a novidade em outras terras. Mas foi o comerciante veneziano Marco Polo que mais se encantou com a técnica de fabricação do papel-moeda chinês, que publicou no seu livro *Le Livre* de Marco Polo, entre suas experiências na China, onde ficou dezessete anos.

No Brasil, os primeiros bilhetes de banco, precursores das cédulas atuais, foram lançados pelo Banco do Brasil, em 1810. Tinham seu valor preenchido à mão, tal como, hoje, fazemos com os cheques.

O dinheiro, portanto, também se apresenta como uma comódite (*commoditie* ou *commodity*); vez que as instituições financeiras e de crédito emprestam dinheiro em troca de juros e negociam moedas estrangeiras no mercado de câmbio. Assim como qualquer metal ou pedra preciosa, o dinheiro é negociado por outras formas de dinheiro (moedas estrangeiras, contratos de taxas de inflação e juros, títulos de crédito, ações, etc.).

A moeda de papel evoluiu quanto à técnica utilizada na sua impressão. Hoje a confecção de cédulas utiliza papel especialmente preparado e diversos processos de impressão que se complementam, dando ao produto final grande margem de segurança e condições de durabilidade.

Com o advento do papel-moeda a cunhagem de moedas metálicas ficou restrita a valores inferiores, necessários para troco. Dentro desta nova função, a durabilidade passou a ser a qualidade mais necessária à moeda. Surgem, em grande diversidade, as ligas modernas, produzidas para suportar a alta rotatividade do numerário de troco.

Ao longo do tempo, foi observado que, apesar do fluxo permanente de conversão e de emissões de certificados mediante novos depósitos, sempre restava uma parcela de metais ociosa. Com base nessa constatação, certificados não lastreados (ou parcialmente lastreados) começaram a ser emitidos, levando à criação da moeda fiduciária (dependente de confiança).

A facilidade em transportar e guardar os recibos fez com que estes passassem a circular no lugar das moedas, alongando-se cada vez mais o tempo que se levava para resgatá-las, transformando-se o depositário em banqueiro. Está aí a origem dos bancos e do papel-moeda. Os recibos aos poucos foram sendo padronizados ou uniformizados, surgindo as notas bancárias. As transferências eram feitas por meio de endossos nos recibos ou por avisos aos bancos. Os avisos também foram se padronizando, dando origem aos cheques.

Em Amsterdã, por volta do ano 1500, o povo costumava depositar seu dinheiro com *cashiers*, o que representava menor risco do que guardá-lo em casa. Os *cashiers* concordavam em arrecadar e cancelar débitos por meio de ordens escritas dos depositantes (cheques).

Na Inglaterra, no fim do século XVII, o povo começou a fazer depósitos com os Goldsmiths. O Goldsmith dava ou emitia a favor do seu cliente, *goldsmith notes*. Estas simples notas escritas a mão continham uma promessa de pagamento ao cliente ou à sua ordem.

O uso do cheque apresenta muitas vantagens: facilita a movimentação de grandes somas; economiza o tempo que tomariam para ser contadas; diminui possibilidade de roubos, além de impedir o entesouramento do dinheiro em espécie.

Em 1696, iniciou-se a moderna emissão fiduciária sobretudo com os bilhetes do Tesouro do Banco da Inglaterra. Estes bilhetes supriram a escassez da circulação e desempenharam um papel importante no advento da estabilidade financeira.

Como o dinheiro é realmente apenas uma representação de valor, não demorou muito para que as pessoas percebessem que poderiam apenas enviar informação sobre o dinheiro por telégrafo, telex, bilhetes ou através de meios eletrônicos, que seria tão eficaz quanto enviar o próprio dinheiro. Depois da Segunda Guerra Mundial, os bancos registravam informações sobre as transações do dia em grandes bobinas magnéticas, que eram levadas ao *Federal Reserve* (Banco Central). Este sistema eliminava a necessidade de notas para grandes valores, que eram impressas antes da guerra para facilitar estas transferências em larga escala. Hoje, as notas de US$ 500, US$ 1.000, US$ 5.000, e de US$ 10.000, impressas durante este período são muito raras, embora haja algumas ainda em circulação.

Depois foram estabelecidas as conexões via cabo entre os bancos para que as informações de transferências pudessem ser enviadas diretamente. Nos Estados Unidos, no início dos anos 90, todas as transferências entre os bancos e o *Federal Reserve* eram feitas eletronicamente.

A Administração de Segurança Social americana (SSA - *Social Security Administration*) foi a primeira a oferecer o depósito eletrônico automático de dinheiro nas contas bancárias em 1975. Em razão de as pessoas se sentirem cômodas, confortáveis e seguras com o dinheiro sendo acrescentado às suas contas sem que tivessem de se preocupar, a prática se espalhou e, assim, passaram a pagar contas, enviar e transferir dinheiro eletronicamente.

Moeda escritural é o nome que se dá ao uso dos depósitos bancários como meio de pagamento. É representada pelos depósitos à vista nos bancos

ou instituições de crédito, e que se encontrem, em tese, à livre disposição dos seus depositantes. Fazem parte dos meios de pagamento da economia e permitem a realização de transações sem necessidade da utilização de moeda (papel-moeda ou peças metálicas). A moeda escritural cumpre satisfatoriamente o papel de meio de troca, diferenciando-se do papel-moeda apenas por não ter curso forçado, sendo, portanto, uma moeda fiduciária, pois seu valor é devido apenas à confiança depositada no banco emissor. Seu principal meio de movimentação hoje em dia são os cheques e os cartões de plástico (bancários, de crédito e de débito) e eletrônicos (imateriais). Há outras formas de movimentação da moeda escritural, que incluem as transferências de crédito, as ordens de pagamento, as transferências eletrônicas disponíveis (TEDs), os documentos de crédito (DOCs) e os documentos (boletos) de cobrança/pagamento.

> "A moeda corrente é composta de papel-moeda e de moeda metálica. No entanto nem toda moeda corrente em circulação é mantida pelo [poder] público. Parte é mantida pelo governo, pelo Bacen, e parte pelos bancos comerciais. Os depósitos dos bancos comerciais no Bacen são classificados na categoria de dinheiro governamental. Esses depósitos, que são simplesmente registros, servem como reservas para os bancos comerciais e são considerados equivalentes às notas do Bacen, desde que as notas e as reservas possam ser trocadas entre si a qualquer tempo a um custo igual a zero. Esses depósitos são tratados como apenas registros contábeis e não como notas legais do Bacen, raramente mudam de propriedade, e o uso de apenas lançamentos contábeis elimina o custo de impressão que seria necessário se tivesse que existir uma correspondência em notas." (Mercado de Capitais, José Wladimir Freitas de Fonseca, IESDE, 2009, páginas 64/65).

Na ficção, os cartões de crédito existem desde 1887, quando foram narrados no livro *Looking backward* de Edward Bellamy. A obra conta a história de um homem que adormeceu e acordou 113 anos mais tarde, em 2000, quando cartões de papelão substituíam dinheiro.

Criado nos Estados Unidos, na década de 1920, o cartão de crédito surgiu quando postos de gasolina, empresas e hotéis começaram a oferecê-los aos seus clientes mais fiéis, fazendo com que eles pudessem usufruir de seus

serviços sem a utilização de dinheiro ou cheque. Mas somente em 1950 que definitivamente apareceu o primeiro cartão de crédito realmente funcional, lançado pela empresa Diners.

Com os avanços tecnológicos, foi possível transformar a moeda em um conjunto de registros eletrônicos que representam uma diversidade de ativos. As trocas, atualmente, são feitas por meios sofisticados, como cartões eletrônicos e cartões de crédito.

Moeda escritural é um tipo de dinheiro não-físico usado como meio de pagamento; ou seja, o saldo existente na conta bancária. Para ser mais preciso, são unicamente os meros dígitos de computador ou caracteres eletrônicos constantes do banco de dados da instituição financeira. Por outras palavras, esse dinheiro não existe de verdade; ou seja, não existe na forma física, não há nenhum lastro equivalente e nem garantia real, não passando de meros números constantes do saldo da conta bancária. Esses valores, não passam de meros dígitos eletrônicos ou informações digitais existentes unicamente dentro dos sistemas (rede de computadores) das instituições financeiras. A moeda escritural, na grande maioria das vezes, é movimentada (entra e sai da conta) através de depósitos e transferências eletrônicas, cheques e os cartões de crédito e débito; portanto, do mesmo modo que entra, ela sai da conta bancária.

Os dados ou informações em um computador são denominados de **códigos binários**. A palavra binário significa que algo possui duas unidades ou é composto por dois elementos de informação; no caso da computação, se refere aos números 0 (zero) e 1 ou positivo e negativo. Portanto, em computação trata-se de um sistema numérico em que todas as quantidades se representam baseados apenas em dois números. Através da alocação de elétrons, um bit convencional é capaz de assumir uma única informação como positiva ou negativa (0 ou 1) e, assim, toda informação assume apenas duas possibilidades. É desse modo que o computador vê tudo e através da álgebra booleana (sim ou não, verdadeiro ou falso, ligado ou desligado, positivo ou negativo, 0 ou 1, etc.) é que o computador processa os dados. É a linguagem própria dos computadores ou das máquinas. O **ASCII** (*American Standard Code for Information Interchange*) é a codificação de caracteres de oito bits usada pelos computadores para a representação

textual. É por meio dos códigos ASCII que o computador reproduz 256 caracteres. Desse modo, no sistema binário o número 0 é representado por 0000, o 1 é 0001 e o 2 é 0010. Em computação, portanto, tudo é 0 e 1. Cada valor do código binário (ou base 2) é denominado de "bit" (*binary digit*), que é a menor unidade de informação. Quando 8 bits se juntam eles formam 1 byte (*Binary Term*) e um agrupamento de 4 bits é chamado de *nibble*. Em resumo, os dados de um computador são medidos em bits e bytes.

Medida	Sigla	Equivalência	Caracteres	Bytes
Byte		2^0	1 (8 bits)	1 byte
Kilobyte	**KB**	2^{10}	1.024	1.024 bytes
Megabyte	**MB**	2^{20}	1.048.576	1.024 KBytes
Gigabyte	**GB**	2^{30}	1.073.741.824	1.024 MBytes
Terabyte	**TB**	2^{40}	1.099.511.627.776	1.024 GBytes
Pentabyte	**PB**	2^{50}	1.125.899.906.842.624	1.024 TBytes
Hexabyte	**HB**	2^{60}	1.152.921.504.606.846.976	1.024 PBytes
Yotabyte	**YB**	2^{80}	1.208.925.819.614.630.000.000.000	1.024 Hexabyte

Do mesmo modo que Samuel Morse, em 1837, inventou o código telégrafo elétrico (Código Morse) através do qual meros sons de bips ou pontos e traços reproduzem o alfabeto e os números, o sistema binário consegue fazer algo semelhante; só que em vez de ponto e traço ou bip curto e longo, o sistema binário usa 0 e 1. O ábaco era capaz de realizar operações aritméticas baseadas em métodos similares aos dos computadores modernos. O ábaco é um antigo instrumento de cálculo, formado por uma moldura com varetas paralelas cotendo pequenas peças atravessadas que podem ser movimentadas com os dedos. Cada vareta representa uma casa decimal (unidades, dezenas, centenas, etc.) e cada peça representa os dígitos dos números. Um microchip é um circuito eletrônico miniaturizado, composto de um aglomerado de transistores, cujo principal componente é o transistor (além de outros componentes eletrônicos menos importantes); que desempenha duas funções: amplificação (controle do fluxo da corrente elétrica) e chaveamento (interruptor da corrente elétrica). No transistor a própria corrente elétrica controla a corrente elétrica. Todo corpo metálico possui elétrons livres que são agitados e movimentados através da temperatura (calor). Através do efeito termoiônico, os elétrons escapam do

material formando uma nuvem eletrônica próxima à superfície do corpo. Se houver um outro corpo metálico positivamente carregado próximo a essa nuvem, os elétrons serão atraídos e uma corrente elétrica se estabelecerá. Um relê é um dispositivo eletromecânico composto por uma bobina e contatos. A bobina é um solenoide que, ao ser percorrido por uma corrente elétrica de amplitude adequada, energiza-se e movimenta os contatos. A posição dos contatos dos relês comporta-se como uma variável booleana, que só pode assumir um de dois estados possíveis, aberto ou fechado. A isso deu-se o nome de álgebra de chaveamento e os valores possíveis das variáveis, 0 ou 1, passaram a representar condições físicas: ligado ou desligado, com tensão alta ou com tensão baixa, aberto ou fechado, entre várias outras. Nos aparelhos receptores de rádio, os cristais retificadores serviam para separar a onda portadora (veja frequência no glossário) da informação que ela carregava; as válvulas termoiônicas substituíram os cristais retificadores. As primeiras válvulas eram do tipo diodo (possuíam dois eletrodos) e nada mais eram do que uma adaptação da lâmpada. Consistiam de um cilindro metálico (o catodo, isto é, o eletrodo negativo), que era aquecido por meio de um filamento existente em seu interior. Este cilindro era envolvido por outro, também metálico, que constituía o anodo da válvula (o eletrodo positivo). Aplicando-se uma tensão elétrica aos dois eletrodos, os elétrons que eram emitidos pelo catodo aquecido em virtude do efeito termoiônico dirigiam-se para o anodo. Assim como os cristais retificadores dos rádios, era possível, com elas, separar uma onda portadora da informação carregada por ela. Depois foi adicionado um novo componente à válvula: um terceiro eletrodo, chamado grade (uma rede ou espiral de pequeninos fios envolvendo o catodo). O potencial negativo da grade controlava o fluxo dos elétrons do catodo para o anodo. Quanto menor o potencial negativo da grade, mais elétrons podiam fluir através da válvula; ou seja, a grade funcionava como uma espécie de controle de corrente elétrica na válvula como uma torneira controla o fluxo de água. Dessa forma, era possível injetar na grade um sinal bem fraco (como o que chega de uma antena) e obter um sinal praticamente idêntico, porém bem mais forte, entre o catodo e o anodo. Em outras palavras, era possível utilizar a válvula como um dispositivo amplificador. Por possuir três eletrodos, esse tipo de válvula termoiônica ficou conhecida como triodo. O próximo passo foi o uso de materiais chamados semicondutores (principalmente silício e germânio); que são materiais que não podem ser classificados nem como condutores e nem

como isolantes, sendo, portanto, intermediários. Ao se adicionar pequenas quantidades de fósforo ao silício, obtém-se um condutor elétrico semelhante a um metal (a condução elétrica é feita por elétrons livres); trata-se do semicondutor tipo n (condução feita por cargas negativas). Já uma pequena quantidade de boro adicionada ao silício puro, também conduz eletricidade, mas com cargas positivas; trata-se do semicondutor do tipo p (condução por cargas positivas). Passou-se, assim, a colocar lado a lado as amostras de silício tipos p e n, formando-se uma junção pn e ligando-a num cristal com o controle desde a resistência total até a fluição total da corrente elétrica pelo cristal. A junção pn, portanto, se assemelha à uma válvula diodo, deixando passar corrente elétrica em um sentido (de p para n) e impedindo a passagem no sentido contrário (de n para p). Depois a válvula triodo também foi substituída por um dispositivo semicondutor. Através de um cristal semicondutor com duas junções (pnp ou npn) produz-se amplificações semelhantes àquelas conseguidas com as válvulas. Assim, uma pequena corrente elétrica na camada central (como um sinal de rádio que viajou grandes distâncias) é capaz de controlar o fluxo maior de corrente entre as duas outras camadas. Dessa forma, a corrente mais forte imita o comportamento da corrente mais fraca. O resultado foi uma versão amplificada do sinal fraco. Esse triodo semicondutor foi chamado de transistor; que desempenha duas funções: amplificação e chaveamento. Portanto, a corrente elétrica também consegue transportar informações como as ondas de rádios fazem. Quem nunca ouviu falar de transmissões de rádio, de TV, de aparelho de FAX, de telefone, de celular, de WIFI, de GPS, etc.?

Em apertada síntese, **moeda escritural são apenas "bits" (dados eletrônicos)**.

> "Toda informação introduzida em um computador (sejam dados que serão processados ou instruções de um programa) precisa ser entendida pela máquina, para que possa interpretá-la e processá-la. Neste texto, as informações apresentadas em forma de caracteres são entendidas pelo leitor porque ele conhece o formato e o significado dos símbolos que representam os caracteres alfabéticos, os numéricos (algarismos) e os sinais de pontuação ou matemáticos (+, -, X, /, >, <, = etc.). O computador, sendo um equipamento eletrônico, armazena e movimenta as informações internamente sob forma eletrônica; esta pode ser um

valor de voltagem ou de corrente (sabemos também que na memória secundária as informações são armazenadas sob forma magnética ou ótica)." (http://www.di.ufpb.br/raimundo/Generalidades/RepInfo.html).

"Bit é a sigla para Binary Digit, que em português significa dígito binário, ou seja, é a menor unidade de informação que pode ser armazenada ou transmitida. É geralmente usada na computação e teoria da informação. Um bit pode assumir somente 2 valores, como 0 ou 1. Os computadores são idealizados para armazenar instruções em múltiplos de bits, que são denominados bytes. [...]. Fisicamente, o valor de um bit é armazenado como uma carga elétrica acima ou abaixo de um nível padrão em um único capacitor dentro de um dispositivo de memória. Mas, bits podem ser representados fisicamente por vários meios, como pela eletricidade, fibras ópticas, rede wireless etc." (http://www.significados.com.br/bit-e-byte/).

"Os computadores "entendem" impulsos elétricos, positivos ou negativos, que são representados por 1 ou 0. A cada impulso elétrico damos o nome de bit (BInary digiT). Um conjunto de 8 bits reunidos como uma única unidade forma um byte. [...]. Para que isso aconteça, os computadores utilizam uma tabela que combina números binários com símbolos: a tabela ASCII (*American Standard Code for Information Interchange*). Nela, cada byte representa um caractere ou um sinal." (http://www.infowester.com/bit.php).

Diante dessas informações iniciais, já podemos dizer que a **moeda escritural é o nome que se dá às transferências de dígitos entre as contas bancárias**. Faz parte, portanto, dos meios de pagamento da economia e permite a realização de transações sem necessidade da utilização de moeda (papel-moeda ou moeda metálica).

- http://exame.abril.com.br/seu-dinheiro/noticias/gustavo-franco-explica-a-magia-do-dinheiro.

Vamos ser bem claros: não existe dinheiro real! Moeda escritural não é dinheiro “de verdade” ou físico! **A moeda escritural, não passa de um valor contábil no sistema eletrônico do banco**. E o banco simplesmente digita esses valores (credita) nas contas como se fosse dinheiro. Todos os

créditos e empréstimos bancários são simplesmente dígitos inseridos no saldo da conta bancária. Não há o dinheiro de verdade. O banco inventa dígitos ou cria dinheiro do nada.

> "Em vez de atuarem como intermediadores da poupança e do investimento, os bancos na realidade possuem o privilégio legal e exclusivo de criar dinheiro do nada, emprestarem este dinheiro e cobrarem juros sobre ele. Como se trata de algo importante e bizarro demais para ser ignorado, vale a pena enfatizar: bancos possuem o privilégio legal, concedido pelo estado, de criar dinheiro eletrônico, de emprestar estes dígitos eletrônicos para pessoas e empresas, e de cobrar juros sobre eles. Algo que lhe daria cadeia se você fizesse, os bancos fazem com a autorização e até mesmo com um forte incentivo estatal. [...]. Os bancos de hoje lidam majoritariamente com dígitos eletrônicos que eles próprios criam. E, quando você lida com dígitos eletrônicos que podem ser criados do nada, você não se preocupa com a origem daquele dígito. Se você pode criar dígitos eletrônicos para emprestar para João, você não tem de se preocupar em remover estes dígitos eletrônicos da conta do José. Você pode criar os dígitos eletrônicos na conta de João ao mesmo tempo em que José segue tendo total e irrestrito acesso aos dígitos eletrônicos dele. Sendo assim, a realidade é que, para todas as operações de concessão de crédito, os bancos criam dinheiro eletrônico do nada e emprestam este dinheiro para pessoas, empresas e governos (federal, estaduais e municipais), em um processo que veremos mais abaixo. Dado que tais depósitos bancários assim criados não vieram da poupança, podemos dizer que está havendo a criação de crédito bancário (e não de crédito real). É importante frisar isso: no atual sistema bancário, todo o crédito é bancário. Trata-se de dígitos eletrônicos que são criados pelos bancos e acrescidos às contas dos tomadores de empréstimos. Nenhum dinheiro está sendo removido de uma conta para outra. Está havendo apenas a criação de dígitos eletrônicos. [...]. Portanto, eis aqui a primeira e primordial constatação: todo o dinheiro que está hoje na forma de dígitos eletrônicos em contas e aplicações bancárias entrou na economia de uma única maneira: criação de crédito bancário. Não há nenhuma outra maneira de o dinheiro entrar na economia geral a não ser pela criação de crédito bancário. E agora a segunda constatação, derivada da primeira: a principal fonte de todos os

> depósitos bancários que hoje existem na economia não são os depositantes, mas sim os empréstimos que os bancos criam do nada. Os depósitos são a consequência destes empréstimos. Contas bancárias são produto da criação de crédito, e não o contrário. Uma pessoa, uma empresa ou um funcionário do governo vai ao banco e pede um empréstimo. Ato contínuo, o banco cria, do nada, dígitos eletrônicos na conta desta pessoa. Nenhuma outra conta foi subtraída neste processo. A quantidade de dinheiro eletrônico na economia simplesmente aumentou. Ao ser gasto, este dinheiro recém-criado vai parar nas contas de outras pessoas e empresas. Dali, ele vai para o depósito ou aplicação que este recebedor final escolher. Os bancos criam dinheiro eletrônico sempre que fazem qualquer tipo de empréstimo ou de investimento. Sem exceção." (O sistema bancário brasileiro e seus detalhes quase nunca mencionados, Leandro Roque, disponível em http://www.mises.org.br/Article.aspx?id=1387).

Desse modo, por exemplo, se alguém possui o saldo de R$ 100.000,00 (cem mil reais) na sua conta bancária, na realidade o banco só tem uma parte desse valor em dinheiro "de verdade" (cédulas). Esse percentual é denominado de reserva e equiparável ao que as empresas prestadoras de acesso à Internet fazem; ou seja, a pessoa contrata uma velocidade, mas a empresa só é obrigada a fornecer apenas um percentual dessa velocidade fictícia contratada (atualmente é de 80% da taxa de transmissão média mensal de Internet e 40% da taxa de transmissão instantânea de Internet). Diante disso, absolutamente nenhum banco tem dinheiro suficiente para poder entregar os equivalentes dos saldos em cédulas a todos os seus clientes.

> "Esse tipo de fraude ou falsificação é dignificado com a alcunha "sistema bancário de reservas fracionárias", o que significa que os depósitos bancários são lastreados por apenas uma pequena fração do dinheiro que o banco promete ter em mãos no momento do resgate. [Nos EUA, esse valor sempre girou em torno de 10%. No Brasil, ele era de 36% até outubro de 2008. Atualmente está em 28%]." (O sistema bancário de reservas fracionárias, Murray N. Rothbard, publicado em 11/05/2010, disponível em http://www.mises.org.br/Article.aspx?id=311).

"No caso da moeda bancária, ocorre o mesmo processo utilizado na moeda-papel conversível. Permanecendo parte dos depósitos sem movimento, os bancos emprestam certa importância que vai de 75% a 93% dos depósitos, ficando a outra parte como encaixe, variando sua percentagem conforme a legislação bancária de cada país. Há uma proporção entre depósitos, encaixe e empréstimos." (http://www.bcb.gov.br/htms/museu-espacos/cheque.asp).

"Nesse sistema, os bancos emprestam grande parte dos depósitos a vista, retendo compulsoriamente apenas uma fração desses depósitos. Isso quer dizer, em termos práticos, que se todos os depositantes forem ao banco ao mesmo tempo sacar seu dinheiro, o banco quebra." (Revista da Procuradoria-Geral do Banco Central, volume 5, nº 1, junho de 2011, p. 35; *in* http://www.bcb.gov.br/pgbcb/102011/PGBC_volume5_n1_internet_rev.pdf).

O depósito compulsório é geralmente feito através de determinação legal, obrigando os bancos comerciais e outras instituições financeiras a depositarem, junto ao Banco Central, parte de suas captações em depósitos à vista ou outros títulos contábeis. O principal objetivo do depósito compulsório é evitar a multiplicação descontrolada da moeda escritural. Esse percentual pode mudar a qualquer tempo se o governo quiser reduzir a quantidade de empréstimos bancários. O depósito compulsório é a reserva obrigatória (reversa bancária ou reserva fracionária) recolhida dos depósitos bancários, conforme percentual fixado pelo Banco Central do Brasil (Circular nº 3.632/2013): recursos à vista: 45% (quarenta e cinco por cento), recursos a prazo: 20% (vinte por cento) e depósitos de Poupança: 15,5% (quinze e meio por cento) da média diária dos saldos na modalidade rural e 24,5% (vinte e quatro e meio por cento) nas demais modalidades.

- http://www.bcb.gov.br/htms/novaPaginaSPB/Resumo_das_normas_dos_compulsórios.pdf;
- https://www.bcb.gov.br/htms/novaPaginaSPB/Resumo_das_normas_dos_compulsórios.pdf;

- http://www.bcb.gov.br/conteudo/home-ptbr/FAQs/FAQ%2012-Dep%C3%B3sitos%20Compuls%C3%B3rios.pdf.

Prova disso é que quando se quer sacar (levantar em cédulas) algum valor relativamente considerável, o funcionário do banco vai verificar se existem cédulas suficientes para isso, senão vai pedir para a pessoa ir em outra agência ou agendar para retornar outro dia.

Quando um cliente do banco encerra sua conta ou saca um percentual alto do seu saldo, na verdade ele está levando as cédulas de vários outros. Portanto, se todos os clientes do banco, de repente, exigirem o seu dinheiro em cédulas, o banco não terá como fazer isso, pois só tem uma parcela desse dinheiro.

O papel-moeda recebe o nome de moeda manual ou moeda corrente para distingui-lo da moeda escritural.

Aí fica uma dica, quando for negociar com o banco, use como "carta na manga" ou "último argumento" a proposta de depositar o valor em cédulas ao invés de simplesmente transferir meros dígitos eletrônicos ao banco. Explica-se. Em razão da moeda escritural não ser obrigatória e do banco não possuir cédulas ("dinheiro de verdade") suficientes, ele faz de tudo para que as pessoas não recebam as cédulas dele, mas que as mesmas lhes entreguem as que possuem. E, detalhe, quanto mais cédulas o banco possuir, mais dinheiro escritural ele pode emitir. Se algumas pessoas passarem a reter consigo (não com os bancos) as cédulas existentes, forçando grande parcela das pessoas a não receberem seus pagamentos mais em cédulas, mas tão somente créditos eletrônicos, os bancos entrarão em desespero para poderem ter as cédulas para entregar aos clientes que exigirem.

De modo semelhante, uma ação escritural ("book shares"), prevista nos artigos 34 e 35 da Lei nº 6.404/1976 (http://www.planalto.gov.br/ccivil_03/leis/L6404compilada.htm), não é representada por uma cautela ou um certificado, de forma que não há movimentação física de documentos na sua negociação, sendo os valores creditados ou debitados diretamente na conta do acionista. Tal desmaterialização na difusão da propriedade de ações, facilita a circulação proporcionada pela transferência mediante ordem à instituição financeira e

mero registro contábil, com a eliminação do custo do certificado (materialização).

Igualmente o serviço de cobrança escritural dos bancos dispensa a emissão de duplicatas, carimbos, assinaturas, borderôs e outros papéis, mantendo as características dos títulos da no sistema do banco.

Ainda mais, o artigo 889, § 3º, do Código Civil de 2002 (http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm), autoriza a emissão de títulos criados em computador ou meio técnico equivalente, estabelecendo que: "O título poderá ser emitido a partir dos caracteres criados em computador ou meio técnico equivalente e que constem da escrituração do emitente, observados os requisitos mínimos previstos neste artigo".

A Lei nº 5.474/1968 (http://www.planalto.gov.br/ccivil_03/leis/L5474.htm), artigo 15-A (que faz referência ao atual CPC/2015, artigo 771), a Lei nº 9.492/1997 (http://www.planalto.gov.br/ccivil_03/leis/L9492.htm), parágrafo único do artigo 8º, combinada com o CPC - Código de Processo Civil (Lei nº 13.105/2015 - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm), artigos 193 e 1.053 e a Lei n.º 11.419/2006 (http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm), que instituiu o processo judicial eletrônico, autorizam a execução de duplicatas eletrônicas, com apoio em apresentação do boleto, quando, no processo, vierem apresentadas as notas fiscais (que atualmente também são eletrônicas), os comprovantes de entrega das mercadorias e os respectivos instrumentos de protesto por indicação. Assim, boletos de cobrança bancária e títulos virtuais suprem a ausência física do título cambial e podem constituir títulos executivos extrajudiciais.

Uma fatura ou um boleto de cobrança não passam de impressos meramente representativos das informações de débito ou de cobrança constantes no banco de dados do credor e da instituição financeira. Desse modo, pode-se destruir, perder ou extraviar esse impresso (pedaço de papel) que não afetará a divida ou sua respectiva cobrança; ou seja, não afetará em nada os dados digitais ou eletrônicos. Tanto é assim que é possível emitir

outra via do boleto e, até mesmo, efetuar o pagamento sem o boleto, apenas informando algum dado identificador do débito que quer quitar. O número serial ou código de barras de um boleto não é uma ordem bancária ou título de crédito, mas consiste apenas numa forma de identificação exclusiva da transação. De modo similar, um endereço de um site (URL) não é o próprio site, mas apenas uma forma de identificá-lo e localizá-lo. De igual modo, a moeda digital criptográfica bitcoin não se resume em um código alfanumérico (letras e números), mas consiste nos dados digitais constantes da *Blockchain* (banco de dados) e que são identificados e localizados através desse serial alfanumérico.

A Lei nº 9.492/1997 (http://www.planalto.gov.br/ccivil_03/leis/L9492.htm), que define competência e regulamenta os serviços concernentes ao protesto de títulos, em seu artigo 8º, dispõe que podem ser recepcionados pelos tabeliões, as indicações a protesto das duplicatas, por meio magnético ou de gravação eletrônica de dados.

A Lei nº 11.076/2004 (http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/L11076.htm), ao criar títulos de crédito ligados ao agronegócio, permitiu sua emissão na forma cartular (em papel), escritural ou eletrônica.

Por outras palavras, a Lei nº 11.076/2004 equipara títulos de crédito eletrônico a escritural.

Em suma, o dinheiro fictício, imaterial, virtual, digital ou eletrônico já existe há décadas e todos utilizam dele diariamente sem perceber. E, da mesma forma que aconteceu com o lastro em ouro, esses dígitos bancários tendem a não ter mais nenhum lastro em cédulas (moeda física). É o processo de desmaterialização.

> "O fenômeno da desmaterialização dos títulos de crédito iniciou-se na França, através de um sistema que foi implantado em 1967 e aperfeiçoado em 1973, com a introdução do Lettre de Change-relevé. Logo após foi adotado pela Alemanha, no chamado LastschriHuerrehr, e por vários outros países, tais como Itália, Estados Unidos e Argentina."

(A duplicata virtual e a desmaterialização dos títulos de crédito, Débora Cavalcanti de Falconeri, https://jus.com.br/artigos/7266/a-duplicata-virtual-e-a-desmaterializacao-dos-titulos-de-credito).

A **desmaterialização do dinheiro** não é algo novo e vem avançando e ganhando força e velocidade com o passar dos anos. Países como Noruega, Dinamarca, Suécia e Holanda possuem projetos em andamento de eliminarem as cédulas ou papel-moeda.

- http://economia.estadao.com.br/noticias/geral,o-fim-do-dinheiro,10000059290;
- http://www.tecmundo.com.br/dinheiro/74882-dinheiro-papel-fim-segundo-paypal.htm;
- http://economia.uol.com.br/noticias/reuters/2016/01/20/dinheiro-em-papel-deixara-de-existir-em-uma-decada-diz-banco-alemao.htm;
- https://www.linkedin.com/pulse/meios-eletr%C3%B4nicos-de-pagamento-do-papel-aos-el%C3%A9trons-zainer;
- http://www.opovo.com.br/app/maisnoticias/mundo/dw/2015/05/19/noticiasdw,3440180/economistas-europeus-defendem-fim-do-dinheiro-em-especie.shtml;
- https://pratapura.com/2016/05/30/a-caminho-do-fim-do-dinheiro-fisico-ao-menos-assim-querem-os-banqueiros/;
- http://www.techtudo.com.br/artigos/noticia/2011/09/na-africa-paga-se-de-tudo-com-o-celular.html;
- https://www.bitcoinbrasil.com.br/projeto-de-lei-propoe-o-fim-da-circulacao-e-uso-de-dinheiro-em-especie-no-brasil;
- http://www2.camara.leg.br/camaranoticias/noticias/ECONOMIA/489566-PROJETO-PRETENDE-ACABAR-COM-USO-DO-DINHEIRO-EM-ESPECIE.html;
- http://viagem.estadao.com.br/noticias/geral,o-fim-do-dinheiro-e-o-aumento-do-iof,10000050008;
- http://exame.abril.com.br/economia/deutsche-bank-preve-fim-do-papel-moeda-em-10-anos/;
- http://exame.abril.com.br/revista-exame/quem-quer-dinheiro-2/;
- http://www1.folha.uol.com.br/mercado/2016/12/1844539-os-paises-onde-o-dinheiro-vivo-esta-prestes-a-ser-extinto.shtml;

- https://economia.terra.com.br/os-paises-onde-o-dinheiro-vivo-esta-prestes-a-ser-extinto,02796109b9cbf11840e08a9f2967e41ekpes6sst.html;
- http://www.forbes.com.br/negocios/2016/07/moeda-fisica-tem-data-para-acabar-diz-diretor-geral-do-paypal-na-al/;
- http://www.smartpaymentsnews.com/desmaterializacao-dos-pagamentos-e-o-caminho/;
- http://www.bbc.com/portuguese/noticias/2015/05/150518_dinamarca_fim_cedulas_moedas_dinheiro_rb;
- http://www.bbc.com/portuguese/vert-cap-38131182.

No Brasil essa questão já foi levantada em projeto de lei (PL 48/2015 apensado ao PL 4.586/2016).

- http://www2.camara.leg.br/camaranoticias/noticias/ECONOMIA/489566-PROJETO-PRETENDE-ACABAR-COM-USO-DO-DINHEIRO-EM-ESPECIE.html;
- http://www.camara.leg.br/buscaProposicoesWeb/pesquisaSimplificada.

CONTROLE ESTATAL DA MOEDA

Com o tempo, da mesma forma ocorrida com as moedas, os governos passaram a conduzir a emissão de cédulas, controlando as falsificações e garantindo o poder de pagamento.

Atualmente quase todos os países possuem seus bancos centrais, encarregados das emissões de suas cédulas e moedas próprias, que por razões de emissão, controle e outros fatores, possuem valores e estampas diferentes.

Portanto, nos dias de hoje, predominam regimes de papel-moeda não conversível, com os governos detendo o monopólio ou o controle sobre sua emissão.

A emissão estatal da moeda tende a centralizar a vida social e instituir um sistema de direção da política monetária. O monopólio monetário amplia a possibilidade de uma decisão no sentido da valorização ou desvalorização num âmbito nacional. A intervenção dos governos na fabricação (emissão ou cunhagem) de moeda justifica-se pela necessidade de evitar a diversidade de moedas e a sua adulteração; bem como sua padronização. Porém é o próprio Estado que viola frequentemente as leis monetárias. A livre emissão particular aconteceu em alguns povos onde as entidades senhoriais locais emitiam moeda própria, o que trouxe consequências de certo relevo às relações entre os homens, designadamente a dispersão dos poderes de decisão política e de intervenção econômica.

A maior parte dos países possui um padrão monetário específico (um dinheiro reconhecido oficialmente). Algumas exceções são o euro (usado por diversos países europeus) e o dólar (utilizado em todo mundo); bem como metais preciosos (ouro e prata), joias (diamantes, por exemplo) e outros bens valiosos (petróleo, água potável, etc.) mantêm muitas das características essenciais de dinheiro.

As cédulas, geralmente, se apresentam no formato retangular e no sentido horizontal, observando-se, no entanto, grande variedade de tamanhos. Existem, ainda, cédulas quadradas e até as que têm suas inscrições no

sentido vertical. Elas retratam a cultura do país emissor e nelas podem-se observar motivos característicos muito interessantes como paisagens, tipos humanos, fauna e flora, monumentos de arquitetura antiga e contemporânea, líderes políticos, cenas históricas etc. As cédulas apresentam, ainda, inscrições, geralmente na língua oficial do país; embora em muitas delas se encontre, também, as mesmas inscrições em outros idiomas. Essas inscrições, quase sempre em latim ou inglês, visam dar à peça leitura para maior número de pessoas.

O conjunto de cédulas e moedas utilizadas por um país forma o seu sistema monetário. Este sistema, regulado por meio de legislação própria, é organizado a partir de um valor que lhe serve de base e que é sua unidade monetária.

SISTEMA FINANCEIRO

O **SFN (Sistema Financeiro Nacional)** é um conjunto de instituições, órgãos e afins que controlam, fiscalizam e executam as operações necessárias à circulação da moeda e do crédito na economia do país. O SFN pode ser divido em entidades normativas, supervisoras e operacionais (http://www.bcb.gov.br/?SFNCOMP).

As entidades normativas são responsáveis pela definição das políticas e diretrizes gerais do sistema financeiro, sem função executiva. Em geral, são entidades colegiadas, com atribuições específicas e utilizam-se de estruturas técnicas de apoio para a tomada das decisões. Atualmente, no Brasil funcionam como entidades normativas o Conselho Monetário Nacional (CMN), o Conselho Nacional de Seguros Privados (CNSP) e o Conselho Nacional de Previdência Complementar (CNPC).

- http://www.bcb.gov.br/pre/composicao/cmn.asp;
- http://www.bcb.gov.br/Pre/CMN/Entenda%20o%20CMN.asp;
- http://www.bcb.gov.br/pre/composicao/cnsp.asp;
- http://www.bcb.gov.br/Pre/composicao/cgpc.asp.

As entidades supervisoras, por outro lado, assumem diversas funções executivas, como a fiscalização das instituições sob sua responsabilidade; assim como funções normativas, com o intuito de regulamentar as decisões tomadas pelas entidades normativas ou atribuições outorgadas a elas diretamente pela Lei. O Banco Central do Brasil (Bacen ou BCB), a Comissão de Valores Mobiliários (CVM), a Superintendência de Seguros Privados (SUSEP) e a Superintendência Nacional de Previdência Complementar (PREVIC) são as entidades supervisoras do nosso Sistema Financeiro.

- http://www.bcb.gov.br/;
- http://www.cvm.gov.br/;
- http://www.susep.gov.br/;
- http://www.previc.gov.br/.

O Bacen (Banco Central do Brasil) foi criado em 1964 com a promulgação da Lei da Reforma Bancária (Lei nº 4.595/1964), mesma Lei que instituiu o Conselho Monetário Nacional.

"É uma autarquia federal que tem como principal missão institucional assegurar a estabilidade do poder de compra da moeda nacional e um sistema financeiro sólido e eficiente.

Entre as competências do BCB destacam-se:

. Assegurar a estabilidade do poder de compra da moeda nacional e a solidez do Sistema Financeiro Nacional;

. Executar a política monetária mediante utilização de títulos do Tesouro Nacional;

. Fixar a taxa de referência para as operações compromissadas de um dia, conhecida como taxa SELIC;

. Controlar as operações de crédito das instituições que compõem o Sistema Financeiro Nacional;

. Formular, executar e acompanhar a política cambial e de relações financeiras com o exterior;

. Fiscalizar as instituições financeiras e as clearings (câmaras de compensação);

. Emitir papel-moeda (a partir da Constituição de 1988, a emissão de moeda ficou a cargo exclusivo do BCB);

. Executar os serviços do meio circulante para atender à demanda de dinheiro necessária às atividades econômicas;

. Manter o nível de preços (inflação) sob controle;

. Manter sob controle a expansão da moeda e do crédito e a taxa de juros;

. Operar no mercado aberto, de recolhimento compulsório e de redesconto;

. Executar o sistema de metas para a inflação;

. Divulgar as decisões do Conselho Monetário Nacional;

. Manter ativos de ouro e de moedas estrangeiras para atuação nos mercados de câmbio;

. Administrar as reservas internacionais brasileiras;

. Zelar pela liquidez e solvência das instituições financeiras nacionais;

. Conceder autorização para o funcionamento das instituições financeiras.

O presidente do BCB e os seus diretores são nomeados pelo Presidente da República após a aprovação prévia do Senado Federal, que é feita por uma arguição pública e posterior votação secreta.

Sua sede é em Brasília e possui representações regionais em Belém, Belo Horizonte, Curitiba, Fortaleza, Porto Alegre, Recife, Rio de Janeiro, Salvador e São Paulo." (Mercado de Valores Mobiliários Brasileiro, CVM - Comissão de Valores Mobiliários, 2014, 3ª edição, p. 41/42; *in* http://www.portaldoinvestidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/LivroTOP-CVM.pdf).

O CMN - Conselho Monetário Nacional:

"É o órgão deliberativo máximo do Sistema Financeiro Nacional. Foi criado pela Lei 4595/64, conhecida como a Lei da Reforma Bancária, em substituição à extinta Superintendência da Moeda e do crédito, em uma década em que o sistema financeiro passou por profundas mudanças estruturais e regulamentares.

O CMN foi criado com a finalidade de formular a política da moeda e do crédito, para promover o progresso econômico e social do país. A política do CMN tem como principais objetivos:

. adaptar o volume dos meios de pagamento às reais necessidades da economia;

. regular o valor interno e externo da moeda e o equilíbrio do balanço de pagamentos;

. orientar a aplicação dos recursos das instituições financeiras;

. propiciar o aperfeiçoamento das instituições e dos instrumentos financeiros;

. zelar pela liquidez e solvência das instituições financeiras;

. coordenar as políticas monetária, creditícia, orçamentária e da dívida pública interna e externa.

Atualmente, o CMN é composto por três membros: Ministro da Fazenda (Presidente), Ministro do Planejamento, Orçamento e Gestão e Presidente do Banco Central.

Em conjunto com o CMN funciona a Comissão Técnica da Moeda e do Crédito (Comoc), que tem como atribuições o assessoramento técnico na formulação da política da moeda e do crédito do País. As matérias aprovadas são regulamentadas por meio de Resoluções, normativos de caráter público, sempre divulgadas no Diário Oficial da União e na página de normativos do Banco Central do Brasil. Também funcionam junto ao CMN diversas comissões consultivas que representam os principais setores do mercado." (Mercado de Valores Mobiliários Brasileiro, CVM - Comissão de Valores Mobiliários, 2014, 3ª edição, p. 39; disponível em http://www.portaldoinvestidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/LivroTOP-CVM.pdf).

Além destas, há as entidades operadoras, que são todas as demais instituições financeiras, monetárias ou não, oficiais ou não; como, também, demais instituições auxiliares, responsáveis, entre outras atribuições, pelas intermediações de recursos entre poupadores e tomadores ou pela prestação de serviços.

Saiba mais sobre o **Sistema de Pagamentos Brasileiro** em:

- http://www.bcb.gov.br/?spb;
- http://www.bcb.gov.br/pt-br/#!/n/SPBASPECTOS;
- http://www.bcb.gov.br/htms/novaPaginaSPB/VisaoGeralDoSPB.asp;
- http://www.tudosobreconcursos.com/materiais/conhecimentos-bancarios/estrutura-do-sistema-financeiro-nacional.

LASTRO EM OURO

O **padrão-ouro** é um sistema monetário no qual a unidade econômica padrão é uma quantidade determinada de ouro. Sob este tipo de sistema, o dinheiro é “endossado por ouro” e os fundos nacionais e outras formas de dinheiro (depósitos bancários e notas) podem ser livremente convertidas em ouro a um preço fixo.

- https://pt.wikipedia.org/wiki/Padrão-ouro.

J. P. Morgan memoravelmente disse ao Congresso americano em 1913: "apenas ouro é dinheiro, nada mais".

As reservas cambiais refletem o montante de moeda estrangeira e de ouro acumulados pelo país; originam-se de superávites (excedente, balança comercial favorável ou lucro) nos balanços de pagamentos e destinam-se a cobrir eventuais déficites (falta ou saldo negativo) das contas internacionais. Assim, um volume maior de reservas serve como um seguro ou uma blindagem contra crises de balanço de pagamentos e, também, como forma de tentar controlar o preço da moeda e a inflação.

O resultado do balanço de pagamentos, que reflete o resultado monetário das transações de bens e serviços realizadas pelos nacionais com o exterior, assim como o fluxo de capitais entre o país e o exterior (sejam empréstimos, financiamentos, aplicações em mercado financeiro, etc.) demonstra se houve acúmulo, ou perda, de moeda estrangeira no período, refletindo, portanto, a variação das reservas cambiais.

Desse modo, entende-se por *superávit* comercial quando as cifras referentes à exportação são maiores do que as cifras relativas à importação de bens e serviços. O *superávit* da balança comercial é um fator positivo na economia de um país, já que mostra que o mesmo está exportando (vendendo) mais bens e serviços do que está importando (comprando). Já quando o país importa mais do que exporta, surge o que é chamado de *déficit* comercial. Existe ainda uma terceira situação chamada de equilíbrio comercial; neste caso, o montante referente às exportações é igual ao

montante das importações. O balanço entre esses valores, de exportação e importação, é denominado de balança comercial.

Tal como as reservas cambiais, os estoques reguladores governamentais (de combustíveis, medicamentos, alimentos, sementes, etc.) objetivam estabilizar os preços praticados (limitar a oscilação dos preços ou combater a inflação), reequilibrando aqueles mercados que estejam sofrendo pressão inflacionária de oferta; bem como são reservas para uso em situações de calamidades, desastres, emergências, escassez, socorros humanitários, guerras, etc.

O ***Fort Knox*** é um posto do Exército dos Estados Unidos no estado de Kentucky, entre as cidades de Louisville e *Elizabeth Town*. Ali encontra-se o famosíssimo Depósito de Ouro dos Estados Unidos (*United States Bullion Depository*), pelo qual o lugar é realmente conhecido como depósito de grande parte do ouro estocado pelo governo do país. O depósito de ouro conquistou popularidade mundial na década de 1960, graças ao filme "007 - Contra Goldfinger", em que o depósito e seus cofres são alvo de um plano de destruição para desestabilizar a economia mundial.

- http://exame.abril.com.br/economia/noticias/os-18-paises-com-mais-ouro-guardado-no-cofre;
- http://top10mais.org/top-10-paises-com-maiores-reservas-de-ouro-no-mundo/;
- http://www.arlloufill.com/pages/os-maiores-depositos-de-ouro;
- http://mundo-nipo.com/economia/16/06/2015/as-10-maiores-reservas-de-ouro-do-mundo-japao-esta-incluido/;
- http://g1.globo.com/economia/noticia/2015/08/venezuela-e-1o-pais-da-america-latina-em-reservas-de-ouro-brasil-esta-em-3o.html;
- http://portugalsempassaporte.com/economia/1053-portugal-está-entre-os-países-com-maiores-reservas-de-ouro-do-mundo.html;
- http://www.jn.pt/economia/interior/portugal-entre-os-paises-com-maior-reserva-de-ouro-2434015.html;
- https://sites.google.com/site/papapaipiopadrepopeblasfemia/padres-tem-a-maior-reserva-de-ouro-do-mundo;
- https://insider.pro/pt/article/15248/.

O **lastro metálico** integral mostrou-se desnecessário quando foi constatado que a reconversão da moeda-papel em metais preciosos não era solicitada por todos os seus detentores ao mesmo tempo e ainda quando uns a solicitavam, outros pediam novas emissões. A derradeira moeda importante a manter parcialmente o padrão-ouro foi o dólar norte-americano (até 1971).

Em 1971, diante da crescente demanda por ouro, o presidente americano, Richard Nixon, abandonou a conversibilidade do dólar por ouro (*Nixon Shock*), pondo fim ao sistema de *Bretton Woods*. Com isso, o dólar estadunidense e todas as demais moedas do mundo passaram a não ter mais lastro em metal precioso. Isso também fez com que o dólar se tornasse uma moeda fiduciária. Depois de 1973, o lastro do dinheiro do mundo (reserva dos bancos centrais dos países) passou a ser o dólar.

O acordo de Bretton Woods foi uma série de disposições acertadas por cerca de 45 países aliados em julho de 1944, na mesma cidade norte-americana que deu nome ao acordo, no estado de *New Hampshire*, no hotel *Mount Washington*. O objetivo de tal concerto (acordo) de nações foi definir os parâmetros que iriam reger a economia mundial após a Segunda Guerra Mundial. O sistema financeiro que surgiu foi amplamente favorável aos Estados Unidos. Por tal convenção, o dólar se tornou uma moeda mundial e fator de referência para as moedas dos outros 44 países signatários de Bretton Woods; ou seja, todas as outras moedas passaram a estar ligadas ao dólar. Como pseudo fundamento de sustento para essa força mundial, o dólar estaria lastreado ao ouro; assim, qualquer um no mundo poderia transformar seus dólares no seu equivalente em ouro. Evidentemente tal afirmativa era inverídica pelo fato de ser totalmente impossível, não passando de mera propaganda de consolidação do dólar em escala mundial e, assim, da supremacia dos Estados Unidos.

Portanto, após a extinção do padrão-ouro, os governos puderam imprimir tanto dinheiro quanto o desejado, já que, para isto, não era necessário ter ouro suficiente para endossá-lo. O dinheiro tornou-se uma moeda corrente e há uma enorme diferença entre dinheiro e moeda corrente.

As moedas tradicionais costumavam ser lastreadas em metais preciosos, como o ouro, e representavam uma fração da riqueza armazenada pelo país emissor (lastro); mas, atualmente, as moedas são lastreadas nas dívidas emitidas pelos países. Portanto, seu valor decorre da confiança de que o governo emissor vai pagar suas dívidas.

A **moeda fiduciária (*fiat money*)** é a moeda que não é apoiada por reservas de alguma mercadoria valiosa. É o dinheiro que é intrinsecamente inútil (exemplo, simples pedaço de papel sem remissão a nenhum bem de valor), mas que é usado como um meio de troca. Pelo fato de não ser apoiada por nada, seu valor é baseado na sua capacidade para ser distribuída ou ser aceita pelas pessoas. O valor dessa moeda é, portanto, definido pela sua confiabilidade, reputação, aceitação, estabilidade e pela correlação oferta - procura.

Saiba mais sobre moeda fiduciária no verbete "Moeda FIAT" no Glossário.

Retomamos o assunto “ouro” nos capítulos: VALOR DO OURO, INVESTIMENTOS EM OURO e TRIBUTAÇÃO SOBRE OURO, AÇÕES E RENDA VARIÁVEL.

DA MOEDA MUNDIAL CONTEMPORÂNEA

O chamado lastro de ouro, como valor de referência para as moedas nacionais, só foi adotado em 1821 pela Inglaterra; antes disso, a prata era o metal monetário por excelência. Recorde a história do thaler e da “lei” de Gresham, que reza que a moeda ruim retira a moeda boa do mercado.

Com o início da Primeira Guerra Mundial, em 1914, o padrão-ouro caiu, refletindo os grandes desequilíbrios causados por ele nas economias ao redor do mundo. Começou, então, um difícil período de transição. As discussões sobre o novo modelo começaram ainda durante a Segunda Guerra Mundial, e consolidou-se, nesse período, a visão de que a melhor estratégia seria algo similar à adotada durante o padrão-ouro, com uma taxa de câmbio fixa, baseada em uma moeda forte. Ainda em meio ao conflito mundial, 730 delegados de 44 países se reuniram em julho de 1944 em Bretton Woods, nos Estados Unidos, para definir uma nova ordem econômica mundial, que ajudaria a restabelecer o capitalismo mundial. Os líderes partiram de duas propostas iniciais, uma norte-americana, do oficial do Tesouro dos Estados Unidos Harry White, e uma britânica, do conhecido economista John Keynes. A proposta de White, que prevaleceu, mantinha a vinculação do câmbio com o ouro, mas o dólar seria a única moeda com valor diretamente fixado em ouro (US$ 35 por onça de ouro). A partir daí todos os outros países teriam um valor fixo para a sua moeda frente à divisa norte-americana.

> "O primeiro Sistema Monetário Internacional, o padrão ouro (clássico), vigorou de 1870 a 1914. Nesse período, a Inglaterra era a potência econômica líder e as outras nações alinhavam-se (ou tinham que se alinhar) ás diretrizes da política inglesa para atingir sucesso econômico. Por sua importância no comércio internacional e pelo desenvolvimento acelerado de suas instituições financeiras, a Inglaterra impunha ao mundo o padrão ouro e Londres torna-se o centro financeiro do mundo.
>
> O padrão ouro clássico como qualquer Sistema Monetário Internacional tem como objetivo básico o equilíbrio interno e externo da economia. Neste padrão, a responsabilidade para atingir tal equilíbrio era dada ao Banco Central, que deveria preservar a paridade oficial entre as moedas e o ouro. Para manter esse preço, o Banco Central

> precisava de um estoque de moeda suficiente em reservas de ouro. O equilíbrio externo caracterizava-se como uma situação em que o Banco Central não estava ganhando ou perdendo ouro pois os superávits ou déficits do balanço de pagamento tinham que ser financiados por embarque de ouro entre os bancos centrais." (O SISTEMA MONETÁRIO INTERNACIONAL: uma interpretação a partir do conceito de hegemonia mundial, Pedro Lopes Marinho; disponível em *in* http://www.uesc.br/dcec/pedrolopes/artigo_prof_pedro_lopes_sistema_monetario.pdf).

A constância do valor da moeda e da economia que a rege é o fator mais importante para que ela seja considerada forte. Desse modo, uma economia estável e uma moeda sem fortes oscilações, gera credibilidade. Por outras palavras, uma moeda que se mantém com o mesmo preço e apresenta raras e baixas variações transmite segurança para os investidores. Assim, por exemplo, o Yene Chinês é uma moeda que oscila bastante, apesar do crescimento brutal da economia chinesa; já a Libra, apesar de ser muito valiosa, possui baixa circulação.

O dólar americano (US$) é uma das moedas mais importantes no mundo. Atualmente, sua hegemonia é incontestável, já que é usada na adoção de reservas internacionais por Bancos Centrais de inúmeros países e como referência em qualquer negócio em nível global. Entretanto, nem sempre foi assim. Na verdade, a hegemonia da moeda norte-americana é relativamente recente, pois só se deu após o fim da Segunda Guerra Mundial.

Durante todo o século XIX, a moeda dominante a nível mundial foi a britânica (inglesa) libra esterlina.

Em suma, o acordo de 1944 em Bretton Woods solidificou o dólar como a divisa de reserva predominante no mundo, substituindo a libra britânica (moeda da Inglaterra).

Desde 1945, o mundo segue a lógica estabelecida pelos acordos de *Bretton Woods*, a cidade de *Massachusetts* na qual nações aliadas, capitaneadas pelos Estados Unidos, reuniram-se para definir as bases do funcionamento capitalista no pós-guerra. Buscavam regras que lhes

propiciassem estabilidade monetária (evitando crises como a de 1929) e que ao mesmo tempo permitissem a liberdade necessária para que seus capitais se espalhassem pelo mundo.

Naquele momento, foram criados o Banco Mundial e o Fundo Monetário internacional, para financiar a reconstrução das economias destroçadas pela guerra e combater crises cambiais. Principalmente, estabeleceu-se ali que o dólar passaria a ser a moeda de troca internacional.

> "A delegação britânica – chefiada por Lord Keynes – e virtualmente todos os demais países participantes, exceto os EUA, prefeririam criam uma nova moeda multilateral através do nascente Fundo Monetário Internacional (FMI) como principal fonte de liquidez global. Mas isso poria abaixo as ambições norte-americanas, que queriam uma ordem monetária centrada no dólar. Apesar de praticamente todos os participantes preferirem a opção multilateral, o poder relativo vastamente superior dos EUA garantiu que, no final, sua preferência predominasse. Assim, sob o padrão ouro de troca de Bretton Woods, o dólar foi ligado ao ouro e as demais moedas foram ligadas ao dólar, gerando a forma principal de liquidez internacional." (http://redecastorphoto.blogspot.com.br/2014/08/cresce-o-petroyuan-e-lenta-erosao-da.html).

Com a formidável cooperação dos bancos centrais e dos bancos comerciais internacionais, o dólar foi aceito, e continua sendo aceito, como se ouro fosse. É o sistema monetário fiduciário (*fiat monetary system*) através do padrão dólar fiduciário (*fiat dollar*).

Desde então todo comércio exterior é realizado somente em dólar; ou seja, os países negociantes não negociam uma conversão direta de suas respectivas moedas, mas primeiramente convertem em dólar e depois em suas respectivas moedas somente para uso interno. Portanto, quando se fala em balança comercial, utilizasse o dólar como medida.

De igual forma, quando se pretende enviar dinheiro para o exterior, o valor é antes convertido em dólar e depois convertido na moeda local do destinatário se pretender usar no local.

Um dos problemas do sistema de *Bretton Woods* foi a dependência da economia dos Estados Unidos. Após a Segunda Guerra Mundial, houve uma escassez grande de dólares no mundo e os países precisavam dele para adquirirem os principais produtos que gostariam de importar, que eram norte-americanos. Mas, para conseguirem dólares eles precisavam gerar

receitas com exportações para os Estados Unidos. Com a recuperação mundial, os países começam a ter *superávits* crescentes com os Estados Unidos, o que significa uma inundação de dólares no mundo. Isso acaba fazendo com que a moeda perca seu poder de se tornar um meio de pagamento internacional confiável.

No final da década de 1960, a França passou a exigir dos Estados Unidos o ouro dos seus dólares. Como os Estados Unidos tinham imprimido muito mais dólares do que sua quantidade de lastro em ouro permitia, em 15/08/1971, Nixon oficialmente acabou com o lastro em ouro para escapar de pagar os credores.

> "O *status* de 'moeda de reserva internacional' do dólar americano após a Segunda Guerra Mundial era baseado no poder da economia dos EUA, mas era também baseado no fato de que o governo americano havia prometido restituir sua moeda em ouro a um valor de US$35 a onça. O ouro era a âncora do dólar, que era a moeda de reserva mundial. Os bancos centrais estrangeiros, em vez de pedir a restituição de dólares em ouro, podiam também utilizar estes dólares para comprar títulos do Tesouro americano e, com isso, auferir receitas.
>
> Qualquer governo estrangeiro podia pedir para o seu banco central criar dinheiro do nada (sua moeda nacional) e então utilizar este dinheiro para comprar dólares, os quais eram imediatamente utilizados para comprar títulos do Tesouro americano. No entanto, por causa do acordo de Bretton Woods, havia limites na capacidade de um país fazer isso. Estes limites tinham a ver com a taxa de câmbio entre a moeda do país e o dólar americano. A taxa de câmbio estava relativamente fixada. As moedas de cada país tinham um valor atrelado dólar (e este valor tinha de ser mantido pelo governo deste país), e o dólar tinha um valor fixo em ouro.
>
> Desta forma, uma inflação monetária em massa não podia ser feita pelos países membros do Fundo Monetário Internacional (o qual também havia sido criado na conferência de Bretton Woods). Afinal, quem inflacionasse, teria dificuldades de sustentar o valor de sua moeda em relação ao dólar. Isto manteve a taxa de inflação de preços, bem como a de inflação monetária, relativamente estável de 1946 a 1971. Era contra

as regras do FMI um país tentar desvalorizar sua moeda com o intuito de estimular suas indústrias exportadoras.

No entanto, um país estava livre para inflacionar: os EUA. E ele fez isso livremente. Os dólares que os EUA criavam iam parar nas reservas dos outros países, os quais podiam então inflacionar suas moedas em cima destes dólares. Na década de 1960, alguns países — e a França, com mais intensidade — passaram a demandar a restituição destes dólares em ouro. Isso gerou uma enorme pressão sobre o governo americano, que havia criado muito mais dólares do que a quantidade de ouro em suas reservas. Para evitar a perda total de seu estoque de ouro, o governo americano simplesmente tomou a decisão unilateral de abolir este regime de conversão em agosto 1971. Naquela data, todo o sistema de Bretton Woods foi para o lixo. E nunca mais voltou." (http://www.mises.org.br/Article.aspx?id=1673).

"A âncora do ouro foi feita para conter uma produção excessiva da massa monetária nos Estados Unidos. Para obter esse objetivo, um mecanismo de controle foi instalado: quando um país estrangeiro tivesse um superávit comercial, ele poderia usar o excesso de dólares para trocar por ouro do Tesouro americano. Com uma paridade fixa entre a massa de dólares em circulação e volume de ouro no Tesouro americano, esse mecanismo imporia um limite à criação excessiva de massa monetária em forma de dólares. O sistema como evoluiu no período do pós-guerra aliviou os Estados Unidos de restrições de câmbio. Entretanto, não levou muito tempo para que os Estados Unidos começassem a abusar dessa vantagem. A melhoria do estado de bem-estar na esfera doméstica juntamente com o recrutamento militar na Guerra Fria e na guerra de Vietnã foi alimentada por um aumento maciço da massa monetária, fazendo com que os EUA já não pudessem cumprir o acordo de fazer moedas estrangeiras conversíveis em ouro. A escassez de dólares das décadas de 40 e 50 se transformou em uma avalanche de dólares e a inflação mundial começou sua ascensão.

No final dos anos 60, o sistema monetário internacional se transformou em uma fonte de criação de liquidez global, que obrigou outras nações a importarem inflação como contraposição a exportações dos Estados Unidos por causa da expansão da massa monetária americana. Em 1971, com o chamado "Acordo Smithsoniano", uma última tentativa foi feita

> para salvar o antigo sistema, quando os EUA renunciaram a obrigação de trocar dólares por ouro e desvalorizavam sua moeda em relação a uma série de outras moedas. Logo ficou claro que aquele sistema não era mais viável. Em 1973, com a adoção da nova regra de que cada país poderia escolher seu arranjo cambial próprio, o antigo sistema de Bretton Woods chegou ao fim." (http://ordemlivre.org/posts/sera-o-fim-da-hegemonia-do-dolar--4).

Diante disso, o Tesouro dos Estados Unidos pode imprimir notas de dólar, aceitas como moeda de troca em todo o mundo, sem ter que garantir seu valor.

Esse regime de câmbio fixo vinculado ao dólar que, por sua vez, era ligado ao ouro, durou até o início da década de 1970, quando alguns países como Canadá, Inglaterra e Japão começam uma onda de fuga dessa paridade.

Com o novo sistema monetário (estabelecido de fato em 1971), todas as moedas do mundo passavam a um sistema de flutuação livre e respaldavam sua moeda com a capacidade de gerar atividade econômica que tinham em sua jurisdição e a qualidade de seu balanço. Os bancos centrais mais importantes do mundo (o *Federal Reserve* - Fed [o Banco Central dos Estados Unidos], o Banco Central Europeu – BCE, o *Bank of England* [Banco da Inglaterra] e o Banco Central da China) possuem o ouro como componente chave de suas reservas de divisas internacionais para criar confiança em suas moedas.

Para se manter como moeda mundial, os Estados Unidos, em 1970, conseguiram que a OPEP (Organização dos Países Exportadores de Petróleo) cotasse o petróleo exclusivamente em dólares norte-americanos em todas as transações do mundo; daí a expressão Petrodollar.

- http://www.opec.org/opec_web/en/.

Com o Choque do Petróleo, em 1973, o sistema de Bretton Woods é deixado oficialmente de lado e passa a vigorar o atual regime de câmbio flutuante. A partir daí o mercado, a intervenção do governo e os interesses diante de suas contas externas, são quem determinam a cotação das moedas

frente ao dólar. Desse modo, se o país está com *déficit* comercial, a tendência é que ele adote políticas mais agressivas para desvalorizar sua moeda, para exportar mais e corrigir esse *déficit*. Isso deu origem à uma disputa entre os países para corrigirem seus desequilíbrios comerciais e no balanço de pagamentos por meio da desvalorização da moeda, o que era exatamente o que se procurava evitar antes.

Conceitualmente, a balança comercial nada mais é do que a diferença entre as exportações e as importações de um determinado país. Por exportações, entendemos todo bem que o país vende para o resto do mundo, enquanto que importações são todos os bens que o país compra do resto do mundo. Dizemos que a balança comercial de um determinado país está favorável, quando este exporta (vende para outros países) mais do que importa (compra de outros países). Do contrário, dizemos que a balança comercial é negativa ou desfavorável. Em síntese, quando a balança comercial é negativa temos um *déficit*, mas quando ela é positiva tempos um *superávit*. A balança comercial favorável apresenta vantagens para um país, pois atrai moeda estrangeira, além de gerar empregos dentro do país exportador.

> "O que absolutamente quase ninguém diz é que, para os habitantes de um país, o único benefício trazido pelas exportações é justamente as importações; a única função de se exportar é que, com isso, pode-se importar. [...]. Qual seria o sentido de exportar sem importar? Do ponto de vista do cidadão brasileiro, as exportações de soja, laranja e aço do país só lhe são boas porque trazem dólares que lhe permitem importar iPads, notebooks, livros, carros e várias outras coisas. Fora isso, as exportações não lhe são nada vantajosas. Ao contrário até: quanto mais um país exporta, menor será a oferta desses bens exportados no mercado nacional. Quanto maior a exportação de soja, laranja, café e aço, menor será a oferta desses produtos para os brasileiros, o que significa que seus preços no mercado interno serão maiores do que poderiam ser caso não fossem exportados. De modo geral, sempre que a balança comercial apresenta um superávit recorde, isso significa que o cidadão brasileiro foi privado de uma maior oferta de bens, tanto aqueles produzidos nacionalmente e que foram exportados, quanto aqueles produzidos no

estrangeiro e que não puderam ser importados por restrições governamentais." (http://www.mises.org.br/Article.aspx?id=1087).

Há tempos muitos países têm lutado em vão contra a hegemonia, domínio ou imperialismo do dólar norte-americano.

> "Claro, toda moeda é antes de mais nada uma questão de confiança: se você acredita que aquele papel pintado possui efetivamente poder de compra, que você poderá utilizá-lo de diferentes formas, para as mais variadas transações, ao longo do tempo, isto é, preservando o seu poder de compra, então você decide, em total liberdade, utilizar aquele papel pintado. Se você não confia, faz qualquer outra coisa, mas se desfaz desse papel pintado que não merece a sua confiança.
>
> Pois bem: o mundo demorou anos, décadas, para construir um sistema multilateral de pagamentos e um regime de trocas que facilite as transações entre os países, com o mínimo de restrições possível. O multilateralismo monetário, por imperfeito que seja -- posto que as autoridades monetárias americanas podem decidir dar um calote no mundo, deixando de honrar seus compromissos externos, com os compradores de títulos do Tesouro, por exemplo -- é o melhor sistema possível, pois permite que a mesma moeda seja usada com os mais diferentes parceiros em todas as transações que eles desejem, sem se amarrar em um instrumento único, como ocorria ainda com o bilateralismo estrito dos anos 1930, baseado em compensações diretas entre os países." (http://diplomatizzando.blogspot.com.br/2014/07/contra-hegemonia-do-dolar-uso-de-moedas.html).

Durante a Segunda Guerra Mundial, os nazistas contrataram alguns dos melhores falsificadores de moeda para produzir dólares estadunidenses e libras falsos, visando a desestabilizar e inflacionar a economia desses países.

Em novembro de 2000, Saddam Hussein (Iraque) exigiu euros pelo seu petróleo. Bastou isso para os americanos o acusarem, sem nunca terem provado, de que ele tinha armas de destruição em massa, seria aliado da Al-

Qaeda e iria cometer atrocidades. Conclusão, o Iraque foi invadido por uma coalisão militar, Saddam foi morto e a hegemonia do dólar se manteve.

Em 2001, o embaixador da Venezuela na Rússia disse que o seu país comutaria para euros todas as suas vendas de petróleo. Dentro de um ano houve uma tentativa de golpe contra Chávez, confirmadamente com a assistência da CIA - *Central Intelligence Agency* (Agência Central de Inteligência dos Estados Unidos).

No século XX, a hegemonia econômica estadunidense foi acompanhada pela preponderância do dólar estadunidense como moeda internacional. Com o surgimento da moeda comum europeia, o euro, em 2002, o dólar passou a dividir a cena mundial com ela. O advento do euro (€) fez sair de circulação tradicionais moedas europeias, como o escudo português, a peseta espanhola, a lira italiana, o franco francês e o marco alemão.

A União Europeia (https://europa.eu/european-union/index_pt) criou uma moeda (euro) para unificar todas as moedas dos países europeus. Logo de cara, o euro já valia bem mais que o dólar. E, no mercado russo o dinheiro europeu é mais frequentemente usado como um substituto para o dólar norte-americano.

A União Europeia (https://europa.eu/european-union/index_pt) tem as suas origens em 1957 e foi, pouco a pouco, durante meio século, expandindo - se por meio de decisões democráticas, nos diversos países, tomadas após consultas populares por meio de plebiscitos e votadas nos diferentes parlamentos. Foi um seríssimo trabalho de unificação e aperfeiçoamento, desde as normas jurídicas maiores, até as normas técnicas. Assim, o território da UE foi consistentemente aumentando de dimensão através da adesão de novos Estados - membros, ao mesmo tempo que aumentava a sua esfera de influência através da inclusão de novas competências políticas. O Tratado de Maastricht instituiu a União Europeia em 1993.

Em 1865, Itália, França, Suíça e Bélgica criaram a União Monetária Latina, que é considerado o protótipo do sistema euro. Entretanto, a mais famosa tentativa de universalização do sistema monetário foi a Liga

Hanseática, que existiu nos séculos XIII a XVI. Ela consistia de 70 a 170 estados em diferentes momentos. Em 1379, houve a união monetária, que previa um sistema único de cunhagem de moeda, que foi adotado nas principais cidades hanseáticas.

George Soros disse a pouco tempo que o objetivo de Putin é promover a desintegração da União Europeia. Em resposta a Rússia disse que aprecia a solidez da União Europeia (UE) e a conveniência de lidar com uma área de comércio consolidada. Moscou foi seriamente abalado quando a moeda única europeia parecia estar em risco, ao ponto de oferecer apoio financeiro ao Banco Central Europeu. Ele viu o colapso do euro como uma ameaça também para a Rússia.

O termo ***Brexit*** é a união das palavras inglesas *Britain* (Grã-Bretanha) e *Exit* (saída). Na votação feita em 24/06/2016, os britânicos decidiram abandonar a UE - União Europeia (https://europa.eu/european-union/about-eu/countries_pt). Com participação de 71,8% dos eleitores (mais de 30 milhões de votantes), 51,9% dos votos foram favoráveis à saída contra 48,1%; uma diferença de mais de 1,2 milhão de votos. As nações do Reino Unido são a Inglaterra, a Irlanda do Norte, a Escócia e o País de Gales. Para a saída do Reino Unido da União Europeia foi invocado o artigo 50 do Tratado de Lisboa, que prevê que qualquer Estado-membro da UE tem a liberdade para sair do bloco econômico de modo voluntário e unilateral. Também fica determinado que o prazo máximo para as negociações de saída é de dois anos, caso não haja uma decisão unânime que prorrogue este tempo. Outros países da UE ameaçam seguir o exemplo britânico e já tentam negociar vantagens com Bruxelas (capital de fato da UE). Simbolicamente, a saída do Reino Unido da UE alimenta uma série de forças anti-integração em todo o continente. O Reino Unido é a única potência nuclear europeia, membro permanente do Conselho de Segurança da ONU, com a França. E isso pode ser desastroso para a política de segurança europeia. Também é temida a imagem enfraquecida da UE frente a potências como EUA, China e Índia. Londres é indiscutivelmente a capital financeira da Europa, tendo os principais bancos e fundos de investimento. Existem razões históricas para que isto suceda (que já vêm desde a época do Império Britânico, ao tempo centro do comércio mundial) que vão para além do livre acesso ao mercado da UE. As consequências exatas do *Brexit* para as empresas ainda não

podem ser previstas e dependem do conteúdo e das negociações de saída e, ainda, de quais passos o governo britânico irá tomar em termos político-econômicos. Provavelmente irá prevalecer a *real politique* (política real); ou seja, a minimização, para ambos os lados, dos efeitos negativos da saída do Reino Unido da EU, procurando-se a manutenção do bloco econômico europeu ainda que nem todos façam formalmente parte da UE.

- http://www.tecmundo.com.br/bitcoin/106531-preco-bitcoin-sobe-frente-saida-reino-unido-da-uniao-europeia.htm;
- http://www.infomoney.com.br/mercados/acoes-e-indices/noticia/5180275/brexit-esta-virando-bremain-bolsa-caminha-para-seu-dia-seguido;
- http://www.dn.pt/mundo/interior/britanicos-nao-podem-esperar-sair-da-ue-e-manter-mercado-unico---theresa-may-5593559.html;
- http://www.valor.com.br/financas/4830844/cautela-domina-e-bolsas-americanas-fecham-sem-direcao-unica;
- http://www.valor.com.br/internacional/4830464/merkel-reino-unido-pode-perder-acesso-mercado-comum-apos-brexit;
- http://istoe.com.br/economista-do-banco-da-inglaterra-assume-erro-em-previsoes-sobre-brexit/.

Depois da saída da Inglaterra da União Europeia, outros países do Euro (Itália, Portugal, etc.) estudam fazer o mesmo.

- https://ipressglobal.com/depois-do-brexit-no-reino-unido-vem-ai-o-portugexit/;
- http://veja.abril.com.br/mundo/italia-sofre-com-incertezas-e-pressao-antissistema-apos-referendo/;
- https://www.knowledgeatwharton.com.br/article/o-que-o-referendo-da-italia-significa-para-europa/;
- http://www.jornaldenegocios.pt/economia/europa/uniao-europeia/detalhe/referendo_constitucional_italiano_pode_ter_maior_impacto_do_que_o_brexit;
- https://br.sputniknews.com/europa/201612067074847-italia-pode-arruinar-ue/;
- https://noticias.uol.com.br/ultimas-noticias/ansa/2016/12/05/casa-branca-nega-ligacao-entre-referendo-italiano-e-brexit.htm;

- http://www.infomoney.com.br/mercados/noticia/5930082/perigo-frente-italia-pode-passar-por-outro-arriscado-referendo-nos.

A **substituição do dólar por uma nova moeda** que seria emitida pelo FMI - Fundo Monetário Internacional (http://www.imf.org/) foi proposta em 2009 pelo presidente do Banco Central chinês. A ideia do projeto chinês é que a nova moeda não deve ser atrelada a um país específico, mas sim composta de uma cesta com as maiores moedas do mundo; com o que diminuiria o risco da turbulência. No entanto, isso depende da reformulação de alguns órgãos internacionais. O Banco de Compensações Internacionais (BIS) ou Banco Mundial precisaria ser transformado num verdadeiro Banco Central mundial. Além disso, seria preciso aumentar a cesta (Estados Unidos, Japão, União Europeia e Reino Unido) que compõe o SDR (*Special Drawing Right* - Direitos Especiais de Saque) para incluir a moeda da China; o que já ocorreu.

No último século foram propostos vários nomes para a moeda única mundial, por exemplo: Bancor, Unitas, Phoenix e Intor. Um protótipo de moeda foi apresentado aos participantes do G8 no ano de 2009 em L'Aquila (Itália); o protótipo é visível no site da associação UFWC - *United Future World Currency* (http://www.futureworldcurrency.com/).

Comenta-se muito a respeito da criação de uma cesta de moedas de países emergentes, que contenha, por exemplo, reais (Brasil), rublos (Rússia), rúpias (Índia), rands (África do Sul), que possuem flutuação de mercado, e os yuanes (China), que não a possuem. Explica-se. A moeda chinesa não é livremente conversível; pois sua cotação é administrada pelo governo chinês, o que impede sua livre flutuação, condição que deveria ser primordial para que o yuan seja futuramente classificado como livremente utilizável pelo FMI e faça parte da cesta que compõe o SDR.

Os BRICS (https://pt.wikipedia.org/wiki/BRICS) estudam lançar uma nova moeda, composta por uma cesta de suas moedas locais, a ser usada para o comércio internacional; bem como de uma nova moeda de reserva, substituindo o dólar. Ainda mais, planejam um novo sistema de solução de pagamento internacional, substituindo as trocas SWIFT e IBAN, quebrando assim a hegemonia do dólar e da manipulação do ouro pelo Banco de

Pagamentos Internacionais (BIS), em Basileia, Suíça (também chamado de banco central dos bancos centrais).

Desde 2010, os BRICS (Brasil, Rússia, Índia, China e África do Sul) estão trabalhando para abandonarem o dólar e o euro como moedas internacionais. Inicialmente pretendem usarem suas próprias moedas em transações comerciais entre si.

Na última década, a China atrelou o yuan a uma cesta de moedas estrangeiras, composta pelo dólar americano (US$), pelo euro (€), pelo iene (¥) do Japão e pelo won (₩) da Coréia do Sul.

Antes disso, em 08/10/2015, a China deu início ao seu Sistema de Pagamentos Internacionais (CIPS - *Cross-Border Interbank Payment System*) em abandono ao SWIFT (*Society for Worldwide Interbank Financial Telecommunication*), que permite o fechamento de operações de comércio internacional para além de suas fronteiras em sua própria moeda, o yuan ou renminbi (Y com apenas um traço horizontal, 𝍦 ou 𝍧). As autoridades bancárias de Angola e do Brasil já efetuaram pagamentos pelo novo mecanismo de transação transfronteiriço em moeda chinesa.

E se os BRICS resolverem derrubar ou destronar o dólar, qual será a moeda que o substituirá ou qual será a forma de evitar perdas?

- http://www.carosamigos.com.br/index.php/economia/7603-se-brics-renunciarem-ao-dolar-isso-pode-levar-a-consequencias-geopoliticas-catastroficas.

Tanto a derrubada do dólar ou o colapso do euro podem impulsionar a bitcoin?

- http://www.hashbtcbrasil.com.br/2016/06/o-colapso-do-euro-vai-impulsionar-o.html;

- http://www.infomoney.com.br/mercados/noticia/5220056/para-greenspan-brexit-apenas-ponta-iceberg-economia-global-esta-serios.

Já se sabe que quando o yuan (moeda chinesa) desvaloriza, a bitcoin é valorizada e que a bitcoin foi a moeda que mais valorizou em 2015.

Recorda-se, ainda, que a cotação (valor ou preço) da bitcoin subiu após a saída do Reino Unido (Inglaterra) da União Europeia em razão do pânico geral de que a União Europeia iria afundar.

- http://rendasegura.com.br/2016/07/30/preco-da-bitcoin-sobe-apos-a-saida-do-reino-unido-da-uniao-europeia/.

A ideia de uma **moeda internacional composta por uma cesta de moedas** não é novidade. Durante a conferência de *Bretton Woods*, essa ideia foi apresentada por John Keynes, representante do Reino Unido, mas foi sobrepujada pela proposta do padrão ouro - dólar, de Dexter White. Keynes propôs a criação de uma central de liquidação internacional, a ICU (*International Clearing Unit*), que emitiria uma moeda de intercâmbio, o bancor, que poderia ser livremente convertido em qualquer outra moeda. Os países com *superávit* comercial poderiam acumular bancors em suas reservas, as quais renderiam juros; os demais poderiam tomá-los emprestados, de modo que o saldo líquido dessa moeda fosse nulo. Este mecanismo permitiria de fato a solução de um dos problemas que persistem até hoje: muitos países acumulam moeda forte por meio de exportações, pois reservas internacionais elevadas são sinal de solidez macroeconômica e proporcionam equilíbrio no preço da moeda local.

O Banco de Compensações Internacionais ou Banco de Pagamentos Internacionais (*Bank for International Settlements*) é uma organização internacional responsável pela supervisão bancária. Visa promover a cooperação entre os bancos centrais e outras agências na busca de estabilidade monetária e financeira. Sediado em Basileia, na Suíça, reúne vários bancos centrais de todo o mundo.

Já o **Banco Mundial** (*World Bank* - http://www.worldbank.org/) é uma instituição financeira internacional que fornece empréstimos para países em desenvolvimento em programas de capital. É composto pelas seguintes instituições: Banco Internacional para Reconstrução e Desenvolvimento (BIRD), Associação Internacional de Desenvolvimento (AID), Sociedade Financeira Internacional (SFI), Agência Multilateral de Garantia de Investimentos (MIGA) e Centro Internacional para Arbitragem de Disputas sobre Investimentos (CIADI).

O BIRD - Banco Internacional para Reconstrução e Desenvolvimento (ou IBRD - *International Bank for Reconstruction and Development*) é a instituição financeira do Banco Mundial que proporciona empréstimos e assistência para o desenvolvimento a países de rendas médias com bons antecedentes de crédito.

Inclusive, há alguns anos, tem havido discussões no âmbito do G20 (*Group of Twenty* ou Grupo dos 20) e do FMI - Fundo Monetário Internacional (ou IMF - *International Monetary Fund*, http://www.imf.org/) para ampliar a cesta do **SDR** (*Special Drawing Rights* ou DES - Direitos Especiais de Saque); a unidade de conta ou ativo de reserva internacional emitido pelo FMI, criado em 1969 para suplementar as reservas oficiais dos países membros.

O G20 (http://www.g20.org/English/ e http://www.oecd.org/g20/), é um fórum internacional, fundado em 1999, para os governos e respectivos bancos centrais das 20 maiores economias mundiais, com o objetivo de estudar, analisar e promover alto nível de discussão de questões políticas relacionadas com a promoção da estabilidade financeira internacional. Em 2016 a reunião do G20 ocorreu na China.

O FMI é uma organização internacional criada em 1944 na Conferência de Bretton Woods, formalmente criada em 27/12/1945 e homologada pela ONU em abril de 1964, com o objetivo inicial de ajudar na reconstrução do sistema monetário internacional no período pós-Segunda Guerra Mundial. Os países contribuem com dinheiro para o fundo e os membros com desequilíbrios de pagamento podem pedir fundos emprestados temporariamente. O FMI diz trabalhar para promover a cooperação monetária global, a estabilidade financeira segura, facilitar o comércio internacional, promover elevados níveis de emprego e crescimento econômico sustentável e reduzir a pobreza em todo o mundo. Em síntese, o FMI trabalha para melhorar as economias dos países.

O SDR não constitue uma moeda e carece de existência material. Seu valor é calculado em função de uma cesta de divisas. Portanto, o valor de moeda da SDR é determinado pela soma dos valores em dólares norte-americanos, com base nas taxas de câmbio de mercado, de uma cesta das

principais moedas mundiais (dólar americano, euro, iene japonês, libra esterlina e iuane chinês [ou renminbi]).

- http://www.imf.org/external/np/exr/facts/sdr.htm/.

O SDR (*Special Drawing Right* - Direitos Especiais de Saque) foi criado em 1969 no contexto do sistema de *Bretton Woods* de taxas de câmbio fixas, sendo o seu objetivo remediar a falta de dólares americanos e reservas de ouro no comércio internacional.

O SDR é o ativo de reserva internacional emitido pelo FMI para suplementar as reservas oficiais dos países membros e cujo valor reflete uma cesta de moedas composta pelo dólar americano, euro, iene japonês, libra esterlina e iuane chinês (ou renminbi).

- http://www.imf.org/external/np/fin/data/sdr_ir.aspx.

A cesta do SDR tem a sua composição e respectivo percentual de cada moeda revisados a cada cinco anos. Na prática, o SDR é a moeda do FMI, que após equalizada é convertida em dólar.

- http://www.imf.org/external/np/fin/data/param_rms_mth.aspx.

E, em 30/11/2015, o FMI anunciou a inclusão do yuan em sua cesta de moedas de reservas (http://www1.folha.uol.com.br/mercado/2015/11/1713009-fmi-anuncia-inclusao-do-yuan-chines-em-cesta-de-moedas-de-reservas.shtml). A moeda chinesa somou-se, assim, ao dólar, o euro, o iene e a libra esterlina.

- http://www1.folha.uol.com.br/mercado/2015/11/1713009-fmi-anuncia-inclusao-do-yuan-chines-em-cesta-de-moedas-de-reservas.shtml;
- http://g1.globo.com/economia/noticia/2015/11/fmi-inclui-o-iuane-em-sua-cesta-de-moedas-de-reservas.html;
- http://www.jornaldenegocios.pt/mercados/cambios/detalhe/yuan_chines_ja_faz_parte_do_cabaz_de_moedas_do_fmi.html;
- http://brasil.elpais.com/brasil/2015/11/30/economia/1448897386_816387.html;

- http://www.voltairenet.org/article189676.html;
- http://economia.estadao.com.br/noticias/geral,yuan-entra-no-clube-das-moedas-fortes,10000003270;
- http://ionline.sapo.pt/481257.

E quanto à crise econômica ou bancária na Itália?

O sistema bancário italiano está no limiar de uma quebra sistêmica (http://www.mises.org.br/Article.aspx?id=2467), que pode afetar toda a Comunidade Europeia (http://www.infomoney.com.br/bloomberg/mercados/noticia/5281344/italia-pode-gerar-crise-bancaria-europa-diz-societe-generale).

Além dos BRICS, também a OCX estuda formas de abandonar o uso do dólar. A Organização para Cooperação de Xangai (OCX) é uma organização política, econômica e militar da Eurásia, formada pela China, Cazaquistão, Quirguistão, Rússia, Tadjiquistão, Uzbequistão, Índia e o Paquistão.

A Eurásia é a massa que forma em conjunto a Europa e a Ásia.

Entre 1980 e 1990 a União Soviética sofreu revoltas internas e traições de nações amigas resultando em declarações de independência de vários de seus países membros; os quais somente eram membros através do convencimento da força bruta russa.

Em 1992, logo após o fim da União Soviética, o Pentágono aprovou uma resolução, intitulada *Defense Planning Guidance* (Guia de Planejamento de Defesa), que estabelece, como um de seus objetivos centrais, “neutralizar” e “impedir o renascimento” da rival Rússia. Isso tinha, como uma das consequências imediatas, “ampliar a presença” dos Estados Unidos nos países que faziam parte da União das Repúblicas Socialistas Soviéticas (URSS), assim como nos Bálcãs e no antigo Leste Europeu.

Em 1994, o Presidente do Cazaquistão, Nursultan Nazarbayev, sugeriu a ideia de criação de uma "União Euroasiática" durante um discurso na Universidade Estatal de Moscovo. Numerosos tratados foram assinados posteriormente para estabelecer o bloco comercial gradualmente.

A União Eurasiática é uma proposta de aprofundamento da integração econômica e política entre a Bielorrússia, o Cazaquistão, a Rússia, o Quirguistão, o Tajiquistão e outros Estados pós-soviéticos, com o objetivo futuro de criar uma organização supranacional. Nitidamente trata-se de uma reformulação da antiga URSS copiando muita coisa da formação da União Europeia.

A URSS - União das Repúblicas Soviéticas Socialistas (USSR - *Union of Soviet Socialist Republics* ou CCCP - Союз Советских Социалистических Республик) foi um Estado comunista, localizado na Eurásia, que existiu entre 1922 e 1991. A URSS era governada por um regime unipartidário, altamente centralizado, comandado pelo Partido Comunista. Sua capital era cidade de Moscou, na Rússia.

O regime chinês possui muita semelhança do que a URSS era e do que a Eurásia quer ser; ou seja, uma reformulação comunista com aparência de democracia.

Em 1995, Belarus, Cazaquistão, Rússia, e os estados mais tarde aderentes Quirguizistão e Tajiquistão assinaram os primeiros acordos sobre o estabelecimento de uma união aduaneira.

Em 1996, Belarus, Cazaquistão, Rússia e Quirguistão assinaram o Tratado de Integração nos campos humanitários e econômico para permitir a criação de mercados comuns de bens, serviços, capital, trabalho e desenvolvimento de transporte único e sistemas de energia e informação.

Em 1996/1997 Rússia, China, Cazaquistão, Quirguistão e Tajiquistão formaram o grupo dos Cinco de Xangai, a assinatura de acordos sobre a confiança mútua.

Em 1999, Belarus, Cazaquistão, Rússia, Quirguistão e Tajiquistão assinaram o Tratado da União Aduaneira e do Espaço Econômico Único, clarificando os objetivos e as políticas que os Estados membros irão empreender, a fim de formarem a União Aduaneira da Eurásia e o espaço econômico único.

A Comunidade Econômica Eurasiática (CEEA ou EurAsEC) começou em 10 de outubro de 2000, quando Bielorrússia, Cazaquistão, Quirguistão, Rússia e Tajiquistão assinaram o tratado. A EurAsEC foi criada quando o tratado foi finalmente ratificado pelos cinco Estados membros em maio de 2001.

Em junho de 2002 foi assinado a Declaração dos Estados-Membros da Organização de Cooperação de Xangai.

A CEEA implantou políticas econômicas para unificar a comunidade. A União Aduaneira da Bielorrússia, Cazaquistão e Rússia foi formada em 01/01/2010 e posteriormente renomeada para União Aduaneira Eurasiática.

Em 2007, Belarus, Cazaquistão e Rússia assinaram um acordo para criar uma União Aduaneira entre os três países.

Em 18/11/2011, os presidentes da Bielorrússia, do Cazaquistão e da Rússia assinaram um acordo, agendando o estabelecimento da União Eurasiática para 01/01/2015.

O acordo inclui a integração e estabelecimento de uma Comissão Eurasiática e de um Espaço Econômico Eurasiático, a partir de 01/01/2012.

As Quatro Liberdades: bens, capital, serviços e pessoas foram completamente implantadas em 25/01/2012, com a formação do Espaço Econômico Eurasiático.

Em 29/05/2014, os presidentes da Bielorrússia, do Cazaquistão e da Rússia assinaram o Tratado da União Econômica Eurasiática abrindo novos horizontes da parceria.

Em 10/10/2014, um acordo assinado em Minsque (ou Minsk), após sessão do Conselho Interestatal da CEEA, pôs fim à Comunidade Econômica Eurasiática. A organização foi, então, extinta em 01/01/2015, quando foi lançada a União Econômica Eurasiática.

A Armênia assinou o tratado de adesão em 10/10/2014, tornando-se membro em 02/01/2015.

O Quirguistão juntou-se à União em 08/05/2015.

O Tadjiquistão considera aderir também.

Todos os membros da União Econômica da Eurásia aceitaram aumentar a cooperação com a China.

A China e a Rússia já adotam há anos um modelo que permite o comércio em moedas locais sob certas condições. No último ano, Moscou, com dificuldade de realizar transações em dólar por causa das sanções econômicas impostas pelo Ocidente, tem tentando promover ainda mais esse modelo no comércio entre os membros.

Em junho de 2016, o presidente russo, Vladimir Putin, pediu à União Europeia para esquecer as diferenças políticas com Moscou e fazer parte de uma parceria mais ampla, a Eurásia.

Uma Europa dividida e tentando se recuperar dos danos do *Brexit* (saída da Inglaterra da União Europeia) fica mais fácil de aceitar as "mãos amigas" da Rússia e da China.

Também em junho de 2016, muitos altos funcionários alemães (dentre eles, os ministros das Relações Exteriores e da Economia e Energia) querem reestabelecer as relações com a Rússia que existiam durante o governo de Gerhard Schröder (antecessor de Angela Merkel). A porta-voz do Ministério das Relações Exteriores da Alemanha, Sawsan Chebli, declarou que é impossível garantir a segurança na Europa sem a Rússia. Ele disse que as palavras do Secretário-Geral da OTAN, Jens Stoltenberg, mostram que as ações da Aliança não são dirigidas contra a Rússia. Já o ministro das Relações Exteriores francês, Jean-Marc Ayrault, disse que a França quer remover as sanções contra a Rússia o mais rápido possível.

Mais de 40 países e organizações internacionais expressaram seu desejo de criar uma zona de comércio livre com a União Econômica Eurasiática. A

interpretação chinesa da Eurásia coincide bastante com a visão russa. Para a Rússia seria uma versão moderna da antiga URSS de uma futura Eurásia interconectada por várias “novas Rotas da Seda” (*New Silk Routes*) como, por exemplos, a "iron silk road" (Rota da Seda Ferroviária) e o Oleogasodutostão.

- http://www1.folha.uol.com.br/mundo/2015/03/1596528-china-ambiciona-poder-global-com-nova-rota-da-seda.shtml;
- http://economia.estadao.com.br/noticias/geral,a-nova-rota-da-seda-da-china--imp-,1816517;
- http://geab.eu/pt-pt/nova-rota-da-seda-new-deal-a-chinesa/;
- http://veja.abril.com.br/blog/cidades-sem-fronteiras/geograficas/rota-da-seda/;
- http://orientalreview.org/wp-content/uploads/2014/08/iron_silk_road.jpg;
- http://br.sputniknews.com/mundo/20160206/3513074/nova-rota-seda-primeiro-trem-chines-chega-russia.html;
- http://www.cartacapital.com.br/politica/as-novas-rotas-da-seda-e-as-controversias-2979.html;
- https://pt.wikipedia.org/wiki/Rota_da_Seda.

Em 01/07/2016, durante a reunião solene dedicada ao 95º aniversário da fundação do Partido Comunista Chinês, o presidente Xi Jinping disse: “O mundo está à beira de uma mudança radical. Vemos como a União Europeia está gradualmente entrando em colapso, como está a economia dos EUA. [...]. Está tudo acabado para a nova ordem mundial. Assim, ele [o mundo] nunca mais será como era antes; em 10 anos teremos uma nova ordem mundial na qual a chave será a união de China e Rússia." Na verdade, o presidente Xi quer ir além de uma mera aliança econômica e política para uma aliança político-militar; capaz não só de suportar os desafios do futuro, mas também de assumir a liderança no caso do colapso da ordem mundial existente.

Por que a Rússia, e principalmente a China, estão comprando toda a América Latina e a África?

Em 2009, a China tornou-se o maior parceiro comercial da África e a China está buscando expandir agressivamente o uso de sua moeda naquele continente.

- https://caminhoalternativo.wordpress.com/2016/05/20/angola-nigeria-e-marrocos-fecham-acordos-monetarios-chaves-com-a-china-ou-a-criacao-do-petroyuan/;
- http://www.macauhub.com.mo/pt/2016/06/06/banco-da-china-em-angola-gera-expectativa/;
- http://www.ccilc.pt/pt/china-inclui-mocambique-na-sua-parceria-estrategica-global.

Em março de 2015 Putin sugeriu a instituição de uma moeda única para a Eurásia.

- http://br.sputniknews.com/noticias/20160408/4072413/economia-uniao-euroasiatca-moeda.html;
- http://www.ultimosacontecimentos.com.br/ultimas-noticias/a-uniao-economica-da-eurasia-prepara-sua-moeda-unica.html.

Ainda mais, a China e os Emirados Árabes Unidos fecharam um acordo para abandonar o dólar e usarem suas próprias moedas nas transações de petróleo entre si.

Desde 2012, as trocas de mercadorias e serviços entre China e Japão são feitas usando suas próprias moedas (o yuan chinês e o yen japonês) ao invés do dinheiro norte-americano.

Entretanto, ao evitarem ficar reféns da volatilidade do dólar e do euro ao realizarem negócios, eles podem, ao mesmo tempo, acabarem sofrendo com problemas das suas próprias moedas.

A estratégia da China é manter, enquanto for possível, os americanos e o resto do mundo comprando produtos industrializados chineses e, com isso, não só estimular a industrialização chinesa, mas, também, promover a expansão de suas industrias no exterior.

Infra uma relação exemplificativa de sites de vendas chineses:

- http://pt.aliexpress.com/;
- http://portuguese.alibaba.com/;
- http://www.banggood.com/;
- http://www.dx.com/;
- http://www.gearbest.com/;
- http://www.tinydeal.com/pt/;
- http://www.dinodirect.com/;
- http://www.miniinthebox.com/pt/;
- http://www.thinkgeek.com/;
- http://www.neatoshop.com/;
- http://www.vitacost.com/;
- http://www.bookdepository.com/;
- http://www.lightinthebox.com/pt/;
- http://www.asos.com/;
- http://www.miniinthebox.com/pt/;
- http://www.geekbuying.com/;
- http://pt.focalprice.com/;
- http://www.tinydeal.com/pt/;
- http://www.milanoo.com/;
- http://www.romwe.com/;
- http://www.chicwish.com/;
- http://www.tmart.com/;
- http://www.chinabuye.com;
- http://www.everbuying.com;
- http://www.dealsmachine.com;

- http://www.lightake.com;
- http://www.sammydress.com;
- http://www.buyincoins.com;
- http://www.rotita.com;
- http://www.DHgate.com;
- http://www.pandawill.com/;
- https://world.taobao.com/;
- http://www.informacaodiaria.com.br/2013/08/melhores-sites-da-china-para-comprar.html.

Em 2015 a China se tornou pela primeira vez o maior parceiro comercial dos Estados Unidos com uma circulação de mercadorias bilateral no valor de 558 bilhões de dólares. Para tudo isso funcionar, o Banco Central chinês comprou alguns trilhões de títulos da dívida pública dos Estados Unidos para controlar o valor do dólar e manter seus produtos e serviços com preços atrativos; ou seja, desvaloriza a própria moeda para valorizar o dólar.

- http://www.jornaldenegocios.pt/mercados/cambios/detalhe/china_desvaloriza_yuan_para_o_valor_mais_baixo_desde_2011.html.

E quando a moeda chinesa cai, a bitcoin sobe.

- http://itforum365.com.br/noticias/detalhe/120006/em-marco-historico-bitcoin-atinge-valor-acima-de-us-500;
- https://www.coinbr.net/blog/bitcoin-dispara-com-aumento-da-demanda-na-china/.

Ainda mais, a China fornecerá aos Estados Unidos 250 bilhões de yuans (38 bilhões de dólares) no âmbito do programa de investidores institucionais estrangeiros qualificados (RQFII na sigla em inglês) do Banco Popular da China. É um número maior do que o do comércio da China com o Japão, a

Coreia do Sul, a União Europeia e a África. O mecanismo de RQFII permite a investidores estrangeiros adquirirem títulos da categoria A no mercado de fundos da China continental em yuans. Anteriormente, a quota dos EUA era de 80 bilhões de yuans, semelhante à da Coreia do Sul e da Alemanha. A quota maior pertence à cidade chinesa de Sangan com 270 bilhões de yuans, porque foi com esta cidade que começou todo o programa de RQFII em 2011.

Detalhe, a China não pode arriscar suas enormes reservas em dólares na tentativa de valorização da sua moeda, pois valorizaria a sua moeda, mas desvalorizaria os dólares que possui e despencariam as suas exportações.

> "A China, por exemplo, compra a moeda americana, através dos títulos do tesouro, em grandes quantidades, de forma a evitar a sua depreciação, que poderia prejudicar as exportações chinesas. Depois de reunir uma reserva da ordem de trilhões de dólares, o Banco central chinês também não pode permitir que ela perca seu valor e, portanto, as aquisições continuam para evitar a depreciação do dólar e para manter as reservas chinesas ancoradas no asset mais seguro do mundo, os T Bonds. O mesmo se repete no Japão, no Brasil e em outros países. Se o mundo sustenta os EUA, eles também sustentam o vício do mundo em dólares." (http://www.mundorama.net/2016/01/05/dolar-e-tecnologia-militar-a-economia-politica-do-poder-americano-por-joao-fabio-bertonha/).

Em 2014 a Rússia divulgou que o seu comércio de hidrocarbonetos passaria a ser realizado em rublos e moedas locais dos seus parceiros comerciais e não mais em dólares (http://sputniknews.com/voiceofrussia/2014_04_04/Russia-prepares-to-attack-the-petrodollar-2335/).

Recentemente, a Rússia passou a aceitar yuan chineses na compra de seu petróleo, prejudicando a Arábia Saudita. Ainda mais, a marca Urais russos, que passou a vende petróleo em rublos, se tornou uma concorrente direta do Oeste Brent e WTI, que negocia exclusivamente em dólares.

- https://actualidad.rt.com/economia/196934-petroleo-ruso-hegemonia-dolar.

Ainda mais os russos estão acumulando enormes quantidades de reservas em ouro.

> "O Banco Central da Rússia somou 6.700.000 onças troy de ouro (208 toneladas) a suas reservas de ouro em 2015. Em abril de 2016, somou de novo 500.000 onças de ouro (15,55 toneladas) e nos meses anteriores de fevereiro e março somou 24,88 toneladas a suas reservas de ouro. Em janeiro, Rússia comprou 700.000 onças (21 toneladas). As reservas de ouro russas aumentaram a um total de 1.477,42 toneladas em abril de 2016." (https://caminhoalternativo.wordpress.com/2016/05/24/o-banco-central-da-russia-compra-de-novo-reservas-de-ouro-em-abril-2016-com-1555-toneladas/).

O maior detentor de **ouro** do mundo é o governo dos Estados Unidos, com 8.133,5 toneladas. Em novembro de 2009, esta oferta de ouro valia cerca de 330.000 milhões dólares. Outros principais detentores de ouro incluem a Alemanha, o Fundo Monetário Internacional (FMI), Itália, França, SPDR Gold Shares, China, Suíça, Japão e Holanda.

A China é a líder mundial em produção de ouro, posição que passou a ocupar em 2007, quando ultrapassou a África do Sul, até então maior produtora do metal no mundo. Os chineses estão apostando fortemente nos preços do metal, já que a produção vem caindo no resto do mundo, com o maior declínio sendo registrado na África do Sul. Assim, a expectativa da China é que os preços do ouro continuem subindo nos próximos anos, embora tenha se registrado uma queda na demanda de alguns grandes países consumidores, como Índia, Turquia e outras nações do Oriente Médio. Além da China, figuram como grandes produtores da comódite (*commoditie* ou *commodity*) ouro a África do Sul, Austrália, Estados Unidos e Peru.

Apesar do ouro nem sempre valorizar muito, ele não perde nunca! Se ele parar de valorizar, nunca vai valer menos que dinheiro. Isso, entretanto, não significa que é um investimento com maior rentabilidade, mas sim, com maior estabilidade.

Ressalta-se, ainda, que ele é a base histórica do sistema financeiro mundial. Tradicionalmente conhecido como um investimento seguro, o ouro ganha força em tempos de crises econômicas. Quando as ações e títulos falham em épocas de tensão e instabilidade, o ouro sempre demonstrou melhores resultados.

O ouro resistiu a guerras e catástrofes naturais, ao invés disso a moeda de papel fica na dependência da especulação do mercado e monopólio dos bancos centrais. Quando um país sofre algumas dessas consequências logo o dinheiro de papel perde seu valor, mas o ouro acumulado é um grande fator de independência monetária e não sofrera nunca as instabilidades do mercado.

A maior indústria onde o ouro é usado é em eletrônica. A maioria dos nossos *gadgets* (aparelhos) e equipamentos têm componentes de ouro que são comumente encontrados em terminais, contatos, revestimento, sistemas de semicondutores e circuitos impressos. Isto é devido às propriedades anticorrosivas de ouro. Ouro e metais preciosos também são usados em isolamento térmico para automóveis. Ele é também formado em fio e usado no bordado tradicional ou moderno.

> "Ouro mantém seu brilho porque a água e o ar – destruidores de outros metais, como ferro, não podem afetá-lo.
>
> Esta resistência à corrosão combinados com notável capacidade de ouro de conduzir a eletricidade o torna ideal para utilização em componentes eletrônicos. E é por isso que a cada ano, cerca de 200 toneladas de ouro são usadas para a fabricação de TVs, videocassetes, telefones celulares, computadores e etc.
>
> Além disso, Cds de alta qualidade contêm uma fina camada de ouro usada para aumentar a longevidade da mídia e assim garantir o armazenamento de dados mais confiável. Uma das grandes vantagens do ouro é que ele pode ser convertido em folhas finíssimas.
>
> Assim, filmes finos de ouro exibem algumas características incomuns. Por exemplo, na interação do metal com a luz. Quando aquecido e comprimido a ponto de gerar folhas ultra-finas, o ouro se torna transparente. Sabia disso?

A bizarrice não acaba aí. Nesta espessura, o ouro permite que as ondas de luz verde possam passar, mas reflete de volta toda a luz infravermelha. Por isso, janelas revestidas com ouro deixam passar a luz, mas refletem o calor.

Por conta disso, as janelas do *cockpit* de aeronaves modernas são revestidas com ouro, do mesmo modo, as janelas de muitos edifícios de escritórios novos (e caros). Além disso, folha de ouro não transparentes é enrolado em torno as partes vulneráveis ??de veículos espaciais, efetivamente protegendo-os de intensa radiação e calor. Por causa disso, as máscaras dos trajes espaciais (EVA) dos astronautas da Apolo 11 eram revestidos de ouro.

Outra curiosidade do ouro é que ele também é altamente resistente às bactérias.

Por isso, os dentistas gostam de usá-lo para reparar ou substituir os dentes danificados ou deteriorados. Nos últimos anos, o ouro provou ser um material ideal para uso em implantes cirúrgicos, como os tubos de *stents*, que são pequenos fios inseridos no interior do corpo para reforçar as veias danificadas ou artérias. Dada a versatilidade do ouro, seu valor e beleza, garimpeiros, sem dúvida, continuam a vasculhar a Terra por este metal atraente." (http://www.mundogump.com.br/10-coisas-incomuns-feitas-com-ouro/).

"O ouro também possui uma grande ductibilidade, a ductilidade ou ductibilidade é a propriedade física dos materiais de suportar a deformação plástica, sob a ação de cargas, sem se romper ou fraturar. Em outras palavras o ouro é uma excelente matéria prima para se fazer fios finos. Por estas propriedades o ouro é largamente utilizado pela indústria eletroeletrônica para fazer trilhas super finas em microchip, e para impedir a oxidação de contatos. Contatos elétricos críticos ou propícios a oxidação costumam ser banhados a ouro para garantir que não haja oxidações." (https://eletronicaparainiciantes.wordpress.com/2013/01/24/porque-o-uso-da-prata-e-do-ouro-em-circuitos-eletronicos/).

"O ouro é utilizado para fabricação de componentes eletrônicos devido às suas propriedades de condução e estabilidade. No entanto, o material é encontrado em quantidades mínimas dentro de celulares ou

computadores, cerca de 0,025% do total." (http://www.ecodesenvolvimento.org/posts/2012/outubro/reciclagem-de-lixo-eletronico-evitaria-que-ouro).

"CONCENTRAÇÃO DE METAIS CONTIDOS EM PLACAS DE CIRCUITO IMPRESSO DE COMPUTADORES DESCARTADOS" - http://monografias.poli.ufrj.br/monografias/monopoli10007207.pdf

"As aplicações funcionais existem na indústria eletrônica e aeroespacial. É comum realizar eletrodeposições de ouro em componentes eletrônicos, escudos de calor, díodos, circuitos impressos ou pinos de ligação. Os filmes de ouro muito finos têm uma excelente refletividade ao infravermelho, uma boa resistência à corrosão e garantem um baixo ruído de contato. Também se utiliza ouro em ligas destinadas a próteses dentárias, contatos elétricos, equipamento químico, fotografia, etc." (http://www.ouroabsoluto.com.br/TudoSobreOuro.aspx).

"O Brasil desperdiça, nos lixões e aterros do país, cerca de 11 toneladas de ouro por ano. Além disso, são perdidos mais 17 tipos de metais preciosos. Entre eles, a prata, o cobre e o zinco. Toda essa riqueza jaz, escondida, nas 500 mil toneladas de celulares, computadores e demais produtos eletrônicos descartados pelos brasileiros anualmente. Com tamanha fortuna inutilizada, os garimpos dos tempos modernos têm trocado a perfuração da rocha pelas montanhas de sucatas. Algumas empresas estrangeiras estão usando o lixo verde amarelo para abarrotar os cofres de dinheiro. Em todo o mundo, essa conta do desperdício chega a 1,1 milhão de quilos do metal dourado." (http://geofisicabrasil.com/noticias/35-noticias/997-brasil-perde-toneladas-ouro-ano.html).

"A reciclagem evitaria que fossem parar no lixo algo em torno de 228 kg de ouro, 1,7 mil kg de prata e 81 mil kg de cobre na Argentina, apenas em 2011. A estimativa foi divulgada no relatório Mineração e Lixo Eletrônico, produzido pela Organização Não Governamental Greenpeace, e se refere somente aos metais preciosos presentes em um tipo de lixo eletrônico: os celulares."

(http://www.ecodesenvolvimento.org/posts/2012/outubro/reciclagem-de-lixo-eletronico-evitaria-que-ouro).

"Além dos riscos à saúde e ao meio ambiente associados à disposição incorreta destes resíduos, deve-se levar em conta que cada tonelada de telefones celulares contém em média cerca de 3,5 kg de prata, 340 g de ouro, 140 g de paládio e 130 kg de cobre, ocasionando perdas econômicas." (SCHLUEP, M., HAGELUEKEN, C., KUEHR, R., MAGALINI, F., MAURER, C., MESKERS, C., MUELLER, E., WANG, F. (2009). *Recycling – From e-waste to resources*, *Final report. United Nations Environment Programme e United Nations University*, 2009).

"Há mais ouro em 1 tonelada de PCs do que em 17 toneladas de minério bruto do metal" (http://planetasustentavel.abril.com.br/noticia/lixo/conteudo_248323.shtml).

- http://canaltech.com.br/noticia/sustentabilidade/apple-consegue-extrair-mais-de-us-40-milhoes-em-ouro-com-smartphones-reciclados-62801/;

- http://brasil.elpais.com/brasil/2016/04/18/tecnologia/1461001432_877021.html.

Mesmo em odontologia, este metal precioso manifesta a sua utilidade já que as ligas de ouro estão sendo utilizados nas restaurações de dentes permanentes, como pontes e coroas. Enquanto na fotografia, toners de ouro estão sendo usados na mudança da cor do brometo de prata de impressões em preto e branco para tons de azul ou marrom e também aumentar a sua estabilidade. Também é utilizado em *alta-end* (alta-extremidade) de discos compactos como uma camada refletora.

"Nanopartículas de ouro são partículas menores que 100 nanômetros, produzidas a partir do ouro e que tem propriedades variadas. Elas podem, por exemplo, transportar medicamentos para o interior das células sem perfurar as membranas celulares. Podem ajudar no

> tratamento do câncer através da liberação de medicamentos em partes específicas do corpo humano em intervalos controlados. As nanopartículas de ouro também têm propriedades de ligação com diversos outros elementos, o que garante sua utilização na obtenção de materiais híbridos. Podem, ainda, ser utilizadas na fabricação de componentes eletrônicos, no tratamento de doenças genéticas, no desenvolvimento de catalisadores para automóveis." (http://www.fundacentro.gov.br/nanotecnologia/nanoparticulas-de-ouro).

Num artigo da IndiaVision News, de 30/08/2012, com o título sugestivo: "China Lança Moeda Mundial Apoiada por Ouro", indica que a China estaria reestruturando toda a sua reserva de ouro em barras de 1 kg para constituir a base de uma nova moeda para o comércio mundial. Se isso se concretizar, será a morte do dólar como moeda internacional privilegiada e do Euro. Todos irão preferir utilizar uma moeda valorizada por ouro, do que uma moeda (Dólar ou Euro) sem valor real.

Um aumento dos juros pelo *Federal Reserve* (Banco Central americano) pode provocar uma queda na inflação, um recuo do crescimento e uma volatilidade maior, fazendo os investidores se afastarem dos ativos de risco e investirem em ouro, ocasionando sua valorização.

O objetivo das compras de ouro dos bancos centrais é diversificar suas reservas e respaldar seu balanço com o único ativo que não se pode manipular por outro banco central. E talvez também preparar o caminho para a seguinte fase do sistema monetário internacional que responda às estruturas de poder do presente e do futuro.

> "Sejamos honestos, transacionar com ouro em espécie é inconveniente. A característica fundamental do ouro como dinheiro reside na sua oferta inelástica, na incapacidade de governos ou bancos inflacionarem a quantidade do metal em circulação. Mas seria a materialidade a única forma de garantir uma moeda inviolável?" (http://www.mises.org.br/Article.aspx?id=2149).

O dólar norte-americano não será substituído da noite para o dia, mas as coisas estão mudando radicalmente e a China vem se preparando por um longo tempo para isso. A China não revela quanto são suas reservas de ouro, mas é fato que se trata de enormes quantidades. Além disso, a China tem comprado vasta quantidade de dívida dos EUA (Estados Unidos da América).

- http://www.opopular.com.br/editorias/noticias/economia/china-e-petróleo-fazem-dólar-cair-1.1099182.

E se a China resolver, do dia para a noite, de uma só vez, vender dólares a preço vil (forçando sua queda vertiginosa) e depois resolver cobrar as dívidas dos Estados Unidos?

As previsões dos especialistas é de que em menos de 10 (dez) anos, o dólar será substituído por um sistema tripolar: dólar, euro e yuan (ou renminbi). Sob a presidência francesa do G20 e G8 em 2011, já se tem sido disseminada a ideia.

Quando falamos em opções de pagamento, nada é mais conveniente do que o pagamento eletrônico. Você não tem que emitir um cheque, passar um cartão ou lidar com dinheiro vivo; tudo o que precisa fazer é inserir algumas informações no seu navegador de Internet, seja no computador, *notebook*, *netbook*, *tablet*, *smartphone* ou, até mesmo, através da *Smart Tv*. Não é de admirar que cada vez mais as pessoas estão optando pelo pagamento eletrônico (*e-payment*), como uma alternativa a enviar cheques pelo correio.

Por fim, a bitcoin é a primeira moeda digital internacional e vários países e empresas estão querendo se apossarem, se apropriarem, controlarem ou dominarem esse novo tipo de moeda. Há uma acirrada disputa para ver quem vence a batalha e se torna o senhor da moeda.

Assim, por exemplo, recentemente a Rússia divulgou que planeja introduzir a sua própria moeda virtual.

- http://gazetarussa.com.br/economia/2016/05/30/governo-russo-planeja-introduzir-criptomoeda-nacional_598619;
- http://br.sputniknews.com/mundo/20160527/4793280/russia-moeda-virtual.html.

QUESTÃO MILITAR E GUERRA

À primeira vista pode parecer estranho falar de militares e de guerras num livro sobre moedas digitais, mas esses temas estão interligados. Explica-se. Esses dois elementos são muito comuns na definição de qual moeda será predominantemente usada, desejada ou valorizada. E tal entendimento é crucial para quem deseja investir em alguma moeda. Um fundamento simples de compreender é que o país que se sobressai com poder bélico, mesmo que seja deplorável ou fraco em outros requisitos, normalmente possui sua moeda forte, estável e valorizada. Explica-se. Como, por exemplo, o antigo Império Romano por possuir uma máquina de guerra proeminente, tomava dos outros países e povos aquilo que não produzia, não tinha, necessitava ou estava em falta. Desse modo, através do poder bélico o Império Romano conseguia suprir as suas necessidades, demandas, insumos e suprimentos, com o que crises, escassezes e inflações eram evitadas. Esse é um dos grandes motivos do dólar norteamericano ser uma moeda forte; vez que, por exemplo, faltar petróleo nos Estados Unidos, eles invadem algum país e tomam o petróleo que necessitam. Essa confiança ou certeza de que não haverá escassez dá estabilidade e força à moeda. Já a insegurança, incerteza ou receio, por outro lado, geram desconfiança e descrédito na moeda, com o que a mesma perde valor. Também de forma defensiva, as forças armadas ajudam muito na força da moeda; vez que impedem que outra nação invada e tome seus recursos ou lhes imponham um bloqueio econômico.

Por óbvio que as informações deste capítulo não estarão atualizadíssimas, mas faltarão apenas algumas atualizações rápidas que ajudarão rapidamente ao leitor compreender e assimilar melhor o que está acontecendo para poder se antecipar ou estar na frente dos demais. Por outras palavras, os antecedentes são essenciais para a exata compreensão das notícias tendenciosas, incompletas, destorcidas ou manipuladas que a Mídia / Imprensa nos passam.

Desde antes e durante as guerras, a população dos países em conflito ficam com receio do governo confiscar seu dinheiro e bens (tal como os nazistas fizeram com o patrimônio dos judeus), dos bancos falirem ou de seus bens serem destruídos nos ataques. Desse modo, as pessoas enviam o

dinheiro e bens para o exterior, onde esperam que sejam preservados. Além disso, muitos também fogem do país e até desertam para não lutarem.

Ainda mais, em tempos de guerra, o governo corta investimentos em diversas áreas para investir tudo na guerra. E, para piorar, as pessoas deixam de gastar dinheiro, de comprar, de contratar serviços, de fazerem investimentos e de empreenderem dentro de tais países. O raciocínio é lógico, em havendo guerra, o patrimônio pode ser destruído num ataque e, a qualquer momento, pode ser necessário empreender fuga. As pessoas nesses países, portanto, se preocupam em economizar, preservar seu patrimônio e em adquirir apenas gêneros essenciais ou de primeira necessidade, tais como, por exemplos, alimentos, água potável, medicamentos, agasalhos, armas e/ou equipamentos de proteção e veículos e respectivos combustíveis e suprimentos de manutenção. Desse modo, imóveis, turismo, moda, grife, esporte, lazer e luxo são supérfluos e dispensáveis nessas circunstâncias.

Outra observação, é que em tempos de guerra existe o receio das moedas desvalorizarem demasiadamente ou até serem extintas, bem como existir dúvidas de qual moeda sofrerá esses efeitos negativos e qual poderá ser valorizada. Diante disso, as pessoas também costumam aplicar suas economias em ouro, pedras preciosas e outras comódites não perecíveis.

Durante a guerra, não só nos países conflitantes, mas também nos aliados e nos fornecedores de insumos e suprimentos, ocorre a escassez de bens e o consequente aumento dos preços dos mesmos. Em razão de que os países em guerra normalmente sofrem imediata baixa na quantidade de empresas, indústrias, fonte de alimentos e de mão de obra em razão dos trabalhadores se tornarem soldados na guerra e dos que restaram (civis), ocorrer grande quantidade de fuga maciça das pessoas residentes nos países envolvidos no conflito e, ainda, da necessidade muito maior do que a habitual de certos suprimentos, bens e serviços, os países em guerra necessitam comprar de outros países. Em razão da extrema necessidade, e até mesmo desespero, esses países pagam valores muito superiores aos normais, com o que os vendedores deixam de fornecer dentro de seus respectivos países para exclusivamente exportarem (bens e serviços) para os países em guerra. Desse modo, ocorre escassez de determinados bens e serviços dentro desses países vendedores e um aumento nos preços de tais bens e serviços. E, em

razão da súbita necessidade de trabalhadores nas indústrias e empresas beneficiadas, ocorre uma valorização salarial nas áreas envolvidas, que pode refletir negativamente em outras áreas e estimular a inflação generalizada.

Um exemplo recente é a tensão político-militar em Moçambique que resultará em graves consequências para a economia do país. Por óbvio que em ocorrendo conflitos armados, os turistas desaparecerão, os cidadãos e os estrangeiros começarão a fugir com seus bens, as empresas encerrarão as atividades no país, o capital estrangeiro parará de entrar e começará a ser repatriado ou enviado para outro país, as exportações diminuirão pela desconfiança do mercado, etc. Tudo isso afeta a economia num efeito dominó e, em consequência, proporciona inflação e enfraquece a moeda do país.

No Brasil, por exemplo, durante os quatro anos da Primeira Guerra Mundial, os países europeus envolvidos no conflito voltaram a produção de suas indústrias para a fabricação de armamentos e equipamentos para os soldados. Desta forma, o Brasil ficou sem opções para importar produtos manufaturados da Europa. Entretanto, o Brasil lucrou muito exportando matérias-primas (como, por exemplo, borracha) e produtos agrícolas (café, cacau e açúcar) para os países em guerra. Essa situação resultou na elevação do preço do café. Diante disso, os cafeicultores brasileiros aproveitaram o momento e investiram capital acumulado na industrialização do Brasil. A partir da entrada do Brasil na Segunda Guerra Mundial, a produção e comercialização de vários produtos considerados importantes para o consumo da população foi restringida e, até mesmo, substituída pela produção de armamentos, vestimentas e alimentação para os combatentes. A importação de produtos supérfluos deu lugar aqueles que poderiam ser utilizados na guerra, tais como, por exemplos, combustíveis, munições, armas e chapas de ferro e aço que seriam transformadas em navios, tanques e aviões de guerra.

Ressalta-se que, normalmente, no país vencedor do conflito militar, as coisas melhoram significadamente após o fim da guerra. O grande exemplo é o Estados Unidos da América (EUA) durante a Segunda Guerra Mundial. Desde a queda da Bolsa de Valores em 1929, com o que surgiu a Grande Depressão, os Estados Unidos estavam em crise, com uma taxa de

desemprego de 30%. Somente com a Segunda Guerra Mundial, a economia dos Estados Unidos se recuperou da Grande Depressão, pois a produção (armas, aeronaves, tanques, munições, etc.) em tempo de guerra criou milhões de novos empregos. Em 1944, a taxa de desemprego caiu para apenas 1,2%. Ao contrário dos Estados Unidos, a maioria dos países envolvidos na Segunda Guerra Mundial sofreram devastação generalizada devido aos combates dentro de seus limites territoriais durante todo o curso da guerra. Um ano depois do fim da II Guerra Mundial, a economia privada americana cresceu 30%. De uma nação de caipiras passou a ser a potência mundial e sua moeda se tornou a moeda universal desde então. Os norte-americanos usaram o dinheiro que haviam economizado durante a Segunda Guerra Mundial para adquirir bens de consumo que não estavam disponíveis durante o conflito. Com o subsequente boom (explosão de crescimento) da economia, milhares de pessoas encontraram emprego nos Estados Unidos. Desse modo, os norte-americanos estavam ganhando mais dinheiro e a nação tinha o mais alto padrão de vida de todo o mundo.

De modo semelhante, até a Segunda Guerra Mundial, a economia da Itália era baseada primariamente na agricultura. Porém, após o fim da guerra, esta passou por grandes mudanças, que a tornaram um país primariamente industrial.

Em razão da atual guerra civil, a Síria perdeu metade da sua economia através da escassez, inflação, sanções e fuga de capital e trabalhadores. O PIB (Produto Interno Bruto) da Síria despencou 57% em termos reais desde 2010. Desde o início da guerra civil síria, a produção de petróleo no país começou a cair rapidamente. E ficou pior ainda depois da aplicação das sanções europeias.

De modo semelhante, em razão das sanções relacionadas à crise ucraniana, a Rússia perdeu acesso aos mercados financeiros dos Estados Unidos e da União Europeia. Pior, a Rússia estava contando com investimentos de US$ 10 bilhões pela Arábia Saudita e de US$ 7 bilhões pelos Emirados Árabes, mas em razão do envolvimento militar russo na Síria, estes investimentos árabes estão suspensos. A Turquia planejou construir diversos gasodutos para ligar Irã, Azerbaijão e Turcomenistão à Europa, os quais, inevitavelmente, tem que passar pela Síria; mas com a

guerra civil na Síria, esse projeto também está suspenso. Recorda-se, ainda, que mais de 50% do orçamento da Rússia advém da venda de petróleo e gás. Estas são as razões da pressa da Rússia em acabar logo com a guerra na Síria.

> "O Mar Cáspio é o maior mar fechado do mundo (Landlocked) e é cercado pelo Azerbaijão, Cazaquistão, Irã, Turcomenistão e Rússia. É, também, amplamente considerada uma fonte de recursos energéticos por suprir a crescente demanda interna do Cáucaso e da Ásia Central, e, por contingenciar aproximadamente uma reserva de hidrocarbonetos válida entre 30 a 40 anos de suprimento, transportando também energia para o leste europeu e para o norte do Paquistão e noroeste da China. É considerado a maior e, dependendo do ponto de vista, melhor alternativa de acesso à hidrocarbonetos que não seja provindo do Oriente Médio – e por isso, é alvo de uma crescente rota de pipelines, ou oleodutos, que cruzam majoritariamente o Turcomenistão, Cazaquistão, Irã, China e Ucrânia consequentemente até seus destinos finais. Até 2010, houve mais de 18 tentativas de pipelines entre território centro-asiático, chinês e russo que cruzaram o Cáspio ou redirecionaram em algum nível seus recursos. As pipelines Blue Stream, South Caucasus gas pipeline, Turkmenistan-China, Turkmenistan-Iran, Baku-Supsa, Caspian Pipeline Consortium, Baku-Tblisi-Ceyhan, Kazakhstan-China foram modelos de sucesso. As pipelines South Stream, Central Asia-Center upgrade, Pre-Caspian Pipeline, Nabucco, Turkey-Greece-Italy, Turk-Afghan-Pakistan-India (TAPI), Iran-Pakistan-India (IPI), Samsun-Ceyhan e Kashgan são modelos novos que ainda estão em discussão, sendo passivos de aceitação ou não." (http://www.mundorama.net/2016/02/16/a-expansao-do-poderio-militar-russo-no-mar-caspio-por-guilherme-mello/).

Desde que Obama assumiu a presidência, as despesas militares dos Estados Unidos estão em forte queda, causando um impacto negativo sobre o crescimento da economia, tendência que deve se manter ao longo dos próximos anos se Donald Trump não retomar os investimentos militares. Explica-se. Toda a economia dos Estados Unidos é construída com base na questão militar. Desse modo, para manter seu crescimento econômico, os Estados Unidos precisam de uma guerra a cada quatro anos. Do contrário, o crescimento econômico diminui.

Segundo informações divulgadas pelo WikiLeaks, o Estado Islâmico seria uma criação dos Estados Unidos, através da CIA (Agência de Inteligência Americana), justamente para servir de desculpa para não só começar uma nova guerra, mas para criar o caos generalizado na região que permitiria os Estados Unidos e seus aliados levarem a democracia da divisão dos despojos de guerra (apropriação do petróleo alheio) como fizeram no Iraque de Saddam Hussein; bem como de enfraquecer os países rebeldes ao império americano.

A OTAN (Organização do Tratado do Atlântico Norte) deveria ter sido extinta imediatamente depois do colapso da União Soviética, porque a ameaça soviética era a única razão para sua existência; mas decidiu se tornar uma agência militar submissa aos Estados Unidos e, assim, ampliar o número de seus membros e a sua presença militar cada vez mais próxima das fronteiras da Rússia. A aliança EUA - OTAN, portanto, está incomodada em ver muitas nações começarem a se levantar contra o imperialismo americano. Demorou muito para a Rússia passar a estranhar e desconfiar das intenções da OTAN, a qual tem se empenhado em promover a guerra ao invés da paz; vez que sempre estimula ou inventa conflitos cada vez mais em direção à Rússia. E, tudo isso, sob as ordens dos Estados Unidos. Explica-se. O colapso da União Soviética desencadeou a unidade neoconservadora para a hegemonia mundial dos Estados Unidos e, Rússia, China e Irã, são as únicas restrições (os últimos obstáculos) para o império americano mundial. Deste modo, destruindo-se os principais países opositores ao imperialismo americano, os demais países insurgentes ficarão intimidados. Recentemente, a OTAN, liderada pelos Estados Unidos, reforçou seu potencial ofensivo nas fronteiras ocidentais da Rússia e Bielorrússia, fato este que obriga a Rússia a tomar medidas de resposta defensivas. Por outras palavras, a Rússia não irá assistir impassível ao aumento das forças militares da OTAN na Europa Central e Oriental. Nesse contexto, Moscou tem investido na modernização de suas Forças Armadas para recuperar o território perdido, restaurar seu controle sobre a Europa Oriental e se livrar das ameaças da OTAN. Diante disso, a Noruega se tornou um possível alvo russo devido às bases navais americanas montadas nas fronteiras do país. Logo, um conflito global poderia seria inevitável.

No início de 2014 os Estados Unidos gastaram US$ 5 bilhões em um golpe de Estado na Ucrânia, derrubando um governo eleito democraticamente e substituindo-o por um governo na capital de Kiev, que incluiu nazistas. Os Estados Unidos estabeleceram uma base no lado ocidental da Ucrânia, onde tropas das Forças Especiais do Exército dos Estados Unidos vêm para treinar neonazistas que foram designados para a recém-criada Guarda Nacional Ucraniana. Essas forças foram então para o leste da Ucrânia, ao longo da fronteira russa, onde nos anos seguintes mataram milhares de cidadãos inocentes bombardeando suas casas, hospitais, igrejas, escolas, creches, aeroportos e estações ferroviárias. O único "crime" do povo no leste da Ucrânia é serem de origem étnica russa. Através dessas práticas, os Estados Unidos pretendiam desestabilizar a Ucrânia para, em última instância, forçar a mudança de regime em Moscou (derrubar Vladimir Putin do poder). Uma das razões para isso é que, devido às mudanças climáticas, o gelo do Ártico está derretendo e as corporações petrolíferas americanas estão ansiosas para perfurar na região do Ártico. Mas a Rússia tem a maior fronteira terrestre, portanto, existe a suposta necessidade de quebrar a grande Federação Russa em pedaços, como aconteceu com a Iugoslávia durante a presidência de Bill Clinton. Ao fazer isso, as companhias de petróleo acreditam que terão mais facilidade em agarrar o óleo perto da costa do Ártico russo. Esses são os verdadeiros motivos para a Rússia ter instalado, recentemente, uma base militar no local e da ONU ter decretado, logo depois, área de preservação marinha.

Em razão disso, o governo americano, sob o controle de Barack Obama, ficou militarmente voltado para a Rússia, maior potência mundial em termos nucleares e que vem mostrando enorme força bélica ofensiva ao invadir a Geórgia, Crimeia e Ucrânia. E, além dessa política ostensiva, o presidente Vladimir Putin vem reforçando ainda mais o arsenal. Como estratégia militar, os Estados Unidos arrastaram os aliados ocidentais atrás deles em preparação para a guerra com a Rússia e a China. Os Estados Unidos também querem a Índia dentro dessa coalização de falsos mocinhos por razões óbvias de geografia, história e poder econômico crescente. Os Estados Unidos também precisam de aliados com dinheiro para ajudar a pagar a conta caríssima da máquina de guerra sem fim do Pentágono.

Já faz alguns anos que os Estados Unidos estão implantando febrilmente em todo o mundo os chamados sistemas de “Defesa de Mísseis” (MD - *Missile Defense*); essencialmente cercando a Rússia e a China.

- https://www.mda.mil/;
- https://www.armscontrol.org/factsheets/usmissiledefense;
- http://www.ucsusa.org/nuclear-weapons/us-missile-defense#.WBtzCvkrLDc;
- https://en.wikipedia.org/wiki/United_States_national_missile_defense;
- https://en.wikipedia.org/wiki/Missile_defense_systems_by_country.

O MD está sendo implantado pelo Pentágono (Departamento de Defesa dos Estados Unidos) no Japão, Okinawa, Coreia do Sul, Taiwan, Guam, Filipinas e Austrália com a desculpa de ser proteção contra os mísseis norte-coreanos. Isso é uma tremenda mentira porque a Coréia do Norte ainda está engatinhando em tecnologia de mísseis. Na verdade, os Estados Unidos estão fazendo um cerco contra a China e a Rússia com a finalidade de controlar e dominar. Outro detalhe, o MD é ilegal nos termos do Tratado Antimísseis Balísticos (ABM - *Anti-Ballistic Missile Treaty*) entre a Rússia e os Estados Unidos. O MD, portanto, é um programa de desestabilização de forças com a finalidade de dar vantagem aos americanos e, assim, colocar a China e a Rússia de joelhos. A principal função do MD é ser um escudo contra a capacidade de retaliação nuclear desses países depois que os Estados Unidos derem o primeiro tiro através da espada do Pentágono bem no coração de suas forças nucleares.

Acrescenta-se, ainda, o remanejamento de 60% das forças militares dos Estados Unidos na Ásia-Pacífico (às portas da China e da Rússia) com a pseuda justificativa de reequilíbrio de forças.

Explica-se. A China importa 80% (oitenta por cento) dos seus recursos em navios e, assim, a aliança EUA - OTAN realizou uma estratégia militar visando bloquear as rotas marítimas da China; similar aos submarinos nazistas que, durante a segunda guerra mundial, tentaram isolar o comércio da Europa, afundando todas as frotas de suprimentos. Em resposta, a China tem construído algumas bases militares em pequenos recifes de coral para

garantir o seu acesso sem entraves às rotas marítimas na sua região. Ainda mais, a China lançou um porta-aviões em sinal de que está pronta para o confronto.

Enfim, é facilmente perceptível as constantes sabotagens de Barack Obama para enfraquecer a Rússia e esfacelá-la em vários pedaços a serem administrados por capachos dos americanos. Recordem das acusações americanas de que Saddam Hussein (Iraque) tinha armas de destruição em massa, mas tais alegações nunca foram provadas; muito menos encontraram qualquer evidência disso. A única constatação foi que os Estados Unidos e seus aliados, através da Guerra do Iraque (Ocupação do Iraque ou Segunda Guerra do Golfo), estavam somente interessados no petróleo do Iraque.

Quando a antiga URSS (União das Repúblicas Socialistas Soviéticas) entrou em colapso, os Estados Unidos prometeram que a OTAN (Organização do Tratado do Atlântico Norte) não expandiria um centímetro em relação à Rússia. Desde então essa promessa tem sido repetidamente quebrada e, recentemente, a OTAN estabeleceu bases ao longo da fronteira da Rússia na Letônia, Lituânia e Estônia. Os sistemas MD do Pentágono foram recentemente implantados na Romênia e estão sendo implantados na Polônia e nas águas ao longo das costas da Rússia e da China. O sistema Aegis nos *destroyers* (destruidores) da Marinha também carregam mísseis interceptores MD *on-board* (a bordo) e estão sendo aportados no Japão, Coreia do Sul, Filipinas e Guam.

- http://missilethreat.csis.org/system/aegis/;
- http://www.lockheedmartin.com/us/products/aegis.html;
- https://www.mda.mil/system/aegis_bmd.html.

Deste modo, através do MD, os Estados Unidos estão querendo o controle exclusivo da lança mortal de Zeus; porque nenhuma outra nação possuirá os satélites e estações terrestres em todo o mundo que darão a Washington a capacidade de ver tudo, ouvir tudo e atacar qualquer alvo em qualquer lugar do planeta.

Em conclusão, o MD é um altíssimo desestabilizador, fortíssimo provocador e perigoso comprometedor da paz mundial. Em vários dos países da região, houveram, e existem, protestos contra a implantação dos MD por essas razões. Mas, a Mídia internacional, submissa aos interesses norte-americanos, omitem esses protestos. E, pior, tem se empenhado em divulgar ao mundo que a Rússia é que estaria querendo começar uma guerra mundial.

- http://www.jornaldenegocios.pt/economia/detalhe/estara-a-russia-a-preparar-se-para-a-terceira-guerra-mundial.

O serviço secreto canadense divulgou, no final de junho, um relatório sobre as ameaças à segurança mundial até 2018. No documento, um espaço considerável é dedicado às ameaças provenientes da Rússia. Segundo os autores, o aumento do potencial militar da Rússia é uma prova de que o país está se preparando para uma guerra real, e não para uma guerra híbrida.

- https://www.csis-scrs.gc.ca/pblctns/ccsnlpprs/2016/2016-06-03/GLOBAL_SECURITY_POST-CONFERENCE_ENGLISH.pdf.

Em julho de 2013, os russos realizaram o maior treinamento militar do país desde os tempos soviéticos. A ação envolveu dezenas de navios da frota do Pacífico, 130 aviões de combate, 160 mil soldados e cerca de 5.000 tanques na Sibéria e na região do Extremo Oriente, em uma demonstração maciça de poderio militar da nação.

As relações entre a NATO - *North Atlantic Treaty Organization* (OTAN - Organização do Tratado do Atlântico Norte) e a Rússia azedaram depois da anexação da península ucraniana da Crimeia pela Rússia em 2014, dando início a uma guerra civil na Ucrânia.

- Capacidade militar da Rússia surpreende a Europa e os EUA - https://www.youtube.com/watch?v=v07J-ie7j_I;

- http://g1.globo.com/mundo/noticia/2016/08/russia-mobiliza-sistemas-antimisseis-ultramoderno-na-crimeia.html.

A aquisição rápida e quase sem derramamento de sangue da Crimeia pela Rússia em 2014 foi efetivamente uma operação secreta.

O governo russo realizou manobras militares de magnitude excepcional para se exibir ao Ocidente: mísseis balísticos (Iskander) disparados no enclave europeu de Kaliningrado, bombardeiros na Crimeia, soldados no Ártico, etc. O Iskander tem a capacidade de passar através do escudo norte-americano e de alcançar metade das capitais europeias, podendo chegar até Berlim. O medo dos russos ressurgiu na Europa.

- http://www.assuntosmilitares.jor.br/2016/07/otan-se-reune-em-varsovia-para-debater.html;
- http://www.defesanet.com.br/otan/noticia/22855/OTAN-se-reune-em-Varsovia-para-debater-ameaca-russa/.

No dia 09/05/2015, com a desculpa de comemorar os 70 anos da vitória sobre os nazistas durante a 2ª guerra mundial, a Rússia fez uma demonstração de seu poderio bélico, numa das maiores comemorações do Dia da Vitória em décadas. Cerca de 16.000 tropas participaram no desfile na Praça Vermelha e, ainda, foram exibidas armas de nova geração, como os tanques Armata T-14 e T-15, os tanques T-90 e BTR-82A, veículo de infantaria de combate Kurganets-25, veículos anfíbios de combate de infantaria BMD-4M e rampas de lançamento do sofisticado míssil terra-ar S-400 e 68 helicópteros e aviões, incluindo os bombardeiros Tu-160 e MiG-29, voaram sobre Moscou. Também foram exibidos os canhões autopropulsados Msta-S e os sistemas de mísseis Yars, de mísseis táticos Iskander-M, e mísseis superfície-ar Tor-M2U, de mísseis antiaéreos S-400 Triumf e de artilharia antiaérea Pantsir-S1.

O alcance de detecção de alvos do S-500 é superior em 200 quilômetros ao do S-400; ou seja, cerca de 800 quilômetros. O S-500 Triumfator-M pode atingir mísseis de cruzeiro hipersônicos com velocidades de 5.500 quilômetros por hora, ou superiores. Equipada com um radar extremamente potente e com um sistema informático muito avançado.

De modo semelhante, as Forças Armadas da China deram uma demonstração de seu poderio militar durante as comemorações dos 70 anos da vitória sobre o Japão na Segunda Guerra Mundial. 12.000 soldados na

rua, uns 200 aviões de combate, um monte de tanques, canhões e mísseis modernos, inclusive nucleares.

Na *Arms Expo* 2015, realizada na cidade de Nizhny Tagil de Urales, as empresas russas apresentaram toda uma série de novos equipamentos militares. Dentre eles, o T-14 Armata, um tanque de guerra da quinta geração; o T-15, um veículo de combate de infantaria pesada, ambos são bons exemplos das tecnologias mais recentes do país; a nova versão do BMP-3, um veículo de combate de infantaria, equipado com uma estação de controle remoto e uma arma automática de 57 milímetros; o tanque T-90MS, dotado de sistemas de proteção nuclear, química e biológica, bem como painéis blindados para proteger o tanque de projéteis e estilhaços, com um fuzil de alta precisão de 125 milímetros e de uma metralhadora de 7,62 milímetros anti-aeronave controlada remotamente e montada no topo da torre, visando alvos estacionários e móveis; e, o Koalitsiya-SV, uma arma automotora de 152 milímetros projetada para neutralizar baterias de artilharia, assim como tanques, armas antitanque, forças de defesa antimísseis e fortificações de campo.

O veículo robótico subaquático Glider-T foi apresentado no fórum militar internacional *Army* 2015 e impressionou por sua tecnologia de última geração.

Durante a edição 2015 do MAKS, o Salão Internacional de Aviação e Espaço, em Zhukovski, nas proximidades de Moscou, uma coletiva de imprensa divulgou o MiG35 (FulcrumF).

O projeto do novo super porta-aviões (*super aircraft carrier*) russo, 23000E “Storm”, foi exibido no fórum militar Army 2015 em Kubinka. Com 330 metros de comprimento e 40 de largura, o “Storm” é projetado para conseguir transportar de 80 a 90 aeronaves, incluindo o novo caça Sukhoi T-50.

O T-50 possui tecnologias inovadoras, sistemas aviônicos avançados e carrega o sistema de navegação inercial atualizado BINS-SP2M, que processa informações de navegação e voo de forma autônoma, determina parâmetros de posição e movimento na ausência de navegação por satélite e

pode se integrar com o GLONASS, sistema de navegação por satélite da Rússia baseada no espaço (GPS russo).

- https://br.sputniknews.com/defesa/201508261959167/.

A Rússia organizou na Síria uma verdadeira exposição real das suas novas armas, e não apenas as armas, mas as habilidades de seu exército modernizado. A guerra na Síria tornou-se uma vitrine para a estreia de diversas armas avançadas russas: mísseis de cruzeiro, navios de guerra, submarinos furtivos silenciosos, caças e bombardeiros.

> "Graças à operação na Síria, a influência russa no Oriente Médio tem alcançado um nível sem precedentes desde o fim da União Soviética, enquanto que as posições dos EUA na região não deixam de debilitar-se por diversas razões, incluindo seu apoio ao terrorismo e sua aliança com regime o despótico da monarquia absolutista da Arábia Saudita e com Israel, que é odiado em toda a comunidade árabe no Oriente Médio." (https://dinamicaglobal.wordpress.com/2015/10/22/russia-se-converte-na-potencia-mais-influente-no-oriente-medio/).
>
> Veja, ainda: https://dinamicaglobal.wordpress.com/2014/01/01/os-passos-de-urso-dos-russos-enquanto-os-americanos-se-afastam-do-oriente-medio/.

Na Síria, com a desculpa de atacar o Estado Islâmico, a Rússia, desde 30/09/2015, mostrou ao Ocidente seu poder de fogo renovado. Foi a maior operação de Moscou no Oriente Médio desde que a União Soviética enviou tropas ao Egito na década de 1970. Os ataques envolveram aeronaves nunca antes testadas em combate. Foram empregados os caças bombardeiros Tupolev TU-24, SU-25M, Su-30SM e Su-34 (Sukhoi 34 que a Otan chama de Fullback) com raio de ação de 4.000 km, bombardeiros táticos Su-24M, jatos Su-25SM 12, helicópteros de ataque Mi-24 e Mi-8AMTSh. A atenção inicial ficou com os mísseis de cruzeiro (Kalibr-NK ou 3M-14T), com alcance de até 2.500 km (o que ultrapassa o equivalente norte-americano em capacidade tecnológica), que foram disparados de navios e de submarinos de nova geração de classe Kilo (Rostov do Don). Também foram enviados para a base um sistema de mísseis anti-aeronaves Pantsir-S1, sistema de

defesa antiaéreo S-300 e complexos de guerra eletrônica IL-20 (equivalente ao Orion americano), equipados com o sistema Krasukha-4 de última geração. Foram empregadas munições de precisão: bombas KAB-500S guiadas pelo GPS russo (satélites GLONASS) e mísseis KH-25ML guiados por laser. Também foram utilizados os lançadores de foguetes TOZ1A de 24 tubos, calibre 220 mm, munição com ogivas termobárica, alcance útil de 3.000/3.500 m, dito "lança-chamas" no jargão militar russo. Depois a atenção mundial se voltou para os drones (aeronaves não-tripuladas) militares russos empregados na Síria.

- https://br.sputniknews.com/infograficos/201609306464809-russia-siria-estrutura-resultados/;
- https://br.sputniknews.com/ciencia_tecnologia/201609296451855-drone-T-16-Enics-Siria/;
- https://br.sputniknews.com/opiniao/201610126543233-s-300-siria-aviso-ocidente/.

O Mi-24 acelera até 300 km/h e sobe a uma altitude de até 4,5 quilômetros. Cada helicóptero está armado com quatro blocos de 20 foguetes de ar para o solo não guiados e um canhão de 30 milímetros.

O Melhor helicóptero de guerra do mundo é o Ka-50 Black Shark Ka-52 Alligator da Rússia.

O Su-34 tem uma velocidade máxima de 1.900 km/h e um alcance máximo de ações de 4.500 quilômetros sem reabastecimento em voo. O teto operacional atinge mais de 14.000 metros acima do nível do mar. Seus 12 pontos de ancoragem permitem ao Su-34 transportar até 8 toneladas de munição. De acordo com relatórios oficiais do Ministério da Defesa, os Su-34 usaram na Síria bombas guiadas KAB-500 e mísseis X-29L guiados por laser.

Os mais recentes ataques dos bombardeiros estratégicos russos Tu-160 se tornaram uma demonstração da capacidade da aviação de longo alcance russa. Em 18 de novembro de 2015 a Rússia pela primeira vez em sua história colocou em ação seus mísseis de cruzeiro ar-terra mais avançados, o X-101, adotados pela Força Aérea do país em 2013. O míssil subsônico X-

101, voa a uma altura de 30 metros a 10 km, tem um fantástico alcance de 5.500 quilômetros, o que excede em muito a capacidade dos seus rivais europeus e americanos. O X-101 é invisível ao radar e muito preciso com um desvio máximo da meta de não mais de 5 metros (contra um alvo fixo) e 10 metros contra um alvo em movimento em uma variedade de lançamento de 5.500 quilômetros. Este foguete combina um sistema de orientação com base inercial, via satélite baseado no sistema de navegação russo Glonass e orientação infravermelha que é ativada no fim do trajeto. Já X-102, também seria invisível para radares, possui ogiva nuclear e tem um alcance de 5.000 km. Detalhe, na madrugada do dia 19 para 20 de novembro de 2015, dois bombardeiros Tu-160, partiram da Base Aérea de Olenegorsk, na Península de Kola, e contornaram a Europa Ocidental antes do ataque à Síria; um trajeto de 13.000 km sem reabastecer. Passaram próximo ao espaço aéreo da Noruega e do Reino Unido. Seguiram sobre o Oceano Atlântico até Gibraltar e entraram no mar Mediterrâneo rumo leste até a Síria.

- http://www.aereo.jor.br/2015/11/20/ataque-a-siria-com-tu-160-serviu-de-recado-para-o-ocidente-tambem/.

O caça multifunção de superioridade aérea Su35S (FlankerE), superior à maioria dos caças ocidentais, também foi utilizado pela Rússia na Síria.

Em setembro de 2015, a Rússia enviou para a Síria o maior submarino do mundo, o Dmitri Donskoy (TK-208), com 200 armas nucleares, com um alcance de 10.000 km.

Em 2015 a Rússia completou a construção de infraestruturas da base marítima na península de Kamchatka, de onde poderão ser baseados submarinos do tipo Borei, dos quais até 2020 terão 8 submarinos deste tipo.

Em dezembro de 2015, ocorreu mais uma etapa da cooperação técnico-militar entre a Rússia e a China. Foi firmado um acordo bilateral de venda de 24 aviões Su-35 de geração 4++. Antes a Rússia já forneceu à China aviões Su-27, sistemas de defesa aérea S-400 e S-300, mísseis antiaéreos Buk e submarinos a diesel da classe Lada.

"Já a China vem se equipando de uma marinha de guerra e mísseis capazes de expulsar a 7ª frota americana do Pacífico. Assim como a

> Rússia na Ucrânia, na Geórgia e na Síria, a China tem contado com a força e praticado a política do fato consumado. Com a ambição de estender sua soberania para todo o mar do Sul da China, ela vai se apropriando de ilhotas de propriedade controversa e as transforma em minibases militares. Em seu entorno imediato, Pequim pretende mostrar que ela é a potência suserana, e não mais os Estados Unidos." (http://noticias.uol.com.br/internacional/ultimas-noticias/le-monde/2015/10/24/russia-china-e-obama-ja-perceberam-que-eua-nao-e-mais-uma-hiperpotencia.htm).

A China e a Rússia, em setembro de 2016, realizaram exercícios militares conjuntos ao largo de Guangdong (Mar do Sul da China). Em maio de 2015 as marinhas russa e chinesa treinaram no mar Mediterrâneo. O regime chinês testou recentemente um míssil antissatélite.

- http://www.revistaencontro.com.br/app/noticia/atualidades/2016/03/17/noticia_atualidades,156415/militares-americanos-dizem-que-russia-e-china-preparam-guerra-espaci.shtml.

A China já lançou o seu primeiro navio porta-aviões e outro mais moderno está quase pronto. O Japão fez o mesmo em resposta.

- http://g1.globo.com/mundo/noticia/porta-avioes-chines-navega-no-pacifico-para-exercicios.ghtml;
- http://www.jn.pt/mundo/interior/porta-avioes-chines-realiza-primeiras-manobras-com-fogo-real-5555594.html;
- http://noticias.uol.com.br/ultimas-noticias/reuters/2016/12/26/porta-avioes-chines-chega-ao-mar-do-sul-da-china-em-meio-a-aumento-de-tensoes.htm.

Atualmente apenas dez países mantêm algum tipo de porta-aviões: Estados Unidos, Reino Unido, França, Índia, Rússia; sendo que Espanha, Brasil, Itália e Tailândia possuem porta-aviões de médio ou pequeno porte, que podem ser utilizados como navios porta-helicópteros. A Marinha da China passou a integrar esse seleto grupo em 2012 com a reformulação do porta-aviões Liaoning, antigo Varyag da URSS. O Japão possui porta-helicópteros que podem operar aviões de pouso e decolagem vertical, funcionando como se fossem porta-aviões de pequeno porte. Batizado com o nome do ex-presidente Gerald Ford, CVN-78 é o primeiro de uma nova

classe de porta-aviões nucleares dos Estados Unidos, responsáveis por levar o poderio militar do país a qualquer ponto do planeta.

Em 01/07/2016, durante a reunião solene dedicada ao 95º aniversário da fundação do Partido Comunista Chinês, o presidente Xi Jinping disse: “O mundo está à beira de uma mudança radical. Vemos como a União Europeia está gradualmente entrando em colapso, como está a economia dos EUA. [...]. Está tudo acabado para a nova ordem mundial. Assim, ele [o mundo] nunca mais será como era antes; em 10 anos teremos uma nova ordem mundial na qual a chave será a união de China e Rússia." Na verdade, o presidente Xi quer ir além de uma mera aliança econômica e política para uma aliança político-militar; capaz não só de suportar os desafios do futuro, mas também de assumir a liderança no caso do colapso da ordem mundial existente.

A Rússia, há tempos, fechou acordo com a China para aumentar o percentual das trocas comerciais entre os dois países realizadas em rublos ou yuans. Nada de dólar. O Iraque serviu de exemplo para quem tentasse abandonar a moeda americana. Mas Irã, Síria, Venezuela e Coreia do Norte fizeram o mesmo, mas não sofreram o mesmo destino que o Iraque. E são os grandes inimigos de Washington.

> "Energia e dólares estão na base de grandes disputas e conflitos. A maior reserva mundial de gás natural foi descoberta em uma área que liga Qatar e Irã. O governo iraniano fechou acordo com Iraque e Síria para construir um gasoduto e levar o combustível à Europa. O gasoduto da amizade, para uns, ou o gasoduto islâmico, para outros. Submetido a um embargo econômico desde 2002, o Irã precisa de uma saída para vender o gás que até recentemente trocava por ouro como forma de fugir das sanções. Mas Washington eliminou essa saída também barrando as trocas com metais preciosos.
>
> A saída do Irã é se juntar aos vizinhos e para isso tem o apoio da Rússia e da China. Dois países que têm todo o interesse de criar alternativas aos domínios econômicos dos Estados Unidos. Putin, me parece, está bem mais investido nesta guerra do que no conflito armado na Ucrânia." (http://brasileconomico.ig.com.br/mundo/informe-new-york/2014-08-18/russia-busca-alternativas-ao-petrodolar.html).

Em meados de 2015, a operação Tridente Juntura, maior exercício militar da Otan em mais de uma década, teve como objetivo treinar as forças da aliança para combater ameaças reais vindas do sul da Europa e uma ameaça percebida vinda do Leste; isto é, da Rússia.

- http://www.jornal.ceiri.com.br/otan-realiza-maior-exercicio-militar-no-leste-europeu-desde-guerra-fria/.

Em outubro de 2016, num artigo para a CNN (*Cable News Network*), o general sênior do Exército Britânico e ex-vicecomandante supremo aliado na Europa, Sir Richard Shirreff, afirmou que o Ocidente enfrenta a maior ameaça da Rússia desde a Guerra Fria e que Vladimir Putin pretende "restabelecer o *status* da Rússia como uma das grandes potências do mundo", marchando para os Estados bálticos da Letónia, Lituânia e Estónia.

- http://edition.cnn.com/2016/10/21/opinions/russia-aggression-nato-shirreff-opinion/;
- http://www.infowars.com/top-british-general-warns-of-nuclear-war-with-russia/.

Rússia e EUA estão perto de um choque cataclísmico, advertiu o chefe do MI6, Sir John Sawers.

Segundo o artigo recém-publicado do site analítico *What They Say About USA* (O que dizem sobre os EUA), a Rússia está vencendo os EUA em todos os aspectos da agenda internacional.

- http://whattheysayaboutusa.com/military/20151206/107929/us-power-decline.html;
- http://www.carosamigos.com.br/index.php/politica/8185-fim-da-farra-tio-sam;
- https://br.sputniknews.com/americas/201609186350000-eua-guerra-com-russia/.

As sanções contra a Rússia por conta da Ucrânia estão surtindo efeitos negativos na Europa. Explica-se. A Alemanha é a maior parceira comercial da Rússia na UE e é a principal economia do grupo. Se a Alemanha sofre, arrasta com ela toda a Europa. Ainda mais, a Rússia suspendeu a compra de

alimentos dos países que aderiram a tais sanções e já está ampliando o comércio com outros parceiros, como o Brasil, para substituir o que comprava da Europa.

Em outubro de 2016, houve um alarde na Imprensa / Mídia britânica: "Os russos estão chegando".

- https://www.thesun.co.uk/news/1999495/vladimir-putins-nuclear-warships-pictured-steaming-towards-the-english-channel-as-royal-navy-prepares-to-scramble-fleet/;
- https://www.thesun.co.uk/news/2013780/royal-navy-pledges-to-man-mark-vladimir-putins-navy-as-russians-begin-ten-ship-pincer-move-on-the-english-channel/;
- http://www.express.co.uk/news/uk/723691/Russia-warships-near-UK-Putin-flotilla-sailing-Channel-Dover.

Tratou-se da divulgação de uma frota marítima militar russa, através do Canal da Mancha, com destino à Síria. O porta-aviões russo Almirante Kuznetsov (*Admiral Kuznetsov*) pode transportar mais de 50 aeronaves.

- http://www.semprequestione.com/2016/10/urgente-russia-movimenta-o-maior.html#.WBeo0vkrKM9;
- http://sicnoticias.sapo.pt/pais/2016-10-24-Frota-russa-na-costa-portuguesa.

O avião-radar A-100 russo, supera seus rivais. Outros "brinquedinhos" russos são: Tu-160, "O Retalhador"; Tupolev (Tu-22M3 Backfire), o “assassino de porta-aviões”; e, Tupolev Tu-95, "O Urso".

Os russos possuem uma estação de alerta antecipado (Voronezh-DM) do sistema de alerta de mísseis, situado no território da região de Kalininegrado (que faz fronteira com a Lituânia e a Polônia).

A instalação dos mísseis russos Iskander perto de Kaliningrado, violam às cláusulas dos acordos estratégicos entre a OTAN e a Rússia.

O Tochka (Point)-U é um sistema de mísseis móvel, projetado para lançar ataques precisos sobre alvos táticos, como postos de controle, pontes, instalações de armazenamento, concentrações de tropas e aeródromos. A versão modernizada do Tochka-U, que pode transportar ogivas nucleares,

biológicas ou químicas, tem um alcance máximo de ejecção de até 185 quilômetros.

A “Bomba Tsar” (chamada oficialmente de AN602), criada em 1961 por cientistas soviéticos, é a bomba atômica mais potente do mundo; é cerca de 3 mil vezes mais potente que a bomba de Hiroshima.

No dia 25/10/2016, a Rússia mostrou ao mundo as primeiras imagens do míssil nuclear RS-28 Sarmat, apelidado de Satã 2, que pode viajar por longas distâncias e tem força para destruir uma área gigantesca; pode dizimar uma área equivalente à França ou cerca de duas vezes maior que a do Reino Unido. Até 2020 o Satã 2 estará em operação.

Os primeiros exemplares de armas radioeletrônicas baseados em novos princípios físicos, que não têm análogos no mundo, foram desenvolvidos e testados com sucesso na Rússia, durante a exibição militar ArmHaitek 2016. Essa arma neutraliza o equipamento do inimigo através de fluxos de energia dirigida. Trata-se da bomba de pulso eletromagnético (EMP).

A Rússia está lançando uma ampla gama de máquinas robóticas inovadoras para otimizar o desempenho de suas forças armadas em 2016. A expectativa é de que na próxima década as plataformas robóticas e de controle remoto sejam responsáveis por cerca de 30% do poder de combate da Rússia, além de dezenas de sistemas robóticos terrestres baseados no mar, bem como centenas de veículos aéreos não tripulados utilizados pelos militares russos.

Os russos dispõem de um sistema de interferência de comunicações que é capaz de deixar a OTAN totalmente surda e cega.

A Rússia projeta um avião não tripulado para detectar e destruir aviões furtivos como os F-22, F-35 e B-2.

O setor militar russo ganhou uma rede de computadores segura que não está conectada à internet global. A rede recebeu o nome de "Segmento Fechado de Transferência de Dados" (ZSPD, na sigla em russo).

Atualmente, os russos podem, efetivamente, mobilizar 30 mil homens e mil tanques em um mesmo lugar, muito rapidamente. Mas, em poucos anos (até 2024), uma frota de aeronaves de transporte pesado será capaz de mover uma unidade estratégica de 400 tanques Armata ou 900 veículos blindados leves como o SprutSD, ambos com munição, para qualquer lugar do mundo. E, provavelmente, a uma velocidade hipersônica, permitindo a Rússia, montar uma resposta militar global. O avião de transporte PAK-DA, possui capacidade de 200 toneladas de carga, alcance de 7.000 quilômetros e velocidade de até 2.000 km/h. A única aeronave que opera com uma carga comparável é o Antonov An225 Mriya (até 250 toneladas), mas este é um avião único criado especialmente para o programa do ônibus espacial soviético Buran. O PAK-DA, capaz de viajar para qualquer lugar do mundo em apenas quatro horas e ainda lançar ogivas nucleares a partir do espaço. O primeiro modelo do PAK-DA poderá começar a voar até 2020.

Para 2020 as forças armadas russas contarão com 2.300 Armata T-14 operativos.

Com o desenvolvimento de uma rede de bases militares no Oriente Médio, América Latina e no Sudeste Asiático, que estão previstas para serem concluídas até 2024, é óbvio que a Rússia está se preparando para um confronto militar em grande escala, e de escala transcontinental.

Atualmente existem bases militares russas nas ilhas da Nova Sibéria, Terra de Francisco José, no arquipélago Severnaya Zemlya, bem como no arquipélago de Novaya Zemlya, no cabo de Otto Schmidt, na ilha de Wrangel e na região do Ártico. Ainda está projetando na Venezuela, Síria, Cuba e Vietnã. Forças russas e venezuelanas realizam exercícios conjuntos desde 2008.

A Marinha da Rússia vai transformar suas instalações no porto de Tartus, noroeste da Síria, em uma base naval russa permanente. A Rússia tem uma base aérea em Hmeimim, perto de Latakia, desde o fim de agosto de 2015.

No dia 12/10/2016, Vladimir Putin anunciou na TV Russa que a Terceira Guerra mundial já começou. E, o canal de notícias Rossia 24, exibiu uma

reportagem sobre a preparação de abrigos antinucleares em Moscou.

- http://brasildebate.com.br/rumo-a-terceira-guerra-mundial/.

O governo russo iniciou em outubro de 2016, um mega exercício militar de resposta a um eventual ataque nuclear.

- http://www.sabado.pt/mundo/europa/detalhe/40_milhoes_de_russos_preparam_se_para_guerra_nuclear.html.

A preocupação dos russos é tanta que o país decidiu desenvolver uma nova aeronave de controle aéreo avançado, que seria utilizada no caso de toda infraestrutura em solo ser destruída por uma guerra nuclear.

Segundo um artigo publicado pelo site israelense Mako.co.il, o fortalecimento da presença militar da Rússia no Oriente Médio preocupa Israel, de modo que um conflito armado entre os dois países é uma questão de tempo.

- https://russian.rt.com/inotv/2016-10-31/Mako-Konflikt-mezhdu-Rossiej-i.

Saiba mais sobre a corrida armamentista russa em:

- https://br.sputniknews.com/;
- http://webkits.hoop.la/home;
- http://www.voltairenet.org/mot60.html?lang=pt;
- http://averdadequeamidianaomostra.blogspot.com.br/2014/09/a-russia-nao-esta-para-brincadeira.html.

Entretanto, com a vitória de Donald John Trump à presidência dos Estados Unidos, aparentemente, as relações com a Rússia serão melhoradas.

- http://g1.globo.com/mundo/noticia/2016/11/putin-telefona-para-donald-trump-e-diz-estar-pronto-para-dialogo.html;

- http://internacional.estadao.com.br/blogs/eua-2016/putin-parabeniza-trump-e-espera-mudanca-na-relacao-russia-eua/;

- http://veja.abril.com.br/mundo/putin-parabeniza-trump-e-defende-melhora-nas-relacoes-bilaterais/;

- http://istoe.com.br/putin-parabeniza-trump-por-vitoria-e-espera-dialogo-construtivo/.

Mas, não se deve esquecer que uma coisa é um elogio e outra é a política. Também há muita diferença entre palavras ditas em campanha eleitoral ou como mero cidadão e atitudes de um Presidente da República. Por fim, inquestionavelmente, os interesses geopolíticos dos EUA e da Rússia são fundamentalmente opostos; salvo se resolverem dividirem o mundo.

VALOR DO OURO

O investimento em ouro (*gold*) faz parte do grupo dos mercados de risco; vez que suas cotações variam segundo a lei da oferta e da procura. Entretanto, o ouro é aceito no mundo inteiro e a sua liquidez é alta.

No mercado internacional, os principais centros que negociam ouro são Londres (Inglaterra) e Zurique (Suíça) onde o ouro é negociado no mercado de balcão e não via bolsas. Outro grande centro mundial de negociação em ouro é a Bolsa de Mercadorias de Nova Iorque (NYMEX - *New York Mercantile Exchange*); através da COMEX; na qual negocia-se contratos futuros desta *commodity* (*Commodity Futures Price Quotes For Gold*). Anteriormente conhecida como o *Commodity Exchange Inc.*, a COMEX se fundiu com a Bolsa Mercantil de Nova Iorque em 1994 e tornou-se a divisão responsável pelo comércio de metais (ouro, prata, cobre, alumínio, etc.).

- http://www.marketswiki.com/wiki/NYMEX_Gold_Futures
- http://www.cmegroup.com/company/nymex.html
- http://www.wikinvest.com/wiki/Commodities_Exchange_(COMEX)

O CME Group (*Bolsa de Chicago* - http://www.cmegroup.com/) é a empresa controladora das seguintes Bolsas americanas: *Chicago Mercantile Exchange* (CME), *New York Mercantile Exchange* (NYMEX), *Chicago Board of Trade* (CBOT) e *Commodities Exchange* (COMEX).

As cotações do ouro neste mercado são baseadas em relação à onça troy, que equivale a 31,104 gramas. Já no Brasil, o maior volume de comercialização de ouro se faz através da BM&F - Bolsa de Mercadorias e Futuros (http://www.bmfbovespa.com.br/) e a cotação é feita em reais por grama de ouro puro. Desse modo, basta dividir a cotação do dia em dólares por 31.1 e multiplicar pelo preço do dólar no país em que se está e obterá o valor de um grama de ouro puro ou 24 quilates.

- http://www.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/commodities/cotacoes-de-ouro.htm.

Uma onça (abreviada: oz, da antiga palavra italiana *onza*, agora escrita *oncia*) é uma unidade de medida de massa, com dois valores diferentes, dependendo do sistema que é utilizado:

No sistema *avoirdupois* (usado para pesar objetos em geral) uma onça equivale a 28,349523125 gramas.

No sistema *troy* (relativo a metais preciosos e gemas, assim como medicamentos) a onça vale 31,1034768 gramas.

1 grama = 0,03215 *onças troy*
1 onça troy = 31,1035 gramas
1 quilo = 32,151 onças troy
1 tonelada métrica = 32.151 *onças troy*
100 onças troy = 3,11 quilos (contrato Comex, Nova Iorque)
400 onças troy = 12,44 quilos (barra *Good Delivery*, Londres)
1 Tael (Hong Kong) = 1,193 *onças troy*

Tradicionalmente, o ouro ganha maior evidência em períodos de crise econômica. O metal amarelo é tipicamente considerado um refúgio para os investidores em tempos de incertezas; pois pode ser utilizado como uma reserva de valor amplamente aceita, quando os investidores perdem a confiança nas demais comódites (*commodities* ou *comoditys*), no mercado de ações e no mercado de câmbio.

Como o preço desse metal varia com base nos fatores de oferta e procura, quando o mercado volta a se estabilizar, aplicações mais práticas e rentáveis atraem os investidores e ele pode sofrer desvalorização. Por causa desta volatilidade, é importante entender bem como funciona o investimento antes de entrar nesta aplicação.

Portanto, em momentos de estabilidade econômica, os investidores tendem a vender o ouro e diversificar o portfólio (inventário, cesta ou coleção) de aplicações, em busca de mais rentabilidade. Com mais ouro em oferta, a cotação cai. O contrário acontece em cenários de crise, quando há mais procura por ouro e, assim, o preço sobe.

Por exemplo, quando o ouro atingiu o pico em 1980, refletiu um medo prevalente de inflação, na esteira da crise do petróleo de 1979 a uma política monetária norte-americana que não tinha credibilidade. O caso para o ouro como um *hedge* (cobertura ou proteção) contra a inflação era persuasivo.

Desse modo, em 1979 e 1980, a falta de confiança na capacidade do governo para restringir a expansão da oferta de dinheiro dos investidores resultou em pânico a compra de metais preciosos como um *hedge* (proteção) contra a inflação. Os preços do ouro subiram, e em janeiro de 1980 o preço do ouro atingiu um recorde de US $ 850 por onça. Durante o período de quatro anos 1976-1980, o preço do ouro subiu mais de 750%.

O preço do ouro é normalmente entendido mundialmente como inversamente proporcional ao dólar. Quando o dólar cai o preço do ouro tende a subir. Mas tem havido muitos casos, quando o preço do ouro não acompanha as mudanças no valor do dólar, ou mesmo ia contra ele.

Assim, em regra, a cotação do ouro tende a subir quando o dólar cai e vice-versa. Quando investidores internacionais compram ouro, o dólar é vendido e isso leva à diminuição do valor da moeda americana. Como consequência, a grande procura pelo ouro faz seu preço subir. Se a inflação sobe, porque tem muito dinheiro no mercado, o ouro naturalmente a acompanha. Logo, é uma boa proteção contra o efeito corrosivo da inflação em tempos incertos. Já quando os governos têm controle da situação, existem poucas justificativas para investir em ouro.

Desde 1919, após a Primeira Guerra Mundial, o preço do ouro é definido pela *London Gold Market Fixing*, em Londres. Os maiores intermediários de ouro do mundo, os bancos Barclays, HSBC, Nova Scotia e Société Générale, informavam duas vezes ao dia, por meio de uma conferência privada, de cerca de 10 (dez) minutos, a que taxa pretendem comprar ou vender para clientes ou adquirir para suas próprias contas.

O preço do grama do ouro, portanto, é definido pela fixação de ouro (Fix Ouro ou Londres Ouro Fixação) através da *The London Gold Market Fixing Ltd.* (atualmente *The London Bullion Market Association*), duas vezes por

dia, às 10:30 GMT e 15:00 GMT (10h30 e 15h00 pelo horário de Londres); antes era através de conferência telefônica (*conference-call*), mas atualmente é de forma eletrônica, que os membros (*traders*) da Piscina/Mina de Ouro de Londres (*London Gold Pool*) se contatam para resolver os contratos entre os membros do mercado do ouro em Londres, fixando o preço do ouro (*gold fixing*) em todo o mundo.

Segundo as regras da *London Gold Market Fixing*, cada representante dos cinco maiores intermediários da matéria-prima declara o número de barras de ouro que está disposta a vender ou a comprar nesse dia ao preço de referência em uso. A negociação começa e o preço vai variando até que a disponibilidade de barras de ouro caia abaixo das 50. É então fixado o preço de referência para o novo período. A gestão do preço final é, depois, apurada por bancos de perfil mundial: Barclays, Bank of China, Goldman Sachs, HSBC Bank EUA, JPMorgan Chase, Morgan Stanley, Société Générale, Standard Chartered, Scotia-Mocatta, Toronto-Dominion Bank e UBS.

A *London Gold Pool* é a conjugação de reservas de ouro por um grupo de oito bancos centrais nos Estados Unidos e sete países europeus que concordaram em 01/11/1961 na manutenção do sistema de Bretton Woods de prefixados de moedas conversíveis e defender um preço de ouro de US $ 35 por onça troy por intervenções no mercado de ouro de Londres.

A primeira fixação do preço do ouro ocorreu em 1919. As reuniões eram mantidas em uma sala com painéis de madeira no escritório da Rothschild em St. Swithin's Lane (em Londres, Inglaterra) até que em 2004 o processo foi substituído por uma conferência telefônica. Os negociantes que se reuniam na sala portavam, cada um, pequenas Union Jacks, a bandeira do Reino Unido (Inglaterra), para sinalizar a necessidade de alterar as ordens.

O ouro foi o último metal precioso a deixar de lado a fixação de preços em Londres depois que a prata, a platina e o paládio abriram caminho para os democráticos leilões eletrônicos em 2014.

- https://www.lme.com/en-gb/pricing-and-data/pricing/official-price/

- http://pratapura.com/2014/05/21/o-comeco-do-fim-da-manipulacao-da-cotacao-dos-metais-preciosos/

O *LBMA Gold Price* (http://www.lbma.org.uk/) foi lançado em 20/03/2015 para substituir o antigo *Fix London Gold* (http://www.goldfixing.com/ já fora do ar).

Há doze participantes do preço que foram acreditados para contribuir para a LBMA Gold Price: Barclays Bank, o Bank of China, China Construction Bank, Goldman Sachs International, HSBC Bank EUA NA, JP Morgan, Morgan Stanley, Société Générale, Standard Chartered, The bank of Nova Scotia - ScotiaMocatta, The Toronto Dominion bank e UBS.

Estima-se que os estoques de ouro acima do solo representam um volume total de aproximadamente 160 mil toneladas, das quais mais de 60% foi minado desde 1950. Todo o ouro já extraído formariam um cubo medindo 20 metros (19 metros) de cada lado.

Nos últimos 6.000 anos, mais de 125.000 toneladas de ouro já foram extraídas no mundo, sendo que 112.500 toneladas (90% do total) foram extraídas a partir de 1848. Estima-se que 60% (75 mil toneladas) deste total esteja concentrado em bancos estatais e governos. Aproximadamente 34.000 toneladas (algo em torno de US$ 400 bilhões) são usados como reserva dos governos. Atualmente, a produção mundial de ouro é de aproximadamente 2.500 toneladas.

O estoque de ouro na superfície aumenta a uma taxa relativamente constante de cerca de 1,7% ao ano. Durante os últimos 50 anos, o maior aumento anual foi de 2,1% e o menor aumento foi de 1,4%.

A China é a líder mundial em produção de ouro, posição que passou a ocupar em 2007, quando ultrapassou a África do Sul, até então maior produtora do metal no mundo. Os chineses estão apostando fortemente nos preços do metal precioso, já que a produção vem caindo no resto do mundo, com o maior declínio sendo registrado na África do Sul. Assim, a expectativa da China é que os preços do ouro continuem subindo nos próximos anos, embora tenha se registrado uma queda na demanda de alguns grandes países consumidores, como Índia, Turquia e outras nações do

Oriente Médio. Além da China, figuram como grandes produtores da comódite (*commoditie* ou *commodity*) ouro a África do Sul, Austrália, Estados Unidos e Peru.

O único maior detentor de ouro do mundo é o governo dos Estados Unidos, com 8.133,5 toneladas. Em novembro de 2009, esta oferta ouro valia cerca de 330.000 milhões dólares. Outros principais detentores de ouro incluem a Alemanha, o Fundo Monetário Internacional (FMI), Itália, França, SPDR Gold Shares, China, Suíça, Japão e Holanda.

Recentemente, a China e a Rússia ampliaram suas reservas em ouro em aposta contra o dólar (http://www.correiodobrasil.com.br/china-e-russia-ampliam-reservas-em-ouro-na-aposta-contra-o-dolar/).

O preço do ouro no Brasil se determina pelas cotações internacionais (bolsas de valores de Nova York [COMEX] e Londres) e, principalmente, pelo dólar norte-americano. A moeda norte-americana subiu 48,49% frente ao real em 2015. Ou seja, o grama do ouro, negociado em dólar, passou a custar mais caro em real. Em momentos de estabilidade econômica, os investidores tendem a vender o ouro e diversificar o portfólio de aplicações, em busca de mais rentabilidade. Com mais metal em oferta, a cotação cai. O contrário acontece em cenários de crise, quando há mais procura por ouro e o preço sobe.

- http://www.brazilpoliticalcomment.com.br/index.php/doze-razoes-para-investir-em-ouro-hoje/.

Saiba mais sobre o ouro no capítulo "DA MOEDA MUNDIAL CONTEMPORÂNEA".

INVESTIMENTOS EM OURO

Quem decide investir em ouro precisa estar ciente de que perde dinheiro sempre que o dólar cai (desvaloriza) em relação ao real (moeda brasileira).

O ouro negociado no Brasil é 0,999; ou seja, por exemplo, a cada contrato de 250 gramas na verdade se está comprando 249,75 gramas de ouro. O restante são impurezas. Pode haver também outros níveis de pureza à venda; por isso é sempre bom estar atento ao que se está comprando.

No Brasil, para as aplicações em ouro iguais ou menores a R$ 20.000,00 (vinte mil reais), não há incidência do Imposto de Renda. Acima deste valor, a alíquota é de 15% (quinze por cento). Saiba maiores detalhes no capítulo "TRIBUTAÇÃO SOBRE OURO, AÇÕES E RENDA VARIÁVEL".

O ouro foi o melhor investimento brasileiro no primeiro mês de 2016. O preço do metal marcou alta de 7,38% em janeiro desse ano. Já a segunda melhor aplicação foi o título do Tesouro Direto, Tesouro IPCA+, com vencimento em 2019: desempenho positivo de 3,83%. O terceiro melhor investimento do mês foi outro título do Tesouro Direto, o Tesouro IPCA+ com Juros Semestrais com vencimento em 2020. A alta do título foi de 3,01% em janeiro.

- http://www.tesouro.fazenda.gov.br/tesouro-direto.

O ouro percorre um caminho longo até ser negociado na Bolsa. Depois da extração, ele é refinado e transformado em barras. Elas são lacradas e embaladas e só então são entregues a uma instituição financeira. Estas instituições são bancos credenciados pela BM&F, que mantêm as barras de ouro sob custódia, armazenando-as em cofres gerenciados. Todo esse processo é atestado pela Bolsa.

É possível comprar barras de ouro pelo site https://goldsilver.com/, diretamente pelo http://www.ebay.com/ ou através do APMEX (http://www.apmex.com/) e, até mesmo, pelo http://www.mercadolivre.com.br/ e http://pt.aliexpress.com/. Também pode-se comprar em joalherias, ourives, casas de câmbio e em bancos.

- http://comprarevenderouro.com/como-vender-ouro-no-ebay/;
- http://www.jornaldenegocios.pt/mercados/detalhe/ebay_satisfaz_fome_de_ouro.html.

Pelas ruas é possível ver placas, cartazes e "homens-sanduíche" anunciando compra e venda de ouro. Muitas vezes os preços de negociação do metal podem parecer mais interessantes que os cobrados pelas empresas autorizadas pelo Banco Central (http://www.bcb.gov.br/pt-br/) e pela Comissão de Valores Mobiliários (http://www.cvm.gov.br/) a realizar esse tipo de transação. No entanto, o risco do investidor também é muito maior. Não há como saber se o ouro passou por um processo de purificação na fundidora e nem se possui certificado de autenticidade. Esse tipo de transação, portanto, só deve ser realizada se o investidor conhecer a origem do metal.

Comprar joias feitas de ouro também é uma forma de investir no metal; já que as peças tendem a se valorizar se as cotações subirem. No entanto, é preciso atestar que as joias são 100% (cem por cento) feitas de ouro, já que é muito comum a mistura de outros metais. Dentro da joalheria, o preço da joia também embute o valor do trabalho do joalheiro; nem sempre será possível repassar esse custo no mercado secundário. Tanto joias quanto barras de ouro podem ser penhoradas caso seus proprietários precisem temporariamente de dinheiro para arcar com outras despesas; ou seja, quem possui joias ou barras de ouro pode utilizar o penhor como forma de capitalização. A operação é muito mais vantajosa do que um empréstimo pessoal, por exemplo, já que o próprio objeto (a joia) serve como garantia do empréstimo feito a partir da penhora. As operações de penhor no Brasil estão concentradas na Caixa Econômica Federal.

- http://www.caixa.gov.br/voce/credito-financiamento/penhor/Paginas/default.aspx.

No mercado informal, a compra e a venda do ouro são feitas em locais não autorizados pelo Banco Central. O risco é grande, já que não se pode garantir a origem do ouro, se passou pelo processo de purificação ou se possui certificado de autenticidade. A compra de joias também é uma opção, desde que tenham garantia de procedência.

Também é possível comprar frações de barras de ouro, que permanecem armazenados em cofres através do serviço de algumas empresas específicas. Como cada barra de ouro padrão possui 400 oz, o seu valor torna seus acessos e liquidez muito restritos. A venda de frações permite aos investidores com menor patrimônio acumularem o metal.

Uma dica é que a Caixa Econômica Federal, em razão do serviço de penhor, costuma realizar leilões. É possível acessar ao catálogo e com isso saber de antemão os ativos que pretende arrematar.

- http://www11.caixa.gov.br/portal/public/sievj/overview/vitrine_de_joias.

A compra e a venda de ouro em barras podem ser feitas no chamado **mercado de balcão**, por meio de agências das instituições financeiras especializadas (bancos, corretoras, distribuidoras), nas fundadoras ou nas empresas de mineração.

Os negócios realizados em Mercado de Balcão são aqueles que acontecem fora do ambiente de negociação eletrônica e de pregão. É basicamente um mercado em que as partes acordam entre si as taxas, prazos e condições de seus contratos.

Comprar ouro no balcão é como comprar dólar na casa de câmbio: não há uma taxa de corretagem. O lucro da corretora vem do *spread* (diferença) entre o preço que ela paga pelo metal e aquele pelo qual o revende ao investidor. A desvantagem é que, geralmente, o ouro comprado no balcão tem entrega física; ou seja, a pessoa sai da instituição com alguns gramas de ouro consigo. Para compensar o risco de ser assaltado e perder o investimento, o aplicador precisa se preocupar com a contratação de seguro e aluguel de um cofre em algum banco, por exemplo, para guardar seu patrimônio. Se quiser vender o metal, terá de transportá-lo novamente até a corretora especializada. A vantagem é que o pagamento é feito à vista, no mesmo dia, em vez de no dia seguinte. O Imposto de Renda segue as mesmas regras do ouro negociado na BM&F.

O mercado de balcão é a maneira menos burocrática de se adquirir ouro físico no Brasil. Esse tipo de operação, na maioria das vezes, é realizada por telefone. Ao concretizar a liquidação do pagamento, via boleto bancário, o comprador terá duas opções: deixar o ouro custodiado em uma instituição bancária credenciada de sua escolha ou levar consigo a quantidade adquirida.

A compra também pode ser realizada através de sites (http://www.grupofitta.com/, http://www.ourominas.com/, etc.), que fazem inclusive o serviço de entrega. Estas empresas normalmente garantem a recompra deste ouro, desde que não seja violado o lacre da barra. Explica-se. O ouro vem embalado com um lacre e, caso se retire o lacre, há o custo de recertificação, que é passado pela fundidora.

Alguns locais **onde se pode comprar ouro**:

- https://goldsilver.com/;
- http://www.parmetal.com.br/;
- http://www.grupofitta.com/;
- http://www.ourominas.com/;
- http://www.reservametais.com.br/;
- http://www.taticaouro.com.br/to/;
- http://www.marsam.com.br/produtos.asp;
- https://www.bancopaulista.com.br/Conteudo/Produtos_Ouro.aspx;
- http://www.dillon.com.br/produtos/ouro.html;
- http://maximeoro.com.br/pag-a-empresa-11;
- http://www.goldbex.com/web_pt/plans.php;
- https://www.bullionvault.com/;
- http://www.royalmint.com/;
- http://globalintergold.com.br/;
- https://www.worldsilver.com.br/;

- http://pt.wikihow.com/Comprar-Ouro.

Outra vantagem é que desta maneira o ouro físico pode ser adquirido em pequenas quantidades.

Portanto, quem não tem cerca de R$ 39.000,00 (trinta e nove mil reais) para investir em ouro ou não quer abrir conta em corretora também pode adquirir barras do metal com entrega física. As duas principais distribuidoras de ouro no Brasil são a OM DTVM (http://www.ourominas.com/) e a Marsam DTVM (http://www.marsam.com.br/). As empresas cobram um ágio de cerca de 1% do valor do ouro negociado na BM&FBovespa para realizarem a entrega física do metal. O ouro pode ser adquirido tanto em lojas dessas empresas como ser comprado pela Internet. A entrega, nesse segundo caso, pode ser feita pelos Correios (até R$ 10.000,00 com seguro) ou por motoboy (o seguro e a entrega costumam custar 1% do valor adquirido). As empresas possuem barras de ouro de diversos pesos. A OM DTVM permite até a entrega da barrinha de ouro em cartões customizados - como do time de futebol do coração. A responsabilidade por guardar o ouro em algum lugar seguro é do comprador. As barras também podem ser custodiadas exclusivamente pelo Banco do Brasil (mas somente para múltiplos de 250 gramas e com a cobrança de uma taxa mensal). Quando o investidor quiser se desfazer do metal, tem a garantia de recompra da própria empresa que lhe vendeu as barras, mas também há um pequeno deságio em relação à cotação da BM&FBovespa.

A pouco tempo atrás, ocorreu a promoção “Marcas campeãs” (https://www.promocaomarcascampeas.com.br/), na qual, dentre outros prêmios, haviam certificados de barras de ouro da Ourominas (http://www.ourominas.com/).

Para quem quer sentir-se mais protegido, o metal pode ser custodiado exclusivamente pelo Banco do Brasil, com cobrança de uma taxa mensal.

A desvantagem desta modalidade (mercado de balcão) é que o preço cobrado é cerca de 10% (dez por cento) mais alto que o da maneira mais

burocrática; e o preço pago na venda também é mais baixo. Detalhe, compras acima de R$ 10.000,00 (dez mil reais) são mais burocráticas.

Dica. Só compensa comprar no mercado de balcão se a pessoa não tem recurso suficiente ou não deseja investir o montante necessário para adquirir o ouro físico na BM&F; e, ainda, se crê numa alta superior a, pelo menos, 20% (vinte por cento) no preço do que pagou.

Também há o custo do frete e do seguro do transporte (este último é de 1% da compra); bem como a despesa com uma caixa depósito no cofre de algum banco, se não sentir seguro guardar em casa.

Outra forma de comprar o ouro físico é **por meio da BM&FBovespa** (http://www.bmfbovespa.com.br/), cuja aplicação mínima é em lotes padrões de 250 gramas ou os contratos fracionários de 10g e de 0,225g, que têm preços mais acessíveis, mas têm menor liquidez.

Para comprar ouro na BM&F, o investidor deve procurar uma corretora (a qual cobra taxa) listada na Bolsa, que negocia o ouro no mercado financeiro.

- http://www.bmfbovespa.com.br/shared/iframe.aspx?altura=1100&idioma=pt-br&url=www2.bmf.com.br/pages/portal/bmfbovespa/associados1/associadosPesquisa1.asp

A Bolsa faz a cobrança da taxa de custódia e a repassa para o banco custodiante. São cobrados 0,07% ao mês, calculados diariamente sobre a posição mantida pelo investidor, de acordo com a seguinte metodologia: Taxa de Custódia ao dia = (preço máximo do ouro no dia x 0,07% x saldo em gramas) / 30 dias.

Quando negociado como ativo financeiro, o ganho de capital do ouro é isento de Imposto de Renda sempre que o valor total dos contratos não superar R$ 20.000,00 (vinte mil reais) em um único mês.

A aplicação está sujeita ainda à cobrança de taxa de corretagem, que varia de acordo com a corretora contratada. Geralmente, a taxa fica na faixa de 0,2% sobre o valor total envolvido na transação.

Há três formas de se adquirir ouro na Bolsa de Mercadorias e Futuros. A mais comum é a compra do metal no mercado à vista. Mas o investidor também pode realizar sua compra através do mercado futuro e de opções.

O mercado à vista é uma modalidade de mercado onde são negociados valores mobiliários e ouro, ativo financeiro, cuja liquidação física (entrega do ativo pelo vendedor) e financeira (pagamento do ativo pelo comprador) ocorrem, no máximo até o 3º (terceiro) dia após ao da negociação.

Uma operação *day trade* é aquela feita com um mesmo ativo, em um mesmo dia e em uma mesma corretora. Antigamente operações em um mesmo ativo e em um mesmo dia eram consideradas *day trade* independente da corretora, o que dificultava o cálculo do imposto devido em alguns casos.

Os contratos do mercado futuro permitem a compra por um determinado preço fixo, em data definida. Porém, até o vencimento, os vendedores e compradores dos contratos devem ir pagando ajustes uns aos outros dependendo se o preço do metal está subindo ou caindo.

Os contratos futuros de ouro já estiveram entre os mais negociados na BM&F. Desde o governo Collor, entretanto, as negociações de ouro veem gradativamente minguando. Mas essa opção ainda está ao alcance dos investidores brasileiros. Cada contrato negociado representa 250 gramas de ouro.

Nos contratos de opções, o investidor paga pelo direito de realizar a compra a um dado preço na data de exercício. Nos contratos de opção, o investidor não tem obrigação de comprar, ao contrário dos negócios do mercado futuro.

Diferentes contratos de ouro na Bovespa:

- Ouro à vista - http://www3.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/commodities/ouro-a-vista.htm;
- Como investir no mercado de ouro à vista - http://www.bmfbovespa.com.br/pt-br/a-bmfbovespa/download/Folheto-Ouro.pdf e http://www.bmfbovespa.com.br/pt-br/a-bmfbovespa/download/Lamina-Ouro.pdf;

- Futuro de ouro - http://www3.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/commodities/futuro-de-ouro.htm;
- Disponível de Ouro - http://www3.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/commodities/opcoes-sobre-disponivel-de-ouro.htm;
- Disponível padrão de ouro de 250 gramas (DIS OZ1) - http://www3.bmfbovespa.com.br/br/com/bvmf/internet/service/common/file/fileDownload.jsp?documentId=8A828D295048C0EF01513FF4E2C61E45;
- Disponível fracionário de ouro de 10 gramas (DIS OZ2) - http://www3.bmfbovespa.com.br/br/com/bvmf/internet/service/common/file/fileDownload.jsp?documentId=8A828D295048C0EF01513FF4E2371DCA;
- Disponível fracionário de ouro de 0,225 grama (DIS OZ3) - http://www3.bmfbovespa.com.br/br/com/bvmf/internet/service/common/file/fileDownload.jsp?documentId=8A828D295048C0EF01513FF4E2921E07;
- Futuro de ouro - http://www3.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/commodities/futuro-de-ouro.htm;
- Futuro de ouro 250 gramas (FUT OZ1) - http://www.bmf.com.br/bmfbovespa/pages/contratos1/Financeiros/PDF/Ouro_Futuro_250Gramas.pdf;
- Termo de ouro - http://www3.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/commodities/termo-de-ouro.htm;
- Emolumentos - http://www3.bmfbovespa.com.br/pt_br/servicos/tarifas/derivativos/emolumentos/ouro.htm.

Os contratos disponíveis são os negociados no mercado à vista. O fracionário é especializado em pequenas quantias. O mercado a termo tem um funcionamento parecido com o mercado futuro, no sentido de estabelecer um preço fixo e uma data de vencimento. Mas, diferentemente do mercado futuro, não exige o pagamento de ajustes diários por conta de mudanças nos preços desses contratos.

O contrato mais negociado hoje é o padrão (250 gramas) à vista (disponível). Em determinados dias, ele representa 100% (cem por cento) dos negócios fechados. O lote padrão negociado é de 249,75 gramas de ouro fino, correspondente a uma barra de 250 gramas. O teor de pureza é de 999 partes de ouro puro para cada 1.000 partes de metal.

As cotações são sempre em reais por grama, com até três casas decimais, e não há um limite de oscilação diária, exceto se, excepcionalmente, a BMF decidir fixar algum teto. A liquidação financeira (pagamento) pelo comprador será efetuada no dia útil seguinte ao da operação no pregão.

Neste tipo de contrato, são admitidas operações de compra e venda para liquidação diária (*day trade* – compra e venda feitas no mesmo dia). Elas devem, porém, ser realizadas no mesmo pregão, pelo mesmo cliente, intermediadas pela mesma corretora e registradas pelo mesmo membro de compensação.

As corretoras e distribuidoras de valores criaram diversos produtos a partir dos contratos e barras de 250 gramas, vendendo desde pequenas quantidades (1g a 10g) em cartões até laminados e barras de tamanhos e pesos diferentes, escolhidos pelo investidor. Os produtos, baseados em cotações do dia mais ágio (lucro), são padronizados, certificados e lacrados. A negociação se dá de forma bastante direta: você escolhe o produto, a quantidade de ouro desejada e faz o pagamento via boleto bancário (limite de R$ 10.000,00 – dez mil reais). O ouro é enviado pelos Correios via SEDEX com AR (Aviso de Recebimento), seguro e entregue em mãos com certificado de garantia e nota fiscal de negociação. Se quiser vender, em geral basta levar o ouro até um balcão de atendimento da corretora escolhida ou enviar o material pelos Correios e ela realizará a avaliação e recompra em até 3 (três) dias úteis.

Para investir em ouro na bolsa, a primeira medida é abrir uma conta em uma corretora de valores; porém, antes, é necessário se certificar de que esta corretora está habilitada para operar o ouro. Quando for fazer seu contrato na corretora, você terá de assinar, além do contrato que lhe permitirá negociar na bolsa, um outro que lhe permitirá negociar na BM&F. Uma vez cadastrado, o investidor requisita a compra do metal por meio da corretora.

Em síntese. Para comprar ouro pela BM&FBovespa, é necessário possuir conta em alguma corretora e enviar a ordem. Assim como acontece no mercado de ações, o investidor terá de pagar à corretora pela realização da operação e arcar com as taxas cobradas pela BM&FBovespa pela compra e custódia de qualquer ativo financeiro.

Feito isso, o contrato do ouro que lhe permite a retirada física tem um código ("ticker") na bolsa: OZ1D. Este é um contrato de 250 gramas de ouro, e é o menor contrato que permite a retirada na BM&F; ou seja, se a intenção era investir menos, esta não é uma opção, a não ser que você queira comprar apenas o certificado de 10 gramas (OZ2D) ou de 0,225 gramas (OZ3D), os quais não lhe permitem retirada (a menos que se junte 250 gramas). Existe a possibilidade de se retirar em lingotes de 100 e 400 onças do ouro, que possuem uma pureza menor que 0,999 (salvo engano, é de 0,995).

A partir da compra, o investidor tem duas opções. A primeira é deixar seu ouro guardado na BM&F ou em algum banco cadastrado pela bolsa para tanto. Quem guarda o ouro é chamado de custodiante, e cobra uma taxa por isso (a taxa de custódia); procedimento bastante familiar para quem já investe em ações. Além disso, ao adquirir o metal, o investidor também contrata um seguro (prevenção contra o roubo no banco).

A outra opção é receber fisicamente o ouro (literalmente pegar as barras). Nesse caso, o principal inconveniente é a segurança. Alguém saindo de um banco com duas ou três barras de ouro está tão ou mais sujeito a ser assaltado do que uma pessoa que sacou algumas notas de real no caixa automático. Deixar o ouro no cofre de casa também expõe o investidor ao mesmo risco de ser assaltado e ver suas joias e outros bens levados.

O outro custo envolvido na compra de ouro é o pagamento pelos serviços da corretora. Ao dar a ordem de compra, o investidor deve desembolsar um percentual do valor total envolvido na transação, de acordo com a corretora. Essa porcentagem envolve a taxa de corretagem, emolumentos e outros custos da instituição.

A compra ou a venda doouro não podem ser feitas pelo *homebroker*, mas pelo telefone. A retirada pode ser agendada através da sua corretora, a qual lhe dará maiores informações sobre o procedimento.

Pode-se também pedir o *delivery* (entrega). Para tal procedimento é necessário avisar a corretora, que avisará a BM&F e esta ao custodiante (o

Banco do Brasil). O cliente terá que fazer um cadastro junto ao custodiante (se ainda não for correntista) e ir pessoalmente à agência fazer a retirada (salvo engano, na cidade de São Paulo). Os custos da custódia sobem bastante no período em que o ouro ficar disponível para a retirada (0,3% do preço máximo do dia x número de gramas / 30 todos os dias; para não correntistas do BB, para correntistas é só substituir o 0,3% por 0,1%).

Em resumo, os **custos do investimento em ouro através da BM&FBovespa** são:

1) A **corretagem** — que varia de corretora para corretora, e;

2) A **taxa de custódia** — que é cobrada mensalmente com cálculo diário (todo o dia se adiciona a conta); através da seguinte fórmula: preço máximo do dia x 0,07% x número de gramas / 30. Caso se deseje retirar o ouro da custódia não há a opção do *delivery*, só se pode retirá-lo fisicamente. Caso sua preferência seja a de retirar o ouro da BM&F e você deseje vendê-lo novamente por lá, o processo é o mesmo: entra-se em contato com a corretora e devolve-se o ouro para o custodiante, o ouro volta a figurar entre seus ativos na BM&F e, ato contínuo, você já pode vendê-lo.

Saiba mais sobre investimento em ouro através da BM&F:

- http://www.bmfbovespa.com.br/pt-br/a-bmfbovespa/download/Folheto-Ouro.pdf;
- http://www.bmfbovespa.com.br/pt-br/a-bmfbovespa/download/Lamina-Ouro.pdf.

Qualquer que seja o caso, ao optar por deixar o ouro no banco, o investidor recebe apenas um certificado de custódia. Isso garante liquidez, segurança e facilidade nas negociações futuras

Já quem decide levar consigo o ouro adquirido terá um maior custo ao revender, além do risco de guardar o metal consigo ou num local privado. Isso porque cada vez que o ouro retorna para custódia, deve passar por uma fundidora credenciada pela Bolsa para apuração do seu teor de pureza e

confecção do lingote-padrão. Assim, precisará primeiro contratar uma empresa especializada em certificar a qualidade e a autenticidade do metal, a fim de evitar fraudes. O preço não é baixo. Na média, esses especialistas cobram 2% (dois por cento) do valor envolvido. Com o certificado de autenticidade, procura sua corretora, dá a ordem de venda e, uma vez fechado o negócio, entrega o metal em algum banco combinado.

Outra maneira de investir em ouro é através de ***Exchange Traded Funds*** (ETFs). Com ETFs se está investindo em uma mercadoria como se faria com ações, mas, ao contrário de quando se compra *bullion* (barra de ouro) diretamente, o comprador realmente não possui nenhum ouro. É uma unidade negociável na Bolsa de Valores como se fosse uma ação, mas que reúne um número variável de ações. No caso, as *Gold ETFs* (Fundos de Índices em Ouro) acompanham o preço do ouro, são negociadas em bolsa e podem ser comprados através de um corretor da bolsa. Eles são baratos, fáceis de comprar e de vender. ETFs são negociados como ações padrões.

- http://bmfbovespa.com.br/etf/fundo-de-indice.aspx?Idioma=pt-br;
- http://www.bmfbovespa.com.br/etf/ETFDetalhe.aspx?Codigo=ISUS11&idioma=pt-BR.

ETFs são fundos de índices da bolsa de valores que replicam a evolução de um determinado índice, com a particularidade de serem transacionados no mercado como se fossem ações. Por isso combinam a vantagem da diversificação, característica dos fundos de investimento, com a facilidade de negociação das ações.

Os ETFs, portanto, possuem em sua composição direitos a barras de ouro que permanecem estocadas em cofres. Cada ação de ETF representa uma quantidade de metal, seja representada em onça (oz) ou grama (gr).

No Brasil os ETFs são regulamentados pela Instrução 359/2002 da CVM - Comissão de Valores Mobiliários (http://www.cvm.gov.br/legislacao/inst/inst359.html).

Alguns **exemplos de ETFs de ouro e prata** são:

- *SPDR Gold Shares (GLD)* – É o maior ETF de ouro do mundo. Seu preço é o equivalente a 1/10 do valor de uma onça de ouro. É negociado nas bolsas de Nova Iorque, México, Cingapura, Japão e Hong Kong.

- *iShares Gold Trust (IAU)* – É negociado na bolsa de Nova Iorque (NYSE-Arca). Também é dos maiores do mundo, com estoque de quase 168 toneladas de ouro.

- *iShares Silver Trust (SLV)* – É negociado na bolsa de Nova Iorque (NYSE-Arca). É o maior ETF de prata do mundo, com estoque de mais de 10 mil toneladas de prata.

- *ETFS Physical Swiss Gold Shares (SGOL)* – É negociado na bolsa de Nova Iorque (NYSE-Arca). É lastreado por ouro 100% alocado em cofres em Zurique (Suíça).

- *ZKB Gold ETF AA USD Klasse (ZGLDUS)* – Gerenciado pelo banco suíço Zurcher Kantonalbank, é negociado na bolsa de Zurique. Investe exclusivamente em ouro 100% alocado na Suíça. É permitido ao investidor retirar as barras de ouro quando quiser. Entretanto, a unidade padrão de resgate é de 12,5kg.

Um dos cuidados que se deve ter é acompanhar se a empresa ou o ETF sofrem auditorias frequentes, para confirmar a quantidade de metal estocada e se permitem a retirada física ou entrega do mesmo.

Também é importante saber em qual país o ouro está armazenado, sendo Suíça e Cingapura, os países de melhor reputação.

Em geral, o investidor abre uma conta na empresa, faz uma transferência bancária e através do acesso online, verifica seu saldo e pode comprar e vender metais.

Há também os fundos de capital protegido, o mercado informal e a aplicação em joias. Nos fundos de capital protegido, que cobram taxa de administração, o banco paga ao investidor a variação do ouro. Nesta

aplicação, o investidor não corre o risco de perder parte do principal se a cotação cair, mas também não recebe toda a valorização do ouro.

Diversos bancos já possuem fundos de capital protegido que pagam ao investidor a variação do ouro, como o Banco do Brasil, o Credit Suisse Hedging Griffo, o HSBC e o Itaú. A grande vantagem de qualquer fundo de capital protegido é que o investidor não corre o risco de perder parte do principal se a cotação do ouro recuar (algo bem interessante em uma época de cotações elevadas). O risco, portanto, é de oportunidade: o dinheiro poderia ter sido investido em outro ativo mais lucrativo. Por outro lado, o investidor não ganhará toda a valorização do ouro se ela for muito expressiva. Outra desvantagem é que os fundos de capital protegido referenciados em ouro costumam ser oferecidos apenas aos clientes de alta renda dos bancos porque o produto visa um investidor mais sofisticado que está em busca de diversificação para seu portfólio. Por último, os fundos de capital protegido costumam permitir aportes somente na fase de captação. Encerrado esse prazo, os fundos se tornam fechados para novas aplicações.

O **Banco do Brasil** (BB) vende o metal somente aos correntistas (Ouro Lingote e Ouro Escritural) e oferece o serviço de custódia (na modalidade Lingote o custo é de 0,20% e na modalidade Escritural 0,15%, sobre o montante custodiado). Uma condição interessante oferecida pelo Banco do Brasil é a garantia de recompra do ouro vendido aos clientes. Com isso, resolve-se um ponto importante para quem carrega o metal em sua carteira de investimentos, que é a liquidez diária. Para pequenos investidores, a possibilidade de converter o ouro em dinheiro a qualquer momento é um fator determinante.

Desse modo, pelo BB é possível comprar ouro lingote ou ouro escritural. O ouro lingote é a comercialização de barras de 250 gramas, padrão da BM&FBovespa. Já o ouro escritural é a modalidade criada pelo BB para seus clientes que querem investir em ouro em quantidades múltiplas de 25g. Nos dois casos é necessário ser correntista do BB. Dessa forma seus investidores podem diversificar seus investimentos sem que sejam necessários recursos no padrão de negociação de 250g do ouro lingote.

- http://br.investing.com/commodities/gold-historical-data;

- http://www.bb.com.br/portalbb/page3,116,2137,1,1,1,1.bb?codigoMenu=1092&codigoNoticia=30853.

A Bradesco Corretora possui opções de investimentos em ouro através de operações BM&F:

- https://www.bradescocorretora.com.br/Corretora/default.aspx?vgnextoid=a378f35b47834310VgnVCM1000003e2ad70aRCRD&vgnextchannel=a378f35b47834310VgnVCM1000003e2ad70aRCRD.

O Santander oferece serviços de negociação de Futuros, Agropecuários e Ouro na BM&F.

- https://www.santander.com.br/portal/wps/script/templates/GCMRequest.do?page=6526.

A CEF (Caixa Econômica Federal) possui o investimento “Caixa FI Ouro Multimercado Longo Prazo”, que atrela o investimento feito à variação do ouro no mercado financeiro.

- http://www.caixa.gov.br/fundos-investimento/multimercado/fi-ouro-multimercado-longo-prazo/Paginas/default.aspx.

Semelhantemente, o ÓRAMA Ouro é um Fundo Passivo que segue a variação do ouro na bolsa (BM&FBovespa). Esta cotação é feita a partir do valor do dólar e do valor do ouro no mercado internacional. Sendo assim, se o dólar sobe, o valor da cotação do ouro sobe também.

- http://www.orama.com.br/como-investir-em-ouro/;
- http://www.orama.com.br/fundos-de-investimento/orama-ouro/.

INVESTIMENTOS NA BOLSA DE VALORES

Quando uma companhia se torna aberta, o patrimônio dela é dividido em várias cotas, que são distribuídas para os investidores. Para ter suas ações negociadas em mercados organizados, como as bolsas de valores, a empresa precisa se registrar como companhia aberta na Comissão de Valores Mobiliários (CVM). Portanto, uma ação representa a menor parcela em que se divide o capital de uma empresa organizada em forma de Sociedade Anônima (S.A.). Desse modo, as ações são pequenas partes (fatias, cotas, participações, etc.) de uma empresa e comprar ações significa se tornar um acionista ou um sócio da empresa.

O investidor em ações é sócio da empresa. Como sócio, tem direito a participar dos lucros da empresa e poderá ganhar dinheiro com os dividendos distribuídos; além da valorização do preço de suas ações. Mas se a empresa tiver dificuldades financeiras, os lucros tendem a diminuir e, com isso, ocorre a queda no preço da ação.

A bolsa de valores é um mercado online onde os investidores se encontram para negociar ações de empresas e outros produtos financeiros.

A bolsa de valores surgiu como um meio para as empresas captarem recursos (dinheiro) para investir em si mesmas a um custo mais barato do que conseguiriam nos bancos. Assim, as empresas vendem cotas de participação para pessoas ou empresas em troca do dinheiro delas. Por outras palavras, em razão das ações compradas, seus titulares ganham uma participação nas empresas, com o que possuem, dentre outros direitos, o de receberem parte dos lucros das respectivas empresas ganham.

As ações podem sofrer oscilações de preço. Quando há grande procura por determinadas ações, a tendência é de alta no seu valor. Já quando ocorre o inverso (pouca ou nenhuma procura) e muitos investidores vendem suas ações, o preço cai. É a chamada lei da oferta e da procura.

A principal forma de ganhar dinheiro na bolsa de valores é comprando uma ação na baixa e ganhando com a sua valorização. Esse é o foco de quase todas as estratégias de investimento e também é a que proporciona a

possibilidade de ganhos maiores. Outra forma é através dos proventos; ou seja, a cota parte do lucro da empresa que é paga aos acionistas na forma de Dividendos e de Juros sob Capital Próprio (JCP).

O acionista pode comprar e/ou vender quantas e quais ações quiser e quando bem quando entender; inclusive pode emprestar suas ações por meio do Banco de Títulos.

As ações conhecidas como *blue chips* são aquelas que apresentam maior liquidez, ou seja, as mais negociadas no mercado.

- http://www.tororadar.com.br/investimento/bovespa/blue-chip-o-que-e-acao.

No Brasil as ações são divididas em ordinárias e preferenciais, sendo que ambas devem ser nominativas; ou seja, os detentores devem ser identificados nos livros de registro da empresa.

As **ações preferenciais nominativas (PN)**, ou simplesmente ações preferenciais, exclusivas do mercado brasileiro, são aquelas onde existe uma preferência no recebimento de dividendos (participação na divisão do lucro da companhia), não dão direito a voto e possuem melhor liquidez do que as ações ordinárias. Diante disso, recebem valores maiores e são negociadas (vendidas e compradas) com maior facilidade. Já as **ações ordinárias (ON)** são aquelas que dão direito de participar das decisões da companhia (assembleia dos acionistas e conselho administrativo) e de participar, de forma não preferencial, nos resultados da empresa. Entretanto, o peso do voto é de acordo com o percentual de ações e os dividendos dados a quem tem ONs nem sempre são iguais aos dados a quem tem PNs.

Porém, mesmo com o inconveniente do acionista minoritário não ter peso ou relevância no seu voto, o titular de ações ordinárias possui um benefício denominado "tag along" (previsto na Lei das S.A., artigo 254-A); que é um mecanismo de proteção aos acionistas minoritários de uma companhia. Através do *tag along* os investidores minoritários possuem o direito de deixarem uma sociedade, caso o controle acionário da companhia seja adquirido por um investidor que até então não fazia parte da mesma. Diante disso, o novo controlador, estranho a quadro anterior, é obrigado a fazer uma

oferta pública de aquisição das ações ordinárias pertencente aos minoritários de, no mínimo, 80% (oitenta por cento) do valor pago pela aquisição das ações do grupo controlador. Nessas circunstâncias, é comum as ações ON se valorizarem acima das ações PN.

- http://www.portaldoinvestidor.gov.br/menu/Menu_Investidor/acionistas/Tag_Along.html;
- http://www.cvm.gov.br/legislacao/index.html;
- Lei das SAs (6.404/1976): https://www.planalto.gov.br/ccivil_03/Leis/L6404consol.htm.

Como o **dividendo** é a parte do lucro que as empresas distribuem para seus acionistas, só pode ser rateado depois da apuração do lucro de um exercício fiscal. Entretanto, há empresas que fazem balanços mensais, trimestrais ou semestrais.

O estatuto social da empresa pode estabelecer o dividendo mínimo a ser distribuído, desde que não seja inferior a 25% (vinte e cinco por cento) de seu lucro líquido ajustado. Mas, se o dividendo não estiver previsto no estatuto social da empresa, o dividendo obrigatório deve corresponder, no mínimo, à metade do lucro líquido ajustado.

Existem também as "**units**" (certificado de depósito de ações), que são recibos representativos de uma pequena cesta de ações da mesma empresa. Units, portanto, são ativos compostos por mais de uma classe de valores mobiliários, como uma ação ordinária e um bônus de subscrição, por exemplo, negociados em conjunto. Unit, portanto, não é uma ação, mas um pacote de classes de ativos, que pode ser formado por ações ordinárias, preferenciais, bônus de subscrição, etc. As units são compradas e/ou vendidas no mercado como uma unidade.

As empresas também podem emitir diferentes e quantas classes de ações, identificando-as por letras (A, B, C, etc.), conforme objetivos específicos, tais como, por exemplos, valores diferenciados de dividendos (dividendo mínimo, dividendo fixo, etc.), proventos especiais, etc. Portanto, cada classe de ações possui seus próprios direitos e restrições; principalmente referente ao recebimento de dividendos, diferenciando-se a porcentagem. Em razão

disso, deve-se consultar o estatuto da empresa para entender as classes das ações.

As ações são negociadas na Bolsa de Valores através de códigos, constituído de 4 letras maiúsculas (normalmente representando o nome da empresa), seguidas de um número que representa o tipo de ação que está sendo negociado (conforme exemplos infra).

- 1 - Direito de subscrição - ação ordinária;
- 2 - Direito de subscrição - ação preferencial;
- 3 - Ordinárias;
- 4 - Preferenciais;
- 5 - Preferenciais Classe A;
- 6 - Preferenciais Classe B;
- 7 - Preferenciais Classe C;
- 8 - Preferenciais Classe D;
- 9 - Recibo de subscrição - ação ordinária;
- 10 - Recibo de subscrição - ação preferencial;
- 11 - BDRs, ETFs e Units.

Exemplificando, PETR3 é o código ações ordinárias da Petrobras. Já UBBR11 é o código das units do Unibanco. E USIM6 é Usiminas PNB (preferencial classe B).

Imediatamente após o código do emissor (exemplo, PETR é a sigla ou prefixo da Petrobras) se encontra a letra que designa o tipo (tabela supra) e o mês de vencimento da opção (tabela infra). E, depois do código do emissor segue uma letra indicativa do mês de vencimento. Com outras palavras, o quinto caractere do código identifica se tarta-se de uma opção de compra ou de venda e qual é o mês de vencimento deste contrato. Por exemplo, VALEK é o código Bovespa de uma opção de compra da Cia. Vale do Rio Doce, com vencimento em novembro.

Mês	**Opção de compra (call)**	**Opção de venda (put)**
Janeiro	A	M
Fevereiro	B	N
Março	C	O
Abril	D	P

Maio	E	Q
Junho	F	R
Julho	G	S
Agosto	H	T
Setembro	I	U
Outubro	J	V
Novembro	K	W
Dezembro	L	X

Os seguintes sufixos (depois do número identificador do tipo) designam ações no mercado à termo: T = Termo comum ou em pontos. S = Termo flexível. D = Termo em dólar. B = Mercado à vista. X = Mercado futuro de ações. F = Mercado fracionário. STNC = Secretaria do Tesouro Nacional. LTN = Letras do Tesouro Nacional. ACN = Ações Nominativas. PR = Preferenciais. Exemplo, PETRB4X se refere a um contrato futuro de compra/venda de ações PN da Petrobras com vencimento em fevereiro.

O site da Bovespa permite consulta pelo nome ou CNPJ da empresa para descobrir o seu código ISIN - *International Securities Identification Number* (Número de Identificação Internacional de Valores Mobiliários).

- http://www.bmfbovespa.com.br/pt_br/servicos/market-data/consultas/mercado-a-vista/codigo-isin/pesquisa/.

O banco de dados ISIN.org (https://www.isin.org/isin-database/#) contém a maior lista de diretórios de banco de dados internacional independente de valores mobiliários (ISIN) do mundo.

Sempre que se compra ou vende ações, há um período de três dias úteis para que o dinheiro saia ou entre na conta que o investidor possui. No caso dos fundos ou dos clubes, cada um tem um regulamento próprio que indica em quanto tempo o dinheiro poderá ser retirado após uma ordem ser efetuada.

Os investimentos consistem em 3 tipos básicos. *Day-Trade* são as operações de compra e vende da ação no mesmo dia. As ações de curto prazo duram entre 1 dia a 2 semanas, possuem ótimo nível de acerto e risco reduzido. Já as de longo prazo, visam ganhar com empresas com excelente

perspectiva no longo prazo. Possuem as opções de dividendo, moderada e agressiva.

As ações podem ser compradas de 4 maneiras básicas:

1) Fundos de Investimento em ações. Como em todos os fundos de investimento financeiro, é um condomínio em que os investidores delegam a um profissional (gestor) a função de escolher onde investir. Desse modo, é o gestor do fundo (corretora de valores, banco ou um gestor de recursos independente, autorizado pela CVM) que escolhe as ações que farão parte da carteira. O investidor não faz qualquer negociação e nem adquire ações, mas sim cotas de um fundo. Desse modo, cada um dos investidores possui uma cota, que corresponde a uma porção do total de ações que o fundo tem. Cada fundo tem seu próprio estatuto, que informa suas regras e o grau de risco de seus investimentos. Todo fundo precisa ter um gestor certificado pela CVM, que coordena as compras e vendas de ações. Assim, quando uma pessoa adere a um fundo, deve estar de acordo com sua política de investimento, especificada em seu estatuto. Deve-se, ainda, pesquisar e comparar a rentabilidade e as taxas dos fundos.

2) Fundos de índices de ações (ETFs - *Exchange Traded Fund*). Trata-se de um fundo negociado em Bolsa que representa uma comunhão de recursos destinados à aplicação em uma carteira de ações que busca retornos que correspondam, de forma geral, à performance, antes de taxas e despesas, de um índice de referência; por exemplos, o IDIV - Índice de Dividendos e o ISE - Índice de Sustentabilidade Empresarial. Também é conhecido por cesta de ações. Neste condomínio, a carteira de ações é espelhada nos índices da Bolsa. Desse modo, através de uma única aplicação, investe-se em um índice da Bolsa, por exemplo, Ibovespa. Também não é preciso escolher as ações em que vai se investir. No Brasil, os ETFs são regulamentados pela Instrução 359 da CVM de 2002 (http://www.cvm.gov.br/legislacao/inst/inst359.html). A legislação permite apenas a criação de ETFs de ações e obriga estes a possuírem ao menos 95% de seu patrimônio investidos em ativos de renda variável ou contratos futuros do índice de referência. É permitida apenas a emissão ou resgate de cotas em ações (*modelo in-kind*).

Confira os ETFs listados na Bolsa de Valores: http://www.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/renda-variavel/etf/renda-variavel/etfs-listados/.

3) Clubes de Investimento; que possuem um caráter menos formal do que um fundo. Diferentemente dos fundos, não precisam de um gestor certificado pela CVM, mas um representante que dê à corretora a ordem de compra ou venda de ações. Portanto, há maior liberdade por parte das pessoas que compõem o clube sobre quanto e onde será investido. Trata-se de um grupo de amigos ou de familiares, que se unem para investir e pode ser aberto com no mínimo 3 e, no máximo, 50 membros. Todos os clubes de investimento têm representantes e estatutos sociais. Todos os membros podem opinar e contribuir nas assembleias do clube. Os ganhos e as perdas são divididas proporcionalmente entre os membros de acordo com o quanto investiram.

4) Individualmente. Nesta opção o próprio investidor é quem decide onde, como, quando e quanto investir. Portanto, é o investidor que controla as ordens de compra e venda de suas ações. Essa modalidade pode ser exercida através do intermédio da corretora, na qual o investidor manifesta suas intenções (dá ordem) de compras e de vendas. Essa decisão do investidor pode ser totalmente voluntária ou influenciada pelas sugestões, orientações e suporte dos analistas da corretora. Ou, o investidor pode fazer tudo sozinho, através da Internet, simplesmente utilizando-se do sistema (*home broker*) da corretora. Essa modalidade é realmente a compra direta de ações. O *home broker* é rápido, transparente e muito seguro. Através dele, o investidor pode pela Internet acompanhar sua conta e o mercado, ter acesso aos custos de operação e negociar (comprar e vender) suas ações e cotas de fundos de casa, no escritório e até durante uma viagem. Apesar de que nos fundos é o gestor quem compra e vende, o investidor pode compras as cotas dos fundos através do *home broker*. Portanto, a compra direta é quando o investidor escolhe, por conta própria ou com a ajuda dos especialistas da corretora, as empresas nas quais quer investir.

O Fundo de Capital Protegido é um Fundo de Investimento Multimercado que busca obter uma rentabilidade vinculado a performance de algum ativo.

Os exemplos mais comuns são Ações, Índice de Ações ou Commodities, como o Ouro. Uma grande parte (até cerca de 90%) do patrimônio do fundo é aplicada em Títulos Públicos e uma parcela menor é aplicada em estrutura de Opções. A estratégia, portanto, consiste em dividir os recursos entre renda fixa (alternativa de menor risco), como títulos públicos e CDBs (Certificados de Depósitos Bancários) e renda variável (de maior risco), como ações e fundos cambiais. Desse modo, a estrutura de opções será a parte de risco do investimento que irá rentabilizar o fundo caso o ativo em questão tenha performance positiva; ou seja, a rentabilidade do produto será a mesma do ativo escolhido pelo fundo, em alguns casos com limite de alta. Em o ativo escolhido apresentar rentabilidade negativa, a estrutura de opções valerá zero e a rentabilidade do fundo será a mesma da parcela aplicada em renda fixa. O somatório da parcela de renda fixa e sua rentabilidade será, aproximadamente, o valor do capital investido menos os custos do produto; ou seja, o capital inicial estará garantido. Por outras palavras, no pior dos casos, ao final de um ano, o investidor vai ter o valor que aplicou (valor nominal, sem descontar a inflação). No caso de fundos há cobrança de taxa de administração. A maioria desses fundos desenvolvidos no Brasil não permite resgate do dinheiro investido durante a vigência da operação, normalmente, no mínimo, entre 1 ano e 1 ano e meio. O resgate não será permitido para que seja garantido o capital protegido dos cotistas que investem no fundo. Entretanto, a recomendação para o investidor que quer retorno, mas não abre mão de controlar o risco dos seus investimentos, é ele mesmo fazer o balanceamento da sua carteira de opções. É preciso também analisar cuidadosamente de quanta rentabilidade se está abrindo mão (o seguro) para garantir o principal. O seguro, em alguns tipos de fundos, pode sair muito caro, tornando a operação toda pouco lucrativa.

Enquanto que os **Fundos de Renda Fixa Referenciados (DI)** aplicam, no mínimo, 95% do patrimônio nos títulos públicos federais do Tesouro Direto (atrelados ao CDI ou Selic) ou em títulos privados de baixo risco, com taxa pós-fixada (por exemplo, os títulos LFT - Letras Financeiras do Tesouro); os **fundos de Renda Fixa (RF)** investem em títulos públicos pré-fixados (por exemplos, LTN [Letras do Tesouro Nacional] e NTN [Notas do Tesouro Nacional]). Desse modo, os fundos DI são mais indicados em momentos de alta de juros (aumento da taxa Selic), pois seu rendimento varia junto com

esse indicador. Os fundos RF, por sua vez, são indicados para momentos de queda de juros; vez que se baseia na compra de títulos de juros pré-fixados.

- http://www.tesouro.fazenda.gov.br/.

POPs (Proteção do Investimento com Participação) são ativos compostos de ações e opções ajustadas de forma a limitar o risco (e ganhos) em operações com renda variável. Trata-se de uma combinação de três instrumentos do mercado de renda variável: uma ação no mercado à vista, uma opção de compra (*call*) e uma opção de venda (*put*). Além disso, é um investimento na bolsa de valores que proporciona proteção contra eventuais perdas. Em períodos de queda, o investidor acumularia prejuízo se comprasse uma ação no mercado à vista. Já no POP o capital do investidor está protegido, só que em períodos de alta, ele não recebe integralmente todo rendimento; pois abre mão de parte do ganho em troca dessa proteção. É como fazer seguro. Ao contrário do fundo de capital protegido (que só pode resgatar as cotas no final do prazo ou em datas específicas de tempo determinadas), no POP pode-se comprar, vender (desde que se haja mercado para a venda) e resgatar a qualquer instante. Pelo fato de um fundo de capital protegido exigir auditoria, contabilidade e registro na CVM, ele é mais caro que o POP.

Para comprar ou vender ações, é necessário procurar uma corretora de valores, uma distribuidora de títulos e valores ou um banco de investimento. Entretanto, como as corretoras são as únicas instituições autorizadas a operar na Bovespa, as distribuidoras e os bancos de investimentos se utilizam dos serviços de uma corretora para poderem realizar os negócios de seus clientes. Portanto, para poder comprar e vender ações na Bolsa de Valores, é necessário possuir conta em uma corretora de ações. Por outras palavras, as corretoras são uma ponte necessária entre o investidor e a Bolsa de Valores.

A corretora deve ser escolhida da lista de habilitadas no site da BM&FBovespa (http://www.bmfbovespa.com.br/pt_br/servicos/participantes/busca-de-corretoras/), após a devida comparação de recursos, serviços, suportes, taxas, localidade, etc.

- http://www.bb.com.br/portalbb/page3,129,9106,0,1,1,9.bb?codigoNoticia=19405&codigoMenu=7140;
- http://www.caixa.gov.br/voce/poupanca-e-investimentos/acoes-online/Paginas/default.aspx;
- https://banco.bradesco/html/classic/produtos-servicos/investimentos/acoes.shtm;
- https://www.itau.com.br/investimentos-previdencia/acoes/;
- https://www.santander.com.br/portal/wps/script/templates/GCMRequest.do?page=9323&entryID=8601;
- http://www.bb.com.br/pbb/pagina-inicial/private/produtos-e-servicos/investimentos---private#/;
- https://www.easynvest.com.br/investimentos/investir-acoes;
- https://www.xpi.com.br/investimentos/acoes/;
- http://www.empiricus.com.br/;
- https://magnetis.com.br/;
- https://verios.com.br/;
- https://www.easynvest.com.br/;
- http://decision-one.com.br/;
- https://www.clear.com.br/;
- http://www.tororadar.com.br/;
- https://daycovalinveste.com.br/.

Antes de realizar um investimento de verdade, deve-se pesquisar e se informar sobre a empresa ou o ativo. É crucial conhecer as estratégias, perspectivas de crescimento, o comportamento do setor e a lógica do mercado. No site da BM&FBOVESPA (http://www.bmfbovespa.com.br/) existem vários documentos sobre todas as empresas listadas e, ainda, o "formulário de referência", no qual se pode saber mais sobre a saúde financeira das empresas.

É possível comprar ações de empresas norte-americanas com bitcoin através do Bitpay (https://bitpay.com/), FoxBit (https://foxbit.com.br/), Bitfinex (https://www.bitfinex.com/), BTC-e (https://btc-e.com/) e Bitstamp (https://www.bitstamp.net/).

- https://drivewealth.com/;
- https://drivewealth.com/drivewealth/es/how-to-fund-your-us-securities-account;
- https://drivewealth.com/drivewealth/pt-br/drivewealth-the-road-towards-connecting-the-world-through-finance;
- https://drivewealth.com/drivewealth/pt-br/drivewealth-the-road-towards-connecting-the-world-through-finance.

Antes de poder abrir uma conta numa corretora, é necessário possuir uma conta corrente para poder enviar e receber o dinheiro. Explica-se. O dinheiro só entra na conta da corretora de uma conta bancária com mesmo CPF ou CNPJ. Da mesma forma, quando o dinheiro sair da conta na corretora, somente poderá ser transferido para uma conta corrente de mesmo CPF ou CNPJ.

As **taxas principais** são as seguintes:

- **Taxa de emolumentos**, paga à BM&FBovespa e calculada em relação ao valor que envolve a compra ou venda de ações. É a única que não varia de acordo com a corretora;
- **Taxa de administração**, cobrada nos fundos e clubes, é calculada anualmente, ou proporcionalmente, em relação ao valor aplicado e cobrada proporcionalmente ao período em que o investidor manteve operações;
- **Taxa de performance**, cobrada quando o fundo supera a rentabilidade esperada;
- **Taxa de corretagem** é o valor cobrado pelas corretoras pelo acesso ao mercado; pode ser um valor fixo para cada ordem

(compra ou venda) dada ou uma porcentagem sobre a operação (compra ou venda) realizada;

- **Taxa de custódia** é o valor mensal cobrado pela guarda das ações pela BM&FBOVESPA e pelos serviços oferecidos pela corretora. Hoje em dia, a grande maioria das ações negociadas é escritural; ou seja, registrada e custodiada sem a emissão das cautelas. Uma das vantagens da custódia escritural é a atualização dos direitos das ações (bonificações, dividendos e subscrição), eliminando qualquer trabalho dessa natureza para o investidor. Este serviço é cobrado pela instituição custodiante à corretora, que, por sua vez, repassa ao investidor, além da taxa de corretagem. A taxa de custodia varia de corretora para corretora, podendo até ser gratuita.

O administrador de fundos de varejo (isto é, não destinados exclusivamente a investidores qualificados), que adquire cotas de outros fundos de investimento, pode estabelecer em seu regulamento:

a) uma taxa de administração máxima, compreendendo a taxa de administração dos fundos em que investiu;

b) uma taxa de administração mínima, que não inclui a taxa de administração dos fundos em que invista, caso em que o prospecto e qualquer material de divulgação que efetue comparação de qualquer natureza entre os fundos, deve referir-se, na comparação, apenas à taxa máxima, permitida a referência, em nota, à taxa mínima e à taxa total efetiva em outros períodos, se houver;

c) nos planos de previdência complementar, a taxa de administração é adicionada, normalmente, de uma taxa de gestão financeira.

O ***home broker*** **(HB)** é um instrumento, semelhante ao *home banking*, que interligado ao sistema de negociação da Bovespa, permite a negociação (ordens de compra e venda) de ações via Internet. Para realizar operações via Internet, é necessário ser cliente de um banco de investimentos, distribuidora ou corretora que disponha do sistema *home broker*. Além da

praticidade e rapidez nas negociações, o *home broker* proporciona: agilidade no cadastramento e no trâmite de documentos; envio de ordens imediatas de compra e venda de ações; recebimento da confirmação de ordens executadas; acompanhamento da carteira de ações; acesso às cotações e, em alguns casos, até de notícias e análises do mercado; etc.

- http://www.tororadar.com.br/home-broker-o-que-e;
- http://app.tororadar.com.br/cursos/home-broker-o-que-e-e-como-funciona/;
- https://www.modalmais.com.br/blog/qual-o-melhor-home-broker;
- https://smarttbot.com/;
- http://lp.rico.com.vc/lp/home-broker;
- https://www.agorainvest.com.br/ferramentas.html;
- http://investcharts.com/;
- http://www.tradergrafico.com.br/trader/;
- http://www.grafix2.com/.

De modo similar a um exame de eletroencefalograma, um monitor de frequência cardíaca, o gráfico de um equalizador de som, a tela de um osciloscópio ou uma medição de sismógrafo, a medição das altas e baixas das cotações na bolsa de valores costuma ser feita através de uma linha, que vai avançando da esquerda para a direita, e tal como um termômetro que possui o grau zero como referência padrão para os graus positivos e negativos, essa linha oscila entre ir subindo, ir descendo ou até manter uma linha reta ou horizontal (como quando inexiste batimento cardíaco no frequencímetro). Nessa montanha russa de subir e descer, similar à uma cobra se contorcendo e fazendo curvas ou a letra S deitada, os picos (pontas, cantos ou quinas) podem possuir o formato de ponta triangular (como a ponta de uma flecha ou faca).

Como um exemplo dos **padrões gráficos e de linhas de tendência**, citamos o padrão (gráfico) de cabeça e ombros (ou OCO - ombro, cabeça e ombro) é um dos mais populares e confiáveis da análise técnica e se baseia na análise de topos e fundos da Teoria de Dow (http://www.tororadar.com.br/investimento/bovespa/teoria-de-dow). Trata-

se de um padrão gráfico ou figura de reversão (mudança de tendência ou comportamento) que, ao se formar, sinaliza a suscetibilidade de uma ação se mover contra uma tendência anterior. Imagine que a representação gráfica da cotação de determinada ação, moeda ou comódite (*commoditie* ou *commodity*) desenhou três triângulos seguidos, sendo os dois dos lados com a mesma altura (ou quase isso) e o do meio, com a maior altura. Por outras palavras, esse desenho lembra um busto (dois ombros e uma cabeça). Esse desenho pode também estar de ponta cabeça (invertido). A linha de base (chão ou fundação) dos três triângulos é a mesma (ou quase) e é determinada traçando-se uma linha reta (linha de pescoço) ligando os dois pontos, quais sejam, os momentos em que a ação para de cair e volta a subir. Entre esses dois pontos está a pirâmide de maior tamanho; ou seja, eles formam a base do triângulo maior (suporte) e a linha desses dois pontos, portanto, se encontram no pico do triângulo maior. A linha de pescoço também pode estar nos picos dos triângulos (resistência). Uma vez tendo noção da **linha de pescoço (*neckline*)**, é possível compreender que a **cabeça (*head*)** é o topo da ascendência (ápice ou ponto mais alto da tendência) e o **ombro (*shoulder*)** se localiza mais abaixo da linha de pescoço. Topo ou resistência maior é a extremidade ou o ponto mais alto de um movimento de alta, o qual antecede um movimento de baixa. É o local onde o preço parou de subir e começou a cair. Fundo é a extremidade ou o ponto mais baixo de um movimento de baixa, o qual antecede um movimento de alta. É o local onde o preço parou de cair e começou a subir. A projeção é a previsão de baixa que o preço pode atingir após romper a linha de pescoço. Portanto, o padrão OCO tradicional sinaliza que uma cotação vai cair quando o padrão se completa; ou seja, geralmente no auge de uma tendência de alta. Já na versão invertida (OCOI), evidencia que o preço vai subir durante uma tendência de baixa. Ambos padrões são confirmados quando a linha de pescoço é ultrapassada, após a formação do segundo ombro.

Saiba mais no e-book "Análise Técnica de Ações" gratuito da Toro Radar (http://www.tororadar.com.br/).

- http://www.tororadar.com.br/ebook/analise-tecnica-de-acoes-pdf.

Os **comandos (ordens) básicos de um *home broker*** são os seguintes: ***Start*** (iniciar ou começar) ou *stop* de compra é uma ordem de compra programada. ***Stop*** (parar) é ordem de venda ou de limitação de prejuízo. O mecanismo ***stop gain*** permite ao investidor vender saindo de uma operação embolsando o lucro após o sinal proporcionado. Explica-se. O **preço de disparo** é o valor (ou percentual) monetário do ativo que servirá como condição para o envio automático da ordem de venda no *Home Broker*. Já o **preço de venda** é o valor (ou percentual) monetário do ativo que será enviado ao sistema quando o preço de disparo for executado; objetiva sair da operação com lucro e encerrar a posição com essa operação. Desse modo, no campo **disparo (gatilho)**, deve-se colocar o preço (ou percentual) em que o *stop* será ativado e, no campo preço, o valor (ou percentual) mínimo de venda. A palavra *gain* significa ganhar. Uma ordem de venda *stop gain* objetiva permitir que o ganho seja aumentado. O limite, duração ou prazo de validade dessa ordem é definido pela ordem de ***stop loss***. A palavra *loss* significa perda. Desse modo, uma ordem de venda *stop loss* tem como objetivo evitar perdas. Para ativar o *stop loss*, é necessário o preenchimento do valor de disparo e do valor de preço mínimo. Ordem de *stop* móvel (***trailing stop***) é uma ordem *stop* na qual o valor do preço de gatilho do *stop* e da ordem limitada de venda vão se ajustando para cima, à medida que o ativo se valoriza. Gatilho é o nível de preço que quando atingido faz com que ordem de *stop* ou de *start* seja acionada; já limite é o nível de preço até onde se permite que a ordem de *stop* ou de *start* seja executada. Detalhe, nem todas as corretoras oferecem a ferramenta de emissão de ordens com percentual.

Saiba mais sobre a programação do *home broker* no e-book "O Guia Absolutamente Completo dos Robôs de Investimento" da Delta Trader (http://eazeus.com.br/guia-robos-de-investimento-gdc/) e em https://www.equipetrader.com.br/5-dicas-para-configurar-o-seu-robo-de-investimento/.

- http://conteudo.decision-one.com.br/escolha-o-robot-mais-adequado-ao-seu-perfil.

Para poder se familiarizar melhor, existem vários **simuladores de *home broker***; ou seja, é possível aprender e testar sem estar arriscando nada.

- http://atendimento.xpi.com.br/consulta-de-cliente/simulador-home-broker/;
- http://www.simulabolsa.com.br/;
- http://www.bbsimulacao.com.br/;
- http://ri.bmfbovespa.com.br/infoinvest/simulador.asp?idioma=ptb.

O **FolhaInvest** (http://folhainvest.folha.uol.com.br/) é um simulador do jornal Folha de São Paulo em parceria com a BM&FBovespa, onde oferece aos participantes a oportunidade de conhecer o funcionamento do mercado de ações na prática. Nele se pode abrir uma conta e receber inicialmente um capital de R$ 200.000,00 para começar a operar na Bolsa; sendo tudo virtual e totalmente gratuito.

O **UOL Invest** (http://uolinvest.economia.uol.com.br/) também é um simulador totalmente gratuito, que oferece aos participantes a oportunidade de conhecer o mercado de ações na prática.

O **Simulador EXAME** (http://simulador-exame.exame.com.br/) é muito parecido com um verdadeiro *home broker*.

As corretoras também disponibilizam **contas demo ou de demonstração** para os iniciantes testarem.

- http://www.investirnabolsa.pt/conta-demo-para-iniciantes-na-bolsa/;
- https://www.xm.com/register/account/demo?lang=pt;
- http://www.tororadar.com.br/;
- https://www.xtrade.com/pb/register/;
- http://www.fxpro.pt/;
- https://www.ig.com/it/conto-demo;
- https://www.markets.com/pt;
- https://www.instaforex.com/pt/demo_account_cabinet;
- https://www.montepio.pt/SitePublico/pt_PT/particulares/mercados/trader/adesao-demo.page;

- http://meivox.infomoney.com.br/;
- https://www.ig.com/por/abrir-conta-demo;
- http://pt.noafx.com/open-demo-account.php;
- http://www.avatradeportuguese.com/;
- https://www.hotforex.com/sv/pt/trading-tools/account-types/hotforex-demo-account.html.

Existem diversos *home brokers*, inclusive os simuladores e as contas demo (de demonstração) para *smartphones* e *tablets*. Para facilitar uma pesquisa, se o sistema operacional do dispositivo for Android, ao invés de procurar pelo Play Store no próprio *smartphone* ou *tablet*, basta acessar pelo computador o site do Google Play (https://play.google.com/store/apps), clicar na aba/guia Apps e digitar os termos de pesquisa.

A melhor forma de ver como funciona a negociação na bolsa de valores de um modo geral e ter uma ideia do que faz a plataforma *market trader* em particular, é abrir uma conta de demonstração. Esta conta permite navegar na plataforma em modo de conta de demonstração, ajudando a aprender comodamente a utilizar as diversas ferramentas e funcionalidades, utilizando fundos de demonstração sem risco.

- https://options.eztrader.com/pt/revista-opcoes-binarias/demo-conta.aspx?regulationpopup=true.

Muitos especialistas enfaticamente aconselham transacionar no modo de demonstração por um período de tempo considerável antes de arriscar dinheiro em uma conta real. Ainda mais, através das contas demo é possível avaliar melhor a corretora antes de efetivamente contratá-la.

Mais informações sobre investimentos podem ser obtidas no site Portal do Investidor (http://www.portaldoinvestidor.gov.br/), do Instituto Educacional BM&FBovespa (https://educacional.bmfbovespa.com.br/), da CVM - Comissão de Valores Mobiliários (http://www.cvm.gov.br/), da Anbima (http://www.anbima.com.br/) e no Serviço de Atendimento ao Cidadão da CVM: (http://sistemas.cvm.gov.br/?SAC). E nos sites infra:

- http://www.bmfbovespa.com.br/pt_br/como-investir/como-investir-em-acoes/#/home;
- http://www.veduca.com.br/cursos/gratuitos/financas-pessoais-e-investimento-em-acoes;
- http://marceloveiga.com.br/aprenda-a-investir-na-bolsas-de-valores-video-curso-gratis/;
- https://www.youtube.com/channel/UCgtjY7s4btFz0eT37CFO5Og;
- https://queroinvestiragora.leadpages.co/leadbox/144fbbb73f72a2%3A14b103630b46dc/5677492304084992/;
- http://conteudo.decision-one.com.br/guia-de-introducao-ao-mercado-de-acoes;
- http://educacao.infomoney.com.br/ebook-opcoes/inscricao.html;;
- http://www.tororadar.com.br/ebook;
- http://www.tororadar.com.br/day-trade-acoes;
- http://www.administradores.com.br/artigos/economia-e-financas/como-investir-na-bolsa-de-valores-passo-a-passo-para-iniciantes/98368/;
- http://escolatrader.net/;
- https://www.equipetrader.com.br/cursos/;
- http://scalpertrader.com.br/intensivo-curso-gratuito-day-trade-fl/;
- http://investidordesucesso.com.br/is/lp-ebook-ric.html;
- http://www.comoinvestir.com.br/;
- http://br.advfn.com/;
- http://dinheirama.com/;
- http://www.invexplorer.com.br/;
- http://carteirarica.com.br/como-investir-na-bolsa-de-valores/;
- http://www.bb.com.br/portalbb/page3,129,9105,0,1,1,9.bb?codigoNoticia=19404&codigoMenu=7118;
- https://www.hotforex.com/sv/pt/trading-tools/forex-education.html;

- http://www.comoinvestir.com.br/glossario/Paginas/default.aspx;
- https://blog.magnetis.com.br/;
- http://investidordesucesso.com.br/;
- http://www.istoedinheiro.com.br/blogs-e-colunas/post/20150326/e-books-praticos-gratuitos-para-empreendedores/6426;
- http://pme.estadao.com.br/noticias/noticias,oito-livros-e-cartilhas-gratis-para-ajudar-o-empreendedor,5335,0.htm;
- https://www.genialbroker.com.br/site/universidade/glossario.aspx;
- http://www.enfin.com.br/;
- https://www.equipetrader.com.br/.

Baixe o **e-books gratuitos**:

- "Como começar a investir em ações" - http://www.tororadar.com.br/ebook/como-investir-na-bolsa-de-valores?utm_source=PPL_LLK-Bases&utm_medium=ads&utm_campaign=facebook&utm_content=LLK-1_Base-Cadastrados-Engajados_BR_Desktop_H_25a50
- "Aprenda com a sabedoria dos 10 maiores investidores do mundo" - http://www.guiainvest.com.br/lp/ebook-aprenda-com-a-sabedoria-dos-10-maiores-investidores/

TRIBUTAÇÃO SOBRE OURO, AÇÕES E RENDA VARIÁVEL

As regras de cálculo e apuração de Imposto de Renda sobre ações e renda variável não são simples e são atualizadas constantemente. Passemos a expor algumas noções gerais da tributação.

Ressalta-se novamente que, como o governo altera subitamente as regras, este capítulo visa apenas apresentar uma noção básica geral da tributação, cujas regras devem ser conferidas periodicamente nos links (sites) para verificar se não houve modificações e quais foram estas. Ao final deste capítulo, antes dos links para saber mais, constam algumas alterações e atualizações. No capítulo seguinte também existem explanações sobre tributação. Quem não quer ter todo esse trabalho, basta pagar um contador.

A Receita Federal do Brasil exige a identificação do beneficiário final das empresas nacionais e estrangeiras que vierem de alguma forma operar no Brasil.

- http://politica.estadao.com.br/noticias/geral,offshore-tera-que-identificar-dono-real,10000014322;

Pelas regras da Receita Federal, qualquer investidor que "realizou operações na Bolsas de Valores, de mercadorias, de futuros e assemelhadas", está obrigado a entregar sua declaração anual de imposto de renda e por conta disso, deve-se calcular e declarar o Imposto de Renda em ações. Nisso estão incluídos todos os investidores, que devem calcular o IR (Imposto de renda) independente de terem lucro ou prejuízo na bolsa de valores. Além disso, a apuração e pagamento do Imposto de Renda em ações deve ser feita mensalmente, e esta responsabilidade é unicamente do próprio investidor.

Após encerrada uma posição (seja vendida ou comprada) deve-se apurar quanto obteve de lucro ou prejuízo, já descontando os custos operacionais (corretagens e taxas). Para isso deve-se utilizar o conceito de preço médio de compra das ações. Ao final desta etapa, deve-se ter claro quanto foi o resultado em cada uma das operações que se realizou durante aquele mês. Uma operação encerrada é aquela em que o investidor já desfez sua posição, não importando se a ordem foi compra seguida de venda, ou venda seguida

de compra (operações à termo). A Receita Federal definiu uma tributação diferente para o Imposto de Renda em *day trade* (compra e venda no mesmo dia) e o Imposto de Renda em operações normais (compra e venda em datas diferentes). Quando o resultado é negativo (prejuízo) não se pagará impostos e deverá guardar este valor para abatê-lo dos lucros futuros.

- http://blog.bussoladoinvestidor.com.br/imposto-de-renda-em-acoes/;
- http://blog.bussoladoinvestidor.com.br/imposto-de-renda-em-fundos-imobiliarios/;
- http://blog.bussoladoinvestidor.com.br/como-compensar-prejuizo-em-acoes/;
- http://economia.estadao.com.br/noticias/geral,mudanca-na-tributacao-sobre-ganhos-de-capital,10000015607;
- http://agenciabrasil.ebc.com.br/economia/noticia/2016-03/novo-imposto-de-renda-sobre-ganhos-de-capital-so-valera-partir-de-2017;
- http://www12.senado.leg.br/noticias/materias/2016/03/18/sancionada-lei-que-aumenta-o-ir-sobre-ganhos-de-capital;
- http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13259.htm.

Confira a diferença de tributação entre Pessoa Física e Pessoa Jurídica em http://www.planalto.gov.br/ccivil_03/LEIS/L8981.htm.

As regras de Imposto de Renda sobre rendimentos no mercado financeiro foram consolidadas numa única norma regulamentadora, a Instrução Normativa RFB nº 1.585/2015: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=67494.

Confira as leis em http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/ir-mercado-financeiro.

Os rendimentos de aplicações em renda fixa, como fundos de investimento (FIF), Notas do Tesouro Nacional (NTN), Certificado de Depósito Bancário (CDB) e fundos de ações são declarados como rendimentos tributáveis exclusivamente na fonte, devendo ser informados pelo seu valor líquido (valor do rendimento menos IOF - Imposto sobre Operações Financeiras e menos o Imposto de Renda retido pela instituição).

O imposto retido é considerado como devido exclusivamente na fonte e os rendimentos dessas aplicações não integram a base de cálculo do imposto sobre a renda na Declaração de Ajuste Anual, também não podendo ser compensado.

Entretanto, várias aplicações de renda fixa são isentas de Imposto de Renda, tais como: Caderneta de poupança, Certificado de Recebíveis Imobiliários (CRI), Certificado de Recebíveis do Agronegócio (CRA), Letra de Crédito Imobiliário (LCI) e Letra de Crédito do Agronegócio (LCA). Tais rendimentos (pelo seu valor total) são informados como rendimentos isentos.

Estão isentas de tributação do IR (Imposto de Renda) somente as operações em que o valor das alienações referente aos ganhos líquidos auferidos, realizados em cada mês, seja igual ou inferior a R$ 20.000,00 (vinte mil reais) para o conjunto de ações e para o ouro, individualmente. Se não ultrapassar o valor entre remuneração e capital em 30 (trinta) dias, não há Imposto de Renda (Lei nº 8.981/1995, artigos 23 e 72, §8º; Lei nº 9.250/1995, artigo 22; Lei nº 11.033/2004, artigo 3º, inciso I; Solução de Consulta nº 401/2009; Instrução Normativa RFB nº 1585/2015, artigos 25, § 1º, e 59). Apesar de isentas, essas operações devem ser informadas da declaração de ajuste anual na ficha Rendimentos Isentos e Não Tributáveis.

- Lei nº 8.981/1995 - http://www.planalto.gov.br/ccivil_03/leis/L8981.htm;
- Lei nº 9.250/1995 - http://www.planalto.gov.br/ccivil_03/leis/L9250.htm;
- Lei nº 11.033/2004 - http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l11033.htm;
- Instrução Normativa RFB nº 1585/2015 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=67494;
- Solução de Consulta nº 401/2009 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=68110.

Com a introdução de FIIs (Fundos de Investimento Imobiliário) negociáveis em bolsa surgiu também um novo tipo de operação, além das *day trade* e posição (não *day trade*) já existentes. Lucros com trades de FIIs são tributados sempre em 20% (vinte por cento) e não podem ser compensados com prejuízos de outros tipos de operações.

"Como regra geral, é possível minimizar os custos tributários agindo em três frentes paralelas: (1) escolhendo investimentos totalmente isentos de imposto de renda (por exemplo, LCIs, LCAs, debêntures de infraestrutura); (2) deixar o dinheiro o maior tempo possível nas aplicações financeiras, a fim de pagar a menor alíquota de imposto de renda (caso, por exemplo, do Tesouro Direto, CDBs e fundos de investimentos em renda fixa, de longo prazo); (3) utilizando as leis isentivas a seu favor, no caso das vendas de ações inferiores a R$ 20 mil mensais, e na escolha dos fundos imobiliários, no lugar dos imóveis, para gerar renda de aluguel." (http://www.valoresreais.com/2016/05/16/como-pagar-menos-imposto-nos-seus-investimentos/).

A isenção não abrange as operações de *day-trade*, as negociações de cotas de fundos de índice (**ETFs - *Exchange Traded Funds***) e os ganhos de capital na venda de cotas de fundos de investimento imobiliário. Não estão isentos, também, os resgates de cotas de fundos ou clubes de investimento em ações e a alienação de ações efetivada em operações de exercício de opções, bem como o vencimento ou liquidação antecipada de contratos a termo.

- http://exame.abril.com.br/mercados/cotacoes-bovespa/etfs;
- http://www.infomoney.com.br/onde-investir/investimentos-no-exterior/etfs/noticia/4381562/que-etf;
- http://www.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/renda-variavel/etf/renda-variavel/etfs-listados/;
- https://ww93.itau.com.br/itnow-pt/o-que-sao-etfs/.

Os rendimentos de aplicação de renda variável, como a feita no mercado de ações, devem ser apurados mensalmente. O lucro ou o ganho líquido do investidor, apurado pela diferença entre o valor de venda e o preço de aquisição, estará sujeito ao recolhimento de imposto de renda, e o rendimento deverá ser declarado como exclusivamente na fonte na declaração.

O ganho de capital é o lucro obtido numa operação de venda ou transferência de um bem ou direito. A diferença entre o valor da venda e o valor declarado na aquisição é o ganho de capital. E é sobre esse valor que incide o imposto a ser pago relacionado a qualquer tipo de bem, como ações negociadas na Bolsa de Valores, imóveis, joias, obras de arte e veículos. Nas empresas, o imposto incide sobre a venda de qualquer ativo, desde máquinas e equipamentos, até a própria empresa.

As corretoras são obrigadas a apurar lucros e reter parte destes para a Receita Federal. O IRRF (Imposto de Renda Retido na Fonte) porém é apenas uma parte do Imposto de Renda total devido pelo investidor. No caso de operações *day trade*, por exemplo, a corretora retém apenas 1% (um por cento) do lucro apurado, porém a alíquota devida é de 20% (vinte por cento) do lucro, cabendo ao investidor emitir então uma DARF (Documento de Arrecadação de Receitas Federais) para pagar os 19% (dezenove por cento) que faltam.

O **ganho líquido** é constituído pela diferença positiva entre o valor de venda do ativo e o seu custo de aquisição. Assim, se em vez de ganhos tiver prejuízo, essa diferença deve ser guardada e descontada do Imposto de Renda que ser pago no próximo mês em que a operação der resultado positivo. Portanto, na apuração dos ganhos líquidos ou perdas, as despesas com corretagens, taxas ou outros custos necessários à aquisição e a realização das operações (despesas operacionais), desde que efetivamente pagas pelo contribuinte, podem ser acrescentadas ao custo de aquisição ou deduzidas do preço de venda dos ativos ou contratos negociados. Despesas como a taxas de corretagens e emolumentos que constam nas notas enviadas pela corretora podem ser descontadas do ganho bruto. O custo com aluguel de ações (taxas BTC) também podem ser abatidos e normalmente são encontrados no extrato do investidor na corretora. Em síntese, o custo de aquisição é calculado pela média ponderada dos custos unitários.

Os prejuízos acumulados servem para compensar ganhos futuros somente para o mesmo tipo de operação (*day trade* ou posição) e valem para diferentes mercados, um prejuízo com *day trade* em opções pode compensar o lucro com *day trade* em ações, por exemplo, mas não pode compensar o lucro em operações não *day trade*, mesmo que feitas com opções também.

O cálculo mensal de ganhos é importante até mesmo para controlar os prejuízos acumulados, se este for o caso, e saber quando deverá voltar a pagar caso tenha ganhos futuros. Um investidor que não faz este cálculo mensalmente pode ser surpreendido pela Receita com uma solicitação de pagamento de impostos sobre um mês que tenha ganhos simplesmente por não ter um controle de seus prejuízos anteriores e não saber quanto ainda pode compensar.

Existem também situações em que um investidor, mesmo que tenha tido prejuízo no mês e que também tenha prejuízos acumulados, deve ainda assim pagar o imposto. Um exemplo simples desta situação é um investidor que vem acumulando prejuízos em operações não *day trade*, tendo tido prejuízo inclusive no mês em apuração, só que teve um lucro (mesmo que menor que o prejuízo) em operações *day trade* no mês. Este investidor deverá emitir uma DARF (Documento de Arrecadação de Receitas Federais) e pagar o imposto sobre o lucro que teve, mesmo tendo perdido dinheiro na bolsa no mês.

Caso se tenha feito uso da faculdade (opção) de pagar o imposto sem a efetiva venda das ações, conforme previsto nos artigos 1º e 2º da Lei nº 10.426/2002, o custo de aquisição, para efeito de apuração do imposto quando da efetiva alienação, será o preço médio ponderado constante das relações de que tratam os Anexos I e II da Instrução Normativa SRF nº 119, de 10 de janeiro de 2002.

- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=14811;
- http://www.planalto.gov.br/ccivil_03/leis/2002/L10426.htm.

Os ganhos líquidos auferidos em operações realizadas em bolsas de valores, de mercadorias, de futuros, e assemelhadas, inclusive *day trade*, serão tributados às seguintes alíquotas:

a) 20% (vinte por cento), no caso de operação *day trade*;

b) 15% (quinze por cento), nas operações realizadas nos mercados à vista, a termo, de opções e de futuros.

O imposto deverá ser pago até o último dia do mês seguinte ao da operação.

GCAP é o nome do Programa (software) de Apuração dos Ganhos de Capital que deve ser baixado do site da Receita Federal.

A condição do alienante, se PF (Pessoa Física) ou PJ (Pessoa Jurídica), determina a forma de apuração do Ganho de Capital.

Quando o alienante é PJ, o ganho de capital é tratado conforme:

a) Regime de apuração adotado: Lucro Real, Lucro Presumido ou Simples Nacional;

b) Atividade da empresa: i) Se for imobiliária, a venda representa uma receita normal; e, ii) Se o bem for do ativo permanente, é uma receita não operacional.

Entretanto, são isentos do imposto sobre a renda os ganhos líquidos auferidos por pessoa física em operações efetuadas:

I – Com ações, no mercado à vista de bolsas de valores ou mercado de balcão, se o total das alienações desse ativo, realizadas no mês, não exceder a R$ 20.000,00 (vinte mil reais);

II – Com ouro, ativo financeiro, se o total das alienações desse ativo, realizadas no mês, não exceder a R$ 20.000,00 (vinte mil reais);

III – Com ações de pequenas e médias empresas a que se refere o art. 16 da Lei 13.043/2014 (http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/Lei/L13043.htm).

Em resumo. O investidor que tiver rendimentos em operações com títulos de renda variável (operações financeiras no mercado à vista de ações nas bolsas de valores e em operações com ouro), deve pagar o IR (Imposto de Renda) na base de 15% (quinze por cento) para operações comuns e 20%

(vinte por cento) para *day-trade*. A obrigação de calcular e pagar o imposto é do contribuinte. O imposto deve ser pago mensalmente, até o último dia do mês seguinte ao que se realizou a operação (em que os ganhos houverem sido apurados). O contribuinte deverá preencher o Demonstrativo de Apuração de Ganhos – Renda Variável, cujo programa está disponível no site da Receita Federal. O código a ser utilizado no Documento de Arrecadação das Receitas Federais (DARF) para pagamento desse tributo é 6015.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/pagamentos-e-parcelamentos/pagamento-do-imposto-de-renda-de-pessoa-fisica/ganho-de-capital/programa-de-apuracao-de-ganhos-de-capital-moeda-nacional/ganhos-de-capital.

Assim, quando negociamos o Ouro como ativo financeiro, o ganho de capital estará isento de Imposto de Renda sempre que o valor total de venda dos contratos não superar R$ 20.000,00 (vinte mil reais) em um único mês. Essa regra é a mesma para o mercado de ações e não concorrem entre si; ou seja, pode-se operar os dois ativos (ações e ouro) até R$ 20.000,00 (vinte mil reais) que permanecerá isento.

Importante afirmar que compra de ouro em barras não é isento de IR em caso de venda.

Reforçando. Os ganhos líquidos são apurados e tributados, mês a mês, em separado, e não integram a base de cálculo do imposto sobre a renda na Declaração de Ajuste Anual. Da mesma forma, o imposto pago não pode ser deduzido do devido na declaração anual.

- Download do programa gerador da Declaração do IRPF 2016: http://idg.receita.fazenda.gov.br/interface/cidadao/irpf/2016/download.

Esta declaração anual só é obrigatória para quem se enquadrar em situações específicas, sendo as principais: quem negociou em bolsa, independente da renda, do patrimônio e de outros critérios de obrigatoriedade; ter tido renda acima de certo valor no ano anterior; ou, ter bens e direitos acima de determinado valor no último dia 31/12. Para quem negociou ações ou derivativos, independente se fez apenas uma operação (como a participação em um IPO - *Initial Public Offering*) ou várias e

mesmo se só teve prejuízos, a declaração anual é obrigatória. Porém, caso tenha tido lucro em renda variável (o que incluí todas operações em bolsa de valores), o investidor deve pagar o imposto de renda referente ao mês que teve lucro até o último dia do mês seguinte e na declaração anual só precisará declarar os lucros já apurados e os impostos pagos.

IPO - *Initial Public Offering* (oferta pública inicial ou abertura de capital da empresa) é um tipo de oferta pública em que as ações de uma empresa são vendidas ao público em geral numa bolsa de valores pela primeira vez. É o processo pelo qual uma empresa se torna numa empresa de capital aberto.

No caso da renda variável, investimentos em Bolsa de Valores, como as Ações, os Derivativos e os Fundos Imobiliários, a declaração de IR funciona como uma prestação de contas; pois a apuração dos lucros deve ser realizada mensalmente e o imposto (caso aplicável) deve ser pago no mês subsequente. Mas isso somente é necessário quando a soma das vendas for superior a R$ 20.000,00 (vinte mil reais) no mês ou o contribuinte realizar operações de *Day Trade* (compra e venda no mesmo pregão) e caso tenha lucro.

Portanto, se investir em ações e não realizar esse controle durante o ano, será necessário lançar os valores numa planilha de Excel e fazer os cálculos para apurar a existência de impostos não pagos. Havendo valores a pagar deverá ser preenchido uma DARF para cada mês e os valores atualizados com juros e correção. A Receita Federal disponibiliza um programa denominado SICALC para facilitar esse processo.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/pagamentos-e-parcelamentos/darf-calculo-e-impressao-programa-sicalc-1.

A maioria das instituições oferece a seus investidores ferramentas bastante eficientes que automatizam esse processo de apuração do IR mensal. Através da calculadora de IR (Imposto de Renda) ocorre a captura automática das notas de corretagem e apuração do imposto devido. Basta emitir o DARF (Documento de Arrecadação de Receitas Federais) e recolher em qualquer banco.

Para Fundos de Investimento, o imposto é retido diretamente na fonte. Ou seja, a declaração é bem mais simples.

Já os Fundos Imobiliários também possuem uma aba específica onde devem ser informados todos os ganhos e/ou perdas mensais auferidos; bem como impostos já pagos durante o ano, visto que, assim como nas ações e derivativos, a apuração e recolhimento do IR é mensal.

Os rendimentos mensais creditados pelo fundo na conta do investidor são isentos de IR para Pessoa Física e devem, portanto, ser lançados na ficha de rendimentos isentos e não-tributáveis.

Outros rendimentos oriundos de investimentos isentos como Caderneta de Poupança, LCI (Letras de Crédito Imobiliário), LCA (Letra de Crédito do Agronegócio), entre outros, também devem ser informados na ficha de rendimentos isentos e não-tributáveis.

Todos os rendimentos obtidos das demais aplicações (não isentas de Imposto de Renda nem de renda variável) como investimentos em Títulos Públicos, CDB's (Certificados de Depósito Bancário), Letras de Câmbio, Debêntures (não-isentas), Fundos de Investimento, entre outros, devem ser informados na aba de rendimentos tributáveis.

Se o contribuinte teve perda de capital (prejuízo) com ações, a quantia também deve ser informada como resultado negativo no demonstrativo de Renda Variável, acrescentando um sinal de menos antes do valor. Se a perda de um mês foi compensada com ganhos líquidos no mês seguinte, deve-se descontar o valor perdido e considerar o resultado consolidado ao longo de todo o ano.

No item "Operações Comuns/Day-Trade", deve-se inserir o valor da venda com o sinal negativo (-) à esquerda no quadro "Mercado à Vista". De forma automática, o programa gerador da declaração irá transportar esse valor para a linha "Prejuízo a Compensar", no quadro "Resultados".

Para investimentos não financeiros, como a aquisição de um imóvel ou obra de arte, por exemplo, o contribuinte deverá declará-los a partir dos

instrumentos de aquisição, pelos respectivos valores de aquisição; não deve ser declarado o valor de mercado do bem em 31.12.

Os ganhos obtidos pelos quotistas de fundos de ações são tributados no resgate de quotas à alíquota de 15% (quinze por cento). Explica-se. Esse imposto será retido pelo administrador do fundo na data do resgate das quotas, sendo considerado exclusivo de fonte.

Aplicações que retêm o Imposto de Renda na fonte (como Tesouro Direto, fundos de renda fixa e CDBs - Certificados de Depósito Bancário), precisam ser informadas na ficha Rendimentos Sujeitos à Tributação Exclusiva/Definitiva.

O ouro possui tratamento peculiar, quando utilizado como metal nobre, o ouro está sujeito ao Imposto sobre Operações Relativas à Circulação de Mercadorias e Prestação de Serviços. Se, todavia, for empregado como ativo financeiro, passa ao âmbito do Imposto sobre Operações Crédito, Câmbio e Seguro ou relativo a Títulos e Valores Mobiliários. A destinação do ouro o identifica como mercadoria ou como ativo financeiro. A entrada do ouro no mercado financeiro e sua permanência nele lhe assegura esse regime vantajoso: o de ser tributado uma só vez (monofasicamente) e de modo exclusivo (unicamente) pelo Imposto sobre Operações de Crédito, Câmbio e Seguro ou Relativas a Títulos e Valores Mobiliários. Tudo nos termos do artigo 153, § 5º, do texto constitucional.

O ouro comprado como mercadoria e posteriormente vendido ao mercado financeiro não se enquadra no conceito de ouro ativo financeiro preceituado pelo art. 1° da Lei n° 7.766, de 1989, porquanto ausente do compromisso formalizado de destinação ao mercado financeiro, que o caracterizaria dessa forma, desde a sua extração. Ao contrário, tal ouro deve ser caracterizado como mercadoria e, por isso, a receita advinda de sua venda não é considerada receita financeira para fins de aplicação da alíquota zero da Cofins de que trata o art. 1° do Decreto n° 5.442, de 2005 (revogado pelo Decreto nº 8.426 de 2015).

- http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8426.htm.

Sobre compra de ouro por pessoa física diretamente dos garimpeiros (também pessoas físicas), há necessidade de emitir nota fiscal de compra/entrada - http://www.joseadriano.com.br/forum/topics/duvida-referente-a-nfe-compra (Instrução Normativa SRF nº 49, de 2.05.2001 - DOU 07.05.2001 e Protocolo ICMS 42, de 3 de julho de 2009).

O fato gerador do IOF (Imposto sobre Operações de Crédito, Câmbio e Seguros) ocorre na primeira aquisição do ouro efetuada por instituição autorizada ou, quando oriundo do exterior, o seu desembaraço aduaneiro (Lei 7.766/89, artigos 4º a 12, e artigos 36 a 40 do Decreto nº 6.306/2007), sendo inconstitucional qualquer incidência do mencionado tributo sobre as operações subsequentes.

- Lei 7.766/89 - https://www.planalto.gov.br/ccivil_03/leis/L7766.htm;
- Decreto nº 6.306/2007 - http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/D6306.htm.

A **Lei n.º 7.766/1989 dispõe sobre o ouro**, ativo financeiro e sobre seu tratamento tributário:

> "Art. 1º O ouro em qualquer estado de pureza, em bruto ou refinado, quando destinado ao mercado financeiro ou à execução da política cambial do País, em operações realizadas com a interveniência de instituições integrantes do Sistema Financeiro Nacional, na forma e condições autorizadas pelo Banco Central do Brasil, será desde a extração, inclusive, considerado ativo financeiro ou instrumento cambial.
> § 1º Enquadra-se na definição deste artigo:
> I – O ouro envolvido em operações de tratamento, refino, transporte, depósito ou custódia, desde que formalizado compromisso de destiná-lo ao Banco Central do Brasil ou à instituição por ele autorizada.
> II – As operações praticadas nas regiões de garimpo onde o ouro é extraído, desde que o ouro na saída do Município tenha o mesmo destino a que se refere o inciso I deste parágrafo.
> § 2º As negociações com o ouro, ativo financeiro, de que trata este artigo, efetuada nos pregões das bolsas de valores, de mercadorias, de futuros ou assemelhadas, ou no mercado de balcão com a interveniência

de instituição financeira autorizada, serão consideradas operações financeiras.”.

“Art. 8º O fato gerador do imposto é a primeira aquisição do ouro, ativo financeiro, efetuada por instituição autorizada, integrante do Sistema Financeiro Nacional.

Parágrafo único. Tratando-se de ouro físico oriundo do exterior, ingressado no País, o fato gerador é o seu desembaraço aduaneiro.”.

A posse de ouro como ativo financeiro deve ser reportada à Receita Federal na ficha “Bens e Direitos” sob o código 46.

No caso de operações com ouro não considerado como ativo financeiro, o lucro apurado na alienação sujeita-se ao tratamento tributário conferido ao ganho de capital; inclusive quando o ouro for transformado em joias ou já adquirido sob a forma de joias, para uso pessoal do adquirente ou de seus familiares. A tributação de ganhos de capital decorrentes da alienação de joias em ouro segue a tributação de bens de pequeno valor: 15% (quinze por cento) sobre o lucro, sendo isentas as operações caso o valor total de alienações no mês for de até R$ 35.000,00 (trinta e cinco mil reais).

No dia 17/03/2016, numa edição extra do DOU (Diário Oficial da União), foi publicada a **Lei nº 13.259/2016**, resultante do Projeto de Lei de Conversão da Medida Provisória 692/2015, que, dentre outras disposições, estabeleceu a incidência progressiva do Imposto de Renda sobre o ganho de capital auferido pelas pessoas físicas e jurídicas, exceto as tributadas com base no lucro real, presumido ou arbitrado, na alienação de bens e direitos.

- http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13259.htm.

Os percentuais conforme as faixas de ganho de capital são os seguintes:

a) 15%, até R$ 5.000.000,00;
b) 17,5%, de R$ 5.000.000,01 até R$ 10.000.000,00;
c) 20%, de R$ 10.000.000,01 até R$ 30.000.000,00; e
d) 22,5%, acima de R$ 30.000.000,00.

Caso ocorra venda do bem ou direito, em partes, a partir da segunda operação, desde que realizada até o final do ano-calendário seguinte ao da primeira operação, o ganho de capital apurado anteriormente deve ser somado para apurar o Imposto de Renda, devendo deduzir o imposto pago nas operações anteriores, inclusive a alienação de ações ou quotas de uma mesma pessoa jurídica.

O ganho de capital que for apurado pela pessoa jurídica optante pelo Simples Nacional na alienação de seus bens e direitos do ativo não circulante está sujeito à mesma incidência do imposto sobre a renda mencionado anteriormente, e devendo ser pago até o último dia útil do mês subsequente ao recebimento do ganho.

A redação final da Lei nº 13.259/2016 instituiu alíquotas progressivas para a tributação do Imposto de Renda das Pessoas Físicas sobre ganhos de capital auferidos em decorrência da alienação de bens e direitos de qualquer natureza. As alíquotas progressivas são:

- 15% sobre a parcela dos ganhos que não ultrapassar R$ 5.000.000,00;
- 17,5% sobre a parcela dos ganhos que exceda R$ 5.000.000,00 e não ultrapasse R$ 10.000.000,00;
- 20% sobre a parcela dos ganhos que exceda R$ 10.000.000,00 e não ultrapasse R$ 30.000.000,00; e,
- 22,5% sobre a parcela que exceda R$ 30.000.000,00.

As referidas alíquotas aplicam-se também para as alienações de bem ou direito localizado no Brasil realizadas por pessoa física ou jurídica não residente no país.

Segundo as novas regras, para lucros até R$ 5 milhões, a alíquota é de 15% (quinze por cento); ela sobe para 17,5% para ganho entre R$ 5 e R$ 10 milhões; e para 20% para ganhos entre R$ 10 e R$ 30 milhões. Para lucros

acima de R$ 30 milhões, a alíquota cobrada será de 22,5%. E isso vale tanto para operações realizadas no Brasil quanto no exterior.

A Lei 13.259/2016 (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13259.htm) trouxe, ainda, uma alteração à regra de tributação dos lucros auferidos por coligadas de empresas brasileiras no exterior, originalmente prevista na Lei 12.973/2014 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12973.htm).

Nesse sentido, a nova lei introduziu o artigo 82-A à Lei 12.973/14, o qual dispõe que a pessoa jurídica coligada no Brasil poderá, opcionalmente, oferecer à tributação os lucros auferidos por coligadas no exterior à tributação pelo regime de "competência"; isto é, à medida em que os lucros são levantados no balanço da coligada.

A regra geral prevista no artigo 81 da Lei 12.973/2014 previa que a tributação dos lucros auferidos por coligada no exterior dava-se pelo regime de "caixa"; isto é, apenas no momento que os lucros eram efetivamente disponibilizados para a coligada no Brasil.

Por meio da nova regra introduzida pela Lei nº 13.259/2016, a coligada no Brasil poderá optar pelo regime de competência ou caixa e, no caso do primeiro, há argumentos para sustentar que estaria sujeita às regras de cálculo de crédito do imposto pago no exterior aplicáveis às controladas. Assim, a coligada no Brasil poderia apropriar como crédito tanto o Imposto de Renda pago pela controlada sobre seu lucro no seu país de domicílio; bem como eventual Imposto de Renda na Fonte sobre dividendos distribuídos à referida coligada no Brasil.

No Diário Oficial da União (DOU), de 03/10/2016, foi publicada a Instrução Normativa (IN) 1.662/2016 da RFB (Receita Federal do Brasil), que aborda a questão da tributação de rendimentos enviados às empresas no exterior. A IN altera as disposições de outras duas, a de número 1.455/2014 e a 208/2002.

- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=77848.

A nova norma determina que os rendimentos, ganhos de capital e demais proventos pagos, creditados, entregues, empregados ou remetidos a pessoa jurídica domiciliada no exterior por fonte situada no país estão sujeitos à incidência do imposto sobre a renda exclusivamente na fonte à alíquota de 15% (quinze por cento), quando não houver alíquota específica. Além disso, os rendimentos decorrentes de qualquer operação em que o beneficiário more no país ou tenha dependência com tributação favorecida estão sujeitos ao imposto sobre a renda na fonte à alíquota de 25% (vinte e cinco por cento).

Dentre as mudanças, destaca-se ainda que o Imposto de Renda na fonte terá alíquota zero quando incidir sobre rendimentos recebidos de fontes situadas no Brasil por empresas domiciliadas no exterior, nas hipóteses de pagamento, crédito, emprego, entrega ou remessa de receitas de fretes, afretamentos, aluguéis ou arrendamentos de embarcações marítimas ou fluviais ou de aeronaves estrangeiras ou motores de aeronaves estrangeiros, feitos por empresas, desde que tenham sido aprovados pelas autoridades competentes; bem como os pagamentos de aluguel de contêineres, sobrestadia (*demurrage*) e outros relativos ao uso de serviços de instalações portuárias.

A Instrução Normativa RFB (Receita Federal do Brasil) nº 1.455/2014 (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=compilado&idAto=50414), que trata da tributação do IRRF (Imposto sobre a Renda Retido na Fonte) sobre rendimentos pagos, creditados, empregados, entregues ou remetidos para pessoas jurídicas domiciliadas no exterior foi alterada para, dentre outras determinações, estabelecer o que segue:

> a) os rendimentos, ganhos de capital e demais proventos pagos, creditados, entregues, empregados ou remetidos a pessoa jurídica domiciliada no exterior por fonte situada no país estão sujeitos à incidência do IRRF à alíquota de 15% (quinze por cento) quando não houver alíquota específica a ser aplicada;

b) os rendimentos decorrentes de qualquer operação em que o beneficiário seja domiciliado em país ou dependência com tributação favorecida, sujeitam-se ao IRRF à alíquota de 25% (vinte e cinco por cento); salvo as operações que tratem de: b.1) arrendamento mercantil de bens de capital, b.2) juros de empréstimos contraídos em países que mantenham acordos com o Brasil; b.3) juros, comissões, despesas e descontos decorrentes de colocações no exterior de títulos de crédito internacionais; b.4) juros de desconto de cambiais de exportação e comissões inerentes a essas cambiais; b.5) juros e comissões relativos a créditos destinados ao financiamento de exportações;

c) a redução à zero, em relação aos fatos geradores que ocorrerem até 31.12.2022, da alíquota do IRRF incidente nas operações decorrentes de contratos de arrendamento mercantil de bens de capital, na hipótese de pagamento, crédito, entrega, emprego ou remessa, por fonte situada no País, à pessoa jurídica domiciliada no exterior, a título de contraprestação de contrato de arrendamento mercantil, operacional ou financeiro, de aeronave ou dos motores a ela destinados, celebrado por empresa de transporte aéreo público regular, de passageiros ou cargas, até 31.12.2019.

Por fim, foi modificada, também, a Instrução Normativa SRF nº 208/2002 (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=15079), a fim de alterar as regras da tributação, pelo imposto de renda, dos ganhos de capital da pessoa física não residente no Brasil, estabelecendo que na impossibilidade de comprovação do valor de aquisição do bem ou direito, sempre será considerado o custo de aquisição igual a zero.

A Instrução Normativa 1.585 da Receita Federal, de 31 de agosto de 2015 (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=67494), dispõe sobre o imposto sobre a renda incidente sobre os rendimentos e ganhos líquidos auferidos nos mercados financeiro e de capitais.

"Art. 37. Os ganhos de capital e rendimentos auferidos na alienação ou no resgate de cotas dos fundos de investimento imobiliário por qualquer

beneficiário, inclusive por pessoa jurídica isenta, sujeitam-se à incidência do imposto sobre a renda à alíquota de 20% (vinte por cento).

§ 1º Os ganhos de capital ou ganhos líquidos serão apurados:

I - de acordo com os procedimentos previstos no art. 56, quando auferidos:

a) por pessoa física em operações realizadas em bolsa; e

b) por pessoa jurídica em operações realizadas dentro ou fora de bolsa;

II - de acordo com as regras aplicáveis aos ganhos de capital na alienação de bens ou de direitos de qualquer natureza, quando auferidos por pessoa física em operações realizadas fora de bolsa.

§ 2º Para efeitos do disposto no inciso I do § 1º, as perdas incorridas na alienação de cotas de fundo de investimento imobiliário só podem ser compensadas com ganhos auferidos na alienação de cotas de fundo da mesma espécie.

§ 3º O resgate de cotas previsto no caput está sujeito à retenção do imposto sobre a renda na fonte, e ocorrerá somente em decorrência do término do prazo de duração do fundo ou da sua liquidação, sendo o rendimento constituído pela diferença positiva entre o valor de resgate e o custo de aquisição das cotas.

§ 4º Na hipótese prevista no § 3º, o administrador do fundo deverá exigir a apresentação da nota de aquisição das cotas, se o beneficiário do rendimento efetuou essa aquisição no mercado secundário.

Art. 38. Sujeita-se à tributação aplicável às pessoas jurídicas, o fundo de investimento imobiliário que aplicar recursos em empreendimento imobiliário que tenha como incorporador, construtor ou sócio, cotista que possua, isoladamente ou em conjunto com pessoa a ele ligada, mais de 25% (vinte e cinco por cento) das cotas do fundo.

Parágrafo único. Para efeitos do disposto no caput, considera-se pessoa ligada ao cotista:

I - pessoa física:

a) os seus parentes até o 2º (segundo) grau; e

b) a empresa sob seu controle ou de qualquer de seus parentes até o 2º (segundo) grau; e

II - pessoa jurídica, a pessoa que seja sua controladora, controlada ou coligada, conforme definido nos §§ 1º e 2º do art. 243 da Lei nº 6.404,

de 15 de dezembro de 1976.

Art. 40. Ficam isentos do imposto sobre a renda na fonte e na declaração de ajuste anual das pessoas físicas, os rendimentos distribuídos pelos fundos de investimento imobiliário cujas cotas sejam admitidas à negociação exclusivamente em bolsas de valores ou no mercado de balcão organizado.

§ 1º O benefício disposto no caput:

I - será concedido somente nos casos em que o fundo de investimento imobiliário possua, no mínimo, 50 (cinquenta) cotistas;

II - não será concedido ao cotista pessoa física titular de cotas que representem 10% (dez por cento) ou mais da totalidade das cotas emitidas pelo fundo de investimento imobiliário ou cujas cotas lhe derem direito ao recebimento de rendimento superior a 10% (dez por cento) do total de rendimentos auferidos pelo fundo.

§ 2º A verificação das condições para a isenção previstas no caput e no § 1º será realizada no último dia de cada semestre ou na data da declaração de distribuição dos rendimentos pelo fundo, conforme previsto no caput do art. 35, o que ocorrer primeiro.

§ 3º O descumprimento das condições previstas neste artigo implicará a tributação dos rendimentos nos termos do art. 37, por ocasião da sua distribuição ao cotista.”.

Veja, ainda, sobre Imposto de Renda no capítulo seguinte.

Saiba mais:

- http://idg.receita.fazenda.gov.br/noticias/ascom/2017/janeiro/receita-federal-divulga-cronograma-do-irpf-2017;
- http://www.receita.fazenda.gov.br/PessoaFisica/IRPF/2015/perguntao/assuntos/aplicacoes-financeiras-renda-fixa-e-renda-variavel.htm;
- https://www.bradescocorretora.com.br/static_files/Corretora/PDF/IR/iroperacoesvista.pdf;
- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/ir-mercado-financeiro;
- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/Ganhos-de-capital;

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/pagamentos-e-parcelamentos/pagamento-do-imposto-de-renda-de-pessoa-fisica/ganho-de-capital/programa-de-apuracao-de-ganhos-de-capital-moeda-estrangeira-bens-ou-direitos-aplicacoes-financeiras-e-alienacao-em-especie;

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/pagamentos-e-parcelamentos/pagamento-do-imposto-de-renda-de-pessoa-fisica/ganho-de-capital/programa-de-apuracao-de-ganhos-de-capital-moeda-nacional/2016/programa-de-apuracao-dos-ganhos-de-capital-gcap2016;

- Tributação das Empresas no Brasil - Lucro Presumido 2016: http://www.migalhas.com.br/dePeso/16,MI245356,71043-Tributacao+das+Empresas+no+Brasil+Lucro+Presumido+2016;

- Pequeno dicionário de expressões tributárias - http://www1.folha.uol.com.br/mercado/2016/02/1740812-sabe-o-que-e-rendimento-tributavel-ou-ganho-de-capital-veja-dicionario-do-ir.shtml.

MEIOS E ENCARGOS DE ENVIAR OU CARREGAR DINHEIRO AO EXTERIOR

As Leis n.ºs 4.131/1962, 4.595/1964 e 7.492/1986 versam sobre o capital estrangeiro no Brasil e as remessas para o exterior.

- Lei nº 4.131/1962 - http://www.planalto.gov.br/ccivil_03/leis/L4131.htm;
- Lei nº 4.595/1964 - http://www.planalto.gov.br/ccivil_03/leis/L4595.htm;
- Lei nº 7.492/1986 - http://www.planalto.gov.br/ccivil_03/leis/L7492.htm;
- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/remessas-para-exterior.

Através de diversos sites é possível consultar a legislação brasileira:

- http://www.planalto.gov.br/legislacao;
- http://normas.receita.fazenda.gov.br/;
- http://www.lexml.gov.br/;
- http://www2.camara.leg.br/atividade-legislativa/legislacao;
- http://www.jusbrasil.com.br/legislacao/;
- http://www.normasbrasil.com.br/.

A **remessa de valores** pode ser definida como o envio de dinheiro do Brasil para o exterior ou vice-versa. Já a disponibilidade no exterior é a transferência de valores por uma pessoa domiciliada no Brasil para conta bancária de sua titularidade em instituição financeira no exterior. Tal operação está conceituada no artigo 8º da Circular nº 3689/2013 do Bacen (Banco Central do Brasil).

- http://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48812/Circ_3689_v3_P.pdf.

Esse envio de dinheiro para o exterior tem que ser feito, obrigatoriamente, por intermédio de uma instituição autorizada pelo Banco Central do Brasil (Bacen).

- http://www.bcb.gov.br/rex/IAMC/Port/Instituicoes/inst_autorizadas.asp.

Portanto, não se pode comprar moeda estrangeira de forma ilegal (mercado negro ou paralelo) e remeter por qualquer via ao exterior; ou seja, sem que passe efetivamente por uma instituição financeira autorizada e sem recolher o IOF (Imposto sobre operações de crédito, câmbio e seguro, ou relativo a títulos mobiliários).

- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/imposto-sobre-operacoes-de-credito-cambio-e-seguro-ou-relativas-a-titulos-ou-valores-mobiliarios-iof.

O chamado **"câmbio paralelo" ou "câmbio negro"**, além de ser crime passível de punição, não oferece nenhuma segurança; sendo que a chance de receber notas falsas é alta. O câmbio paralelo também não fornece o contrato de câmbio ou qualquer tipo de garantia. Realizando a compra nas instituições credenciadas no Bacen, estar-se-á protegido; pois caso ocorra algum problema e a casa de câmbio se negar a resolver, pode-se recorrer ao Bacen reclamando da casa de câmbio.

Portanto, deve-se sempre utilizar de instituições autorizadas pelo Banco Central (http://www.bcb.gov.br/pt-br/#!/n/INSTCRED). Além de garantir a legalidade da transação, evita-se problemas graves e em um país estrangeiro.

Conheça algumas das **condições do Banco Central** relativas às operações que envolvem moeda estrangeira:

1) É obrigatório o uso da moeda nacional em operações no Brasil;

2) A identificação do remetente é obrigatória em toda operação de câmbio;

3) A compra e a venda de moeda devem ser feitas em instituição autorizada a operar no mercado de câmbio ou em empresa conveniada;

4) Operações acima de US$ 3,000.00 (três mil dólares) serão necessariamente formalizadas mediante contrato de câmbio;

5) No território nacional, só é possível receber ou entregar moeda estrangeira em espécie nas compras e nas vendas de moeda estrangeira relacionadas a viagens internacionais;

6) Os recursos recebidos do exterior devem ser obrigatoriamente convertidos para reais.

Para **mandar dinheiro para o exterior**, basta ir até qualquer instituição financeira e solicitar o envio dos recursos por meio da transferência bancária por ordem de pagamento. Basicamente, será preciso informar os dados da pessoa que vai resgatar o dinheiro, bem como o código (*Swift*) do banco onde os recursos serão sacados. A característica principal desta operação é que o beneficiário deve necessariamente ter uma conta bancária. Ambas instituições financeiras (remetente e destinatária) cobrarão pelo serviço. A tarifa é conhecida como ordem de pagamento expedida. Assim, o depositante desembolsará uma taxa para que o dinheiro chegue ao destino pretendido, mesmo não sendo correntista do banco contatado. E, a agência que recebeu o montante, também descontará uma determinada quantia (cerca de 20 a 40 dólares no exterior e, no Brasil, de 20 a 100 dólares) do que irá disponibilizar ao cliente. O processo é o mesmo para quem deseja receber dinheiro do exterior. A transferência bancária é mais vantajosa para valores mais altos. Muitas vezes as agências de remessas não têm a política de mandar mais de US$ 10.000,00 (dez mil dólares) para o exterior para evitar lavagem de dinheiro.

- http://www.360meridianos.com/2014/09/como-levar-dinheiro-para-o-exterior.html;
- http://www.360meridianos.com/2014/09/como-transferir-dinheiro-para-o-exterior.html;
- http://www.pequenosmonstros.com/2016/04/transferir-dinheiro-do-brasil-para-o-exterior/.

Swift é uma sigla da “Society for Worldwide Interbank Financial Telecommunication”, que existe desde 1973 e é formada por bancos do mundo inteiro, sendo uma sociedade cooperativa sem fins lucrativos, pertencente e administrada por bancos que constituem seus membros. A rede

Swift, uma rede de computadores, serve para que os bancos troquem mensagens padronizadas, com segurança e rapidez, 24 horas por dia, sendo utilizada para transferência de dinheiro entre bancos.

- https://portal.febraban.org.br/pagina/3094/18/pt-br/swift.

O código *Swift*, na verdade ISO 9362 (também conhecido como código BIC), é uma norma da entidade aprovada pela ISO com a finalidade de identificar uma instituição bancária por meio de um código único de 8 ou 11 caracteres. Para indicar uma agência específica usa-se um código estendido de 11 dígitos. Grandes bancos, com várias agências e filiais pelo país e pelo mundo, podem ter vários códigos *Swift* para identificar cada região. Esses códigos são usados em transações financeiras interbancárias, principalmente em transferências internacionais, e algumas outras comunicações entre os bancos.

Para agilizar a operação e incentivar o recebimento de remessas por meio das suas instituições, a maioria dos bancos já disponibiliza formulários semipreenchidos em seus sites, com os SWIFTs devidamente indicados.

Para consultar os códigos *Swift* basta acessar o site da *Society for Worldwide Interbank Financial Telecommunication* (https://www2.swift.com/bsl/index.faces).

Entretanto, as operações internacionais podem ser feitas não só pelo sistema *Swift*, mas, também, por outros; tais como, por exemplos, o ABA - *American Banker's Association* (http://www.aba.com/) ou o *Fedwire* (https://frbservices.org/fedwire/index.html), sistema que serve para que os bancos norte-americanos façam pagamentos entre si mediante troca de reservas bancárias mantidas no FED (*Federal Reserve*), o Banco Central americano (http://www.federalreserve.gov/).

Atualmente (sem cogitar em moedas virtuais ou câmbio paralelo), as opções mais vantajosas para mandar regularmente quantias para outro país são a **transferência entre contas e a remessa sem conta no exterior**. Saiba mais em http://exame.abril.com.br/seu-dinheiro/noticias/seis-formas-enviar-ou-receber-dinheiro-exterior-564526.

Atualmente, ao efetuar uma remessa de dinheiro ao exterior, por uma das formas tradicionais ou convencionais, basicamente, se paga, no mínimo, 3 (três) encargos:

- **Taxa da transferência**: um valor fixo cobrado pela instituição financeira para realizar a operação;

- **IOF**: 0,38% sobre o valor a ser transferido;

- ***Spread* dólar**: palavra inglesa, que tem o significado de comparar, se refere à lacuna ou diferença entre dois valores, taxas, atos ou coisas, tais como, por exemplos: compra (procura) x venda (oferta), juros cobrados aos tomadores de crédito x juros pagos pelos bancos aos depositantes (captação de recursos), preço de custo x preço de venda, etc. No *spread* não consta somente a remuneração, contraprestação ou o lucro, mas também todas as despesas da operação que não foram calculadas separadamente, o desgaste (conservação, manutenção, reparos, substituição e modernização) e insumos (todos os elementos consumidos) da infra estrutura utilizada, despesas com perdas, infortúnios, acidentes, calamidades, seguros, indenizações, etc. Assim, trata-se da diferença entre o preço de mercado do dólar e o preço que a instituição está cobrando pelo dólar.

Há, ainda, a possibilidade do ressurgimento da CPMF (Contribuição Provisória sobre Movimentação Financeira) e sua eventual incidência. Em 2016 tentaram, em vão, incluir ela no orçamento de 2017; mas, volta e meia, tentam ressuscitá-la.

Sempre que alguém precisa fazer pagamento ou recebimento envolvendo moedas de países diferentes, seja para viagem internacional, doação, compra de produtos ou outro motivo qualquer, é necessário trocar a moeda de um país pela moeda de outro país. Isso caracteriza uma operação de câmbio. E o dólar é a moeda internacional.

- http://www.bcb.gov.br/?MERCCAMFAQ;

- http://www.receita.fazenda.gov.br/dvssl/atbhe/falecon/comum/asp/formulario.asp?topico=191;
- http://www.bcb.gov.br/?cambio;
- http://www.bcb.gov.br/?TXCAMBIO;
- http://www.bcb.gov.br/?CAMBIOLEGRESUMO;
- http://www.bcb.gov.br/Rex/LegCE/Port/circulares.asp?idpai=RMCCI.

No Brasil, o mercado de câmbio, em que são realizadas as operações cambiais, é regulamentado pelo CMN - Conselho Monetário Nacional (http://www.bcb.gov.br/Pre/CMN/Entenda%20o%20CMN.asp) e pelo Bacen - Banco Central do Brasil (http://www.bcb.gov.br/pt-br/#!/n/CAMBIO).

Os recursos recebidos do exterior destinados a residentes devem ser obrigatoriamente convertidos em reais em instituição autorizada a operar no mercado de câmbio pelo Banco Central do Brasil. Da mesma forma, a moeda estrangeira destinada ao exterior deve ser adquirida nessas instituições. As operações de câmbio feitas em desacordo com essas condições são consideradas ilegais.

Não é necessário qualquer tipo de autorização governamental para fazer remessas do Brasil para o exterior e nem para receber recursos do exterior. As operações de câmbio com recebimento ou entrega de moeda estrangeira em espécie tem se restringido aos casos de viagens internacionais.

A Lei n.º 7.492/1986 (http://www.planalto.gov.br/ccivil_03/leis/L7492.htm), no artigo 22, define como sendo crime "Efetuar operação de câmbio não autorizada, com o fim de promover evasão de divisas do País" ou quem "a qualquer título, promove, sem autorização legal, a saída de moeda ou divisa para o exterior, ou nele mantiver depósitos não declarados à repartição federal competente".

Já o artigo 65 da Lei nº 9.069/1995 (http://www.planalto.gov.br/ccivil_03/leis/L9069.htm) reza que: "O ingresso no País e a saída do País de moeda nacional e estrangeira devem ser realizados exclusivamente por meio de instituição autorizada a operar no mercado de câmbio, à qual cabe a perfeita identificação do cliente ou do beneficiário.".

Convém lembrar a Lei n.º 13.254/2016 (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/l13254.htm), que versa sobre o RERCT (Regime Especial de Regularização Cambial e Tributária); ou seja, visa a repatriação de dinheiro brasileiro no exterior. A Receita Federal a regulamentou através da IN (Instrução Normativa) RFB nº 1627/2016 (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=72224). O prazo de adesão ao regime teve início no dia 04/04/2016 e, a data limite, foi 31/10/2016.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/declaracoes-e-demonstrativos/dercat-declaracao-de-regularizacao-cambial-e-tributaria/perguntas-e-respostas-dercat;

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/declaracoes-e-demonstrativos/dercat-declaracao-de-regularizacao-cambial-e-tributaria/dercat-orientacoes-gerais.

As instituições integrantes do sistema financeiro que podem ser autorizadas a operar no mercado de câmbio são os bancos, a Caixa Econômica Federal, as corretoras, distribuidoras e sociedades de crédito, financiamento e investimento, além de agências de fomento.

- http://www.bb.com.br/portalbb/page20,116,3417,1,1,1,1.bb?codigoNoticia=238&codigoMenu=12953&codigoMenu=12953;

- http://www.caixa.gov.br/site/Paginas/pesquisa.aspx?k=c%C3%A2mbio.

A remessa de dinheiro do Brasil para o exterior e vice-versa (do exterior para o Brasil), pode ser feita de forma prática e segura de três maneiras diferentes: por intermédio de instituição autorizada pelo Banco Central do Brasil a operar em câmbio através de ordem de pagamento, por cartão internacional ou pelos Correios.

A lista das instituições autorizadas a operar no mercado de câmbio pode ser encontrada na página do Banco Central do Brasil, no endereço http://www.bcb.gov.br/?INSTCRED.

Qualquer informação adicional, inclusive sobre os correspondentes cambiais contratados, pode ser obtida diretamente no Banco Central do Brasil – seja presencialmente nas cidades onde há representação desta autarquia, pelo telefone 0800-9792345 ou, ainda, por meio do endereço http://www.bcb.gov.br/?PORTALATEND.

É possível aos **bancos brasileiros e à Caixa Econômica Federal** aceitar remessas de valores dos brasileiros que estão no exterior por meio de cartão emitido no exterior. O valor, em reais, pode ser creditado em conta corrente ou poupança no Brasil, do próprio remetente ou de outro beneficiário, ou ser recebido em dinheiro, diretamente pelo beneficiário, desde que observado o limite em vigor de R$ 10.000,00 (dez mil reais).

Quem é cliente do **Banco do Brasil** pode ir a qualquer agência do banco que tenha a função câmbio para enviar dinheiro para qualquer lugar do mundo. É possível também ativar essa função através do *internet banking*. O BB Remessa é uma solução que permite o envio de moeda estrangeira para o Brasil diretamente dos Estados Unidos, Portugal, Áustria, França, Itália, Alemanha, Inglaterra, Espanha e Japão, de forma rápida e descomplicada. Os beneficiários podem optar por receber o dinheiro em conta corrente/poupança ou, ainda, retirar a quantia disponível nas agências do BB em todo o País.

- https://bbremessa.com/;
- http://www.bb.com.br/pbb/pagina-inicial/voce/produtos-e-servicos/contas/todos-os-servicos/remessas-de-recursos-do-exterior-para-o-brasil-e-do-brasil-para-o-exterior#/.

O **Banco do Brasil** (BB) disponibiliza aos clientes a remessa de recursos para o exterior pela Internet, com débito em conta corrente ou conta de poupança. Essas remessas podem ser realizadas até US$ 3,000.00 (três mil dólares) por pessoas físicas e US$ 100,000.00 (cem mil dólares) por pessoa jurídica. Através do BB, as transferências de valores feitas para o exterior, além do IOF (0,38%), têm a tarifa de (1,66%). Caso o cliente opte em pagar as despesas externas (*Swift*) na origem, será cobrado adicionalmente o valor de US$ 100.00 (cem dólares).

O Banco do Brasil, ainda, possui convênio com a Western Union (http://www.bb.com.br/wu).

- http://www.bb.com.br/pbb/pagina-inicial/atendimento/western-union#/.

Travel check (cheque de viagem) é uma modalidade que está em desuso porque os cartões eletrônicos são, evidentemente, mais práticos. São como cheques comuns que podem ser trocados por dinheiro ou mesmo usados diretamente em locais que os aceitam; mas não são todos os estabelecimentos que aceitam e, mesmo nos que aceitam, ou é difícil uma casa de câmbio com conversão justa ou uma empresa que não cobre uma taxa adicional.

- https://www.citibank.com.br/cambio/travelers_cheques.html;
- http://www.bradescocambio.com.br/index.asp?pag=produtos/pro_ven_cont.asp;
- http://banco.bradesco/html/classic/produtos-servicos/cartoes/servico-de-cambio-e-travelers-cheques.shtm;
- https://www.santander.com.br/portal/wps/script/templates/GCMRequest.do?page=6127;
- http://ww2.itau.com.br/universitarios/produtos.aspx/embarque/compra-traveller-cheque;
- http://www.agkcorretora.com.br/pagina/travellers-cheques;
- http://www.safranet.com.br/safranet/servicos/travelers.asp?FlagPagina=travelers.

Também existe o Cartão de Viagem Multimoeda Cash Passport do Daycoval Câmbio (http://portal.daycovalcambio.com.br/ParaVoce/CartoesViagem).

O **Visa Travel Money** (VTM) é um cartão internacional pré-pago, recarregável em dólar ou em euro, com acesso à rede de caixas eletrônicos da Visa/Plus, para uso em viagens internacionais (https://www.visa.com.br/pague-com-visa/cartoes/cartoes-pre-pago/visa-travelmoney-detalhes.html).

O VTM pode ser usado para compras e saques na moeda local do seu destino. O pagamento de compras somente é válido em estabelecimentos afiliados à rede Visa. É aceito em mais de 30 milhões de estabelecimentos

filiados à VISA (restaurantes, lojas entre outros) e um milhão de caixas automáticos (ATMs) Visa Plus distribuídos por 150 países ou em lojas “duty free” nos aeroportos do Brasil e do exterior. Possui central de atendimento gratuita 24 horas por dia em português. Os caixas eletrônicos no exterior podem cobrar taxas de serviços por volta de € 2,50 em cada saque. Os bancos que emitem o VTM como o Banco do Brasil e o Bradesco exigem conta corrente no próprio banco, bem como podem cobrar tarifas adicionais (de € 3,00 a € 5,00) para manutenção da conta VTM.

- https://www.visa.com.br/pague-com-visa/cartoes/cartoes-pre-pago/visa-travelmoney-detalhes.html;
- https://s7study.com/cartao-visa-travel-money/perguntas-frequentes/;
- https://www.e-dublin.com.br/voce-sabe-usar-bem-o-seu-visa-travel-money-vtm/;
- http://www.bb.com.br/pbb/pagina-inicial/estilo/produtos-e-servicos/cartoes/todos-os-cartoes/ourocard-visa-travelmoney#/.

O **MasterCard Cash Passport** (http://www.cashpassport.com/1/pt/Brasil/single-currency/) é muito semelhante ao VTM, possui parceria com a Travelex financeira (https://www.travelexae.com/) e pode ser carregado com dólar americano, libra esterlina ou euro.

O **aQui CARD** (https://www.aquicard.com.br/) é um cartão pré-pago sem mensalidade ou anuidade, que pode ser carregado por meio de boleto no site aquicard.com.br e app aQUI! CARD, através da Central de Atendimento e nas lojas credenciadas com o serviço de Recarga MasterCard pré-pago usando a maquininha da GetNet (https://www.getnet.com.br/).

Também existe a opção do **American Express Global Travel Card**, que cobra 4% de tarifa na conversão, bem como o pagamento de compras somente é possível em um estabelecimento afiliado à rede Amex (https://www.neteller.com/pt/features/cards).

- https://www.americanexpress.com/brazil/personal/travel/prepaid-travel-card/Sobre-o-Cartao.shtml#/gtc-fees.html.

Já o cartão **Itaú Travel Money** (https://ww2.itau.com.br/hotsites/itau/solucoes_viagem/travel-oquee.html) pode ser carregado em dólar americano, euro ou libra esterlina. O cartão é aceito em milhões de estabelecimentos, como lojas, restaurantes, hotéis e muitos outros, e também em caixas eletrônicos espalhados por todo o mundo conveniados às redes Cirrus e Plus.

O **Wirex** (https://wirexapp.com/pt/travel-debit-card.html) também é outro cartão pré-pago para viagens.

Mais uma opção é o **cartão Mastercard *Travel Card*** (http://www.mastercard.com/br/consumidores/travel_card.html).

O **CI Travel Money** (https://www.ci.com.br/fazer-uma-viagem/ci-travel-money) ou *Cash Passport Multi Moedas MasterCard*, é um cartão internacional da bandeira MasterCard, que é recarregável, pré-pago e multimoda; ou seja, é possível carregar 6 diferentes moedas em um único cartão, são elas: Dólar Americano, Euro, Libra Esterlina, Dólar Australiano, Dólar Canadense e Dólar Neozelandês.

- http://www.trevisocc.com.br/multimoedas.

O **STB Cash Passport** é o cartão de débito internacional (http://www.stb.com.br/tudo-para-sua-viagem/cartao-travel-money/).

Há, ainda, o **cartão Multi Moeda Cash Passport** (https://www.confidencecambio.com.br/produtos/cartao-pre-pago/).

Outra opção é sacar da própria conta corrente do Brasil, por meio de um **cartão de débito** internacional filiado às bandeiras Cirrus e Plus. A modalidade facilita, pois quem fica no Brasil deposita a quantia necessária, em reais, na conta corrente da pessoa que está fora, e esta saca nos caixas eletrônicos do próprio banco (caso este possua agência no exterior) ou de correspondentes. Antes de embarcar, deve-se verificar se o banco e o cartão permitem esse tipo de transação e, além disso, checar o limite para saques no exterior. Tal operação é tarifada e os valores variam de banco para banco e, em algumas situações, de acordo com o valor do saque.

Em regra, os **cartões de crédito** emitidos por bancos locais são limitados a compras nacionais em reais. Desse modo, os cartões bancários somente são válidos dentro do território nacional. Para poder usá-los no exterior é necessário comunicar a agência bancária; ou seja, pedir habilitação ou, no máximo, apenas conseguirá acessar caixas eletrônicos da própria instituição.

A habilitação do cartão para uso no exterior é exigida também para compras feitas pela Internet. Transações realizadas em sites hospedados fora do Brasil somente serão processadas se o cartão estiver habilitado para uso no exterior. A habilitação pode ser feita na Internet, no aplicativo do celular, nos caixas eletrônicos ou pela Central de Atendimento da instituição bancária. O titular da conta é que vai determinar o tempo que o cartão ficará com as funções liberadas para uso no exterior.

Economize em compras no exterior usando cartão de débito Internacional (como, por exemplo, o **ADVCash** - http://advcash.com/en/), em dólar, emitido por uma empresa estrangeira (sem IOF, portanto) e carregado em bitcoins (podendo comprar dólar mais barato do que a cotação do dólar turismo), por exemplo, na **FOXBIT** (https://foxbit.com.br/). Também há opção do cartão da **Neteller** (https://www.neteller.com/pt).

O cartão **InstaForex Benecard** (https://www.instaforex.com/pt/instaforex_benecard), fornecido aos clientes da InstaForex (https://www.instaforex.com/pt/), também pode ser uma opção; ainda mais que, também, trabalha com bitcoins (https://www.instaforex.com/pt/bitcoin_trading). A **Bitnovo** (https://www.bitnovo.com/tarjeta-monedero-bitcoins), é uma plataforma espanhola de pagamentos com bitcoin, que conta com cartões de débito carregados com bitcoin para serem usados em lojas e caixas eletrônicos que aceitem MasterCard. Outra dica, a **Paysafecard** (https://www.paysafecard.com/pt-pt/) é líder no mercado europeu de meios de pré-pagamento. Confira, ainda, os seguintes links:

- https://www.weswap.com/it/;
- https://www.schwab.com/;
- https://www.okpay.com/pt/personal/payment-cards/;
- https://www.okpay.com/pt/personal/fees/;

- https://www.bil.com/en/Pages/Index.aspx;
- https://www.dkb.de/;
- https://www.wirecardbank.com/;
- https://avuba.de/;
- https://www.fidor.de/;
- https://www.fidorbank.uk/;
- https://www.hype.it/;
- https://worldcore.eu/;
- https://www.leupay.eu/;
- https://n26.com/;
- https://www.paymix.eu/;
- https://www.papaya.eu/;
- https://www.paysera.com/;
- https://www.paxum.com/;
- https://www.payoneer.com/;
- https://revolut.com/;
- http://www.smartpaycard.net/si/default.wlgt;
- http://www.veritascard.com/;
- https://vikingcard.com/en/;
- https://www.viabuy.com/;
- http://boonpayment.com/.

O **Advcash** (http://advcash.com/en/) é um cartão de débito que pode ser recarregado com bitcoin. Ele é ideal para quem precisa comprar no exterior ou até mesmo no Brasil usando a moeda virtual. O Advcash é emitido por uma instituição financeira sediada em Belize, um pequeno país no mar do Caribe. A vantagem da Advcash é que o cliente pode escolher entre um cartão com dólar ou euro. A vantagem de ter os dois cartões é não pagar nenhuma tarifa para comprar em sites ou estabelecimentos que usam o dólar ou o euro como moeda. Há duas opções de cartões, o virtual e o físico, ambos são emitidos com a bandeira MasterCard. Tanto o virtual e o físico possuem validade de 3 (três anos) contados a partir da data de emissão do cartão.

O cartão da **Uquid** (https://uquid.com/), permite o uso de 40 (quarenta) diferentes altcoins através da rede global da Visa (https://bitcointalk.org/index.php?topic=1485950.0).

- http://www.btcsoul.com/2016/11/26/nasce-o-cartao-visa-que-aceita-suas-altcoins/.

O cartão de débito Visa do Uquid (https://uquid.com/uquid-card) também é o primeiro no mundo a oferecer o carregamento ilimitado e gastos sem

verificação de identidade. Além disso, os usuários podem carregar cartões com uma enorme seleção das altcoins mais populares, incluindo Ethereum, Ripple, Litecoin, Monero, Dash, Augur, MaidSafeCoin, Steem, Dogecoin e muito mais. As principais vantagens do cartão Uquid inclui nenhuma identificação ou verificação de crédito necessário, a emissão instantânea e entrega gratuita em todo o mundo, o suporte da placa ilimitada e zero por cento de taxas de ponto-de-venda. Os clientes também podem obter cartões virtuais denominados em GBP, EUR ou USD. Os cartões de débito vêm com AVS de harmonização e o cartão Uquid também pode ser recarregado a partir de qualquer processador de pagamento em todo o mundo. Os usuários Uquid também pode recarregar instantaneamente qualquer número de telefone celular em 150 países e em mais 600 operadores móveis de todo mundo.

Outra opção é o **Banco Intermedium** (https://www.intermedium.com.br/), que é um banco completo 100% gratuito, online, isento de tarifa bancária e com cartão de débito Mastercard. O usuário abre uma conta corrente como se fosse um banco comum e passa a ter acesso a todas as opções geralmente reservadas a bancos convencionais, como transferências TED e DOC para outros bancos, pagamentos de boletos através do Pague Fácil Intermedium e saques em caixas eletrônicos do Rede Banco 24 horas. No Intermedium a conta é totalmente gratuita e isenta de tarifas até mesmo para serviços como TED e Saque na rede 24h. Enfim, a propaganda é de tudo ser sem taxas, cobranças ou limites de transações; mas deve ter algumas exceções. O cliente recebe um cartão múltiplo habilitado na função débito. A ativação do cartão de crédito pode ser solicitada e passa por uma análise. Não há a cobrança de anuidade! O cliente Intermedium tem lastro garantido para investir nas opções de LCI da instituição (CDI, IPCA e IGPM) e, ainda, conta com os outros produtos de investimentos do banco, como o CDB. Todo o atendimento é feito via smartphone (sistemas Android e iOS), além de chat, no horário bancário, para pendências mais detalhadas. Depois de aberta a conta, é possível enviar um e-mail com documentos (RG [identidade] e comprovantes de endereço e de renda) solicitando a liberação de limite de crédito no cartão MasterCard.

Há, ainda, o **Banco Neon** (https://www.banconeon.com.br/), com cartões (um físico e outro virtual) internacional, de débito, na bandeira Visa, sem

mensalidade e nem anuidade, participante do programa de benefícios "Vai de Visa" (https://www.promocoesvisa.com.br/vaidevisa/site) e que também é operado por aplicativo de smartphone. O usuário poderá fazer operações diversas pelo celular, como verificar saldo, realizar transferências, pagar contas, receber pagamentos. Os usuários podem fazer um saque pela rede 24horas e um TED por mês de graça. Para fazer um depósito para a conta, o Neon recorre ao bom e velho boleto. Quando a transação é solicitada, o *app* gera um boleto que o usuário pode pagar em qualquer lotérica. O cartão do Neon só permite compras na função débito atualmente. O atendimento ao cliente é feito, 24 horas por dia, 7 dias por semana, por telefone 0800, por chat dentro do próprio aplicativo e através das redes sociais (FaceBook, Twitter, Instagram e LinkedIn).

O **Brasil Pré-Pagos** (https://www.brasilprepagos.com.br/brasil-prepago-digital.html) possui o cartão pré-pago digital que permite compras em sites internacionais sem precisar de um cartão de crédito internacional. O cartão é carregado, através de boleto ou cartão de débito, com o qualquer valor e o controle é feito em tempo real pelo app disponível para iOS e Android.

Acesso (https://www.acessocard.com.br/) é um cartão pré-pago da MasterCard que permite saques nas redes Cirrus ou Camisarias Colombo. O cartão possui custo.

Conta Super (http://www.contasuper.com.br/), do Santander, é um cartão pré-pago internacional da Mastercard, com diferentes planos de taxa. Só é possível sacar na rede Banco24Horas (que possui taxa) e só dá para transferir dinheiro para outras pessoas que também tenha Conta Super (sem pagar nenhuma taxa).

PayPaxx (https://paypaxx.com.br/) é um cartão pré-pago para empresas para controle de despesas pelos funcionários.

Contaum (https://www.contaum.com.br/) é uma conta corrente digital com um cartão de crédito internacional e pré-pago, que incorpora benefícios, promoções e serviços exclusivos. Para carregar o cartão basta entrar no site e gerar um boleto com o valor que desejado para disponibilizar na conta. Usufrui dos benefícios do programa MasterCard Surpreenda. É voltada para

as necessidades empresariais. Os usuários das contas salário possuem taxas de movimentação da conta menores que de um banco tradicional e podem fazer pagamentos de contas, transferências, consulta de saldo e extrato, saques, recarga de celular, a qualquer momento e sem taxas com direito a todo o suporte de atendimento através do menu Ajuda do aplicativo, no próprio celular.

O **Cartão Petrobras Visa International** é sem anuidade, sem taxa de adesão, sem tarifas de manutenção e de extrato. Possui programa de pontos e descontos e benefícios em diversos parceiros comerciais conveniados.

- http://www.br.com.br/wps/portal/portalconteudo/cartaopetrobras.

O **Nubank** (https://www.nubank.com.br/) é um cartão de crédito internacional da Mastercard, na variante Gold (http://www.mastercard.com/br/consumidores/gold-mastercard.html), livre de anuidade e de taxas de cadastro, emissão e manutenção (serviços básicos), com as demais taxas e os juros inferiores aos concorrentes convencionais, o primeiro cartão gratuito e com controle total através do smartphone com sistema iOS ou Android (cadastro e solicitação 100%, atendimento 100% via chat, faturas 100% online se possuir conta bancária com acesso ao *internet banking*, etc.). Um dos seus concorrentes é o **Digio** (http://digio.com.br/); administrado pelo Banco CBSS (http://www.bancocbss.com.br/), uma instituição financeira pertencente a Elo Participações S/A (*holding* do Banco do Brasil, do Bradesco e da Caixa Econômica Federal), que oferece os mesmos benefícios do Nubank; mas com a bandeira Visa, na modalidade Classic (https://www.visa.com.br/pague-com-visa/cartoes/cartoes-de-credito/visa-classic-detalhes.html). Nos dois cartões o desbloqueio é feito de forma online no próprio aplicativo e funciona instantaneamente. Nenhum dos dois oferece pontos ou milhas; mas o Nubank possui os pontos do MasterCard Surpreenda (https://surpreenda.naotempreco.com.br/rewards/vouchers/surpreenda) e o Digio pode passar a ter os pontos do programa Livelo (http://www.pontoslivelo.com.br/). Não existem seguros de viagem, locação de veículos, seguro saúde e outras vantagens de alguns cartões comuns. Não há crédito rotativo para quem quiser parcelar a fatura em atraso, o cliente terá que parcelar o valor. O Nubank possibilita que o cliente em dificuldade

pague um valor mínimo na data de vencimento de sua fatura, pagando juros pelo restante até que haja quitação total ou parcial. O Digio não oferece essa opção, assim que ocorrer o atraso o cliente terá que parcelar a dívida total, acordando uma taxa de juros no momento do parcelamento. A modalidade é parecida com uma renegociação da dívida, a diferença é que a fatura do cartão de crédito se torna um empréstimo pessoal com juros também bastante altos. **Dos dois, o Nubank é o melhor** por cobrar menos taxas, a bandeira Mastercard Gold oferecer mais vantagens que o Visa Classic e o atendimento do Nubank ser muito superior. O Nubank só perde por ainda precisar de convite e por ter passado a cobrar anuidade pelo programa de fidelidade do cartão. Conselho, não use o Nubank para pagar compras no Ebay (PayPal) para evitar dupla conversão Real - Dólar

- http://emalta.com.br/visa-ou-mastercard-comparativo-cartoes-credito/.

Também existe a conta corrente 100% digital, sem tarifas e cartão de crédito com condições especiais do **Banco Original** (https://www.original.com.br/), do grupo J&F, dono de empresas como a Friboi e Havaianas. A conta é totalmente digital (desde que a conta corrente seja aberta através do aplicativo do Banco Original para Android ou iOS) e tudo é feito de forma online. Se o cliente abrir a conta pelo seu smartphone, em momento algum precisa imprimir, assinar ou enviar papéis. A exceção fica para a conta aberta pelo computador (restrita à algumas cidades), onde um gerente do banco irá até a residência do cliente coletar os papéis da abertura de conta assinados. O aplicativo permite depósito de cheque através de fotografias enviadas pelo smartphone. Existem, ainda, alguns locais chamados de “espaço original”, onde o cliente pode realizar depósitos em espécie. Caso precise sacar dinheiro em espécie, a opção é realizar saques pelo Banco24Horas (http://banco24horas.com.br/). Quem ainda trabalha com dinheiro vivo pode ter muitas dificuldades em realizar depósitos e custos altos para realizar saques no Original. O foco não é ser uma opção 100% gratuita, e sim apostar na praticidade e redução de custos nas suas operações. **Diferente do Digio e do Nubank, que se restringem ao serviço de cartão de crédito, o Banco Original oferece conta corrente, com cartão** (https://www.original.com.br/pessoafisica/cartoes/) de débito ou crédito (se aprovado) e opções para aplicação de valores (CDB e não é possível aplicar em fundos de investimento ou no Tesouro Direto, aplicação

mínima de R$ 5.000,00 [cinco mil reais], não há aplicação automática, oferece gerenciador financeiro completo). Não há opção para pagamento de boletos de arrecadação (luz, água, telefone, etc.), apenas boletos de cobrança comuns. O cliente conta com atendimento personalizado, com um gerente e consultores, através por telefone, site oficial, vídeo chamada ou via chat no aplicativo do celular. Trata-se de um banco tradicional cujo principal diferencial é a forma de atendimento. As tarifas cobradas são em geral iguais ou superiores às dos bancos tradicionais. A "franquia original", como é chamado o pacote básico de conta corrente do banco, oferece mensalmente 10 folhas de cheque, 5 saques na Rede24horas, 2 transferências entre bancos que podem ser via TED ou DOC e transferências entre contas do banco ilimitadas.

Outros bancos tradicionais também estão migrando para a virtualização. O Banco do Brasil, conta com a **Conta Fácil BB**, que pode ser aberta por meio de um aplicativo para celular nos sistemas Android e IOS.

- http://www.bb.com.br/pbb/pagina-inicial/voce/produtos-e-servicos/cartoes/cartoes-com-promocoes-e-vantagens-especiais/conta-facil#/;
- http://www.bb.com.br/pbb/pagina-inicial/voce/produtos-e-servicos/contas/conta-facil#/.

Depois de descontinuar a conta digital, que oferecia serviços bancários sem cobrança de pacote de serviços, o Banco do Brasil a relançou reformulada com o nome de Conta Fácil BB. Trata-se de uma conta de pagamento para maiores de 18 anos que não possuam conta no Banco do Brasil. A conta não substitui integralmente uma conta corrente. Conforme regulamentação do Banco Central, a conta de pagamentos tem limite de movimentação mensal de R$ 5.000 e não tem serviços de crédito e investimentos associados. Serão dois pacotes de conta. Um gratuito e um segundo com cobrança de R$ 9,90 por mês, conversíveis em créditos para celular. Com a Conta Fácil BB é possível realizar saques, depósitos em dinheiro, transferências, pagamentos, recarga de telefone celular e compras com cartão de débito Ourocard Conta Fácil (bandeira Elo). Cadastrar débito automático para contas (água, luz, telefone, etc.), contratar consórcios, seguros e título de capitalização. Registrar a Livre Opção Bancária (LOB) para permitir o crédito do salário. A movimentação é realizada no celular e

tablet, através do aplicativo BB. Também estão disponíveis os Terminais de Autoatendimento BB, terminais compartilhados (BRB – Banco de Brasília), Banco 24 horas, Lotéricas e rede de correspondentes Banco Postal ou Mais BB.

- http://www.bb.com.br/pbb/pagina-inicial/voce/produtos-e-servicos/contas/conta-facil#/;
- http://www.bb.com.br/pbb/pagina-inicial/voce/produtos-e-servicos/contas/conta-facil/perguntas-frequentes#/.

O Itaú, por sua vez, possuía a **iConta** (https://www.itau.com.br/conta-corrente/abra-sua-conta/iconta/); uma conta digital e sem tarifa, que é operada por um aplicativo para smartphones.

Pelos sites http://www.goodfinancialcents.com/best-cash-back-credit-cards/ e http://www.mybanktracker.com/credit-cards é possível **comparar os cartões americanos** e, em http://www.comparecards.com/reward os programas de recompensas de cartões americanos. Já em https://www.comparaonline.com.br/cartao-de-credito e https://comparabem.com.br/cartoes-credito compara-se os **cartões de créditos brasileiros**. Também é possível comparar os bancos em https://wallethub.com/banks/ e http://banks.credio.com/; em http://www.findabetterbank.com/ é possível localizar mais bancos. Já no Brasil, é possível comparar as tarifas bancárias em http://www.febraban-star.org.br/ e http://www.febraban-star.org.br/CompararTarifaPasso1.asp. Sobre bancos europeus, há uma relação em https://pt.wikipedia.org/wiki/Lista_de_bancos_da_Europa.

A enorme vantagem da bitcoin e das altcoins é que podem, em poucos minutos, serem enviadas para qualquer pessoa, em qualquer parte do mundo, desde que o destinatário (recebedor) também possua uma conta (endereço) para o recebimento da moeda virtual. Por não possuírem regulamentação, não há cobrança de tributos e nem de tarifas pela sua utilização. Já o cartão de crédito, diferentemente, está sujeito às anuidades, tarifas, juros e tributos que devem ser pagos pelos seus utilizadores. E, detalhe, o uso das moedas criptográficas, em regra, não é rastreado pelos governos, enquanto que o uso do cartão de crédito é.

Em geral, o valor de qualquer compra que se faça com **cartão de crédito no exterior** é convertido pela média do dólar comercial no dia do fechamento ou do vencimento da fatura (e não do uso ou da compra) e nesse período o dólar pode subir ou cair. Inclusive, haverá um câmbio da moeda local para dólar e, depois, do dólar para real. A vantagem do cartão de débito em relação ao de crédito é que o câmbio é do dia do uso do cartão. Além desses câmbios duplos e imprevisíveis, também há a cobrança da taxa da operação de câmbio e a incidência do IOF (6,38%) e, ao ingressar no Brasil com o produto, existe a tributação do II (Imposto de Importação) e, dependendo, até do ICMS (Imposto sobre Operações Relativas à Circulação de Mercadorias e Serviços). Pior. A interpretação dada pela Receita Federal é que o envio de dinheiro ao exterior (para custear gastos pessoais lá fora de pessoas físicas que morem no Brasil) em viagens de turismo, negócios, serviço, treinamento ou missões oficiais estão sujeitas a pagar a alíquota de 6% (seis por cento) de **Imposto de Renda**, seja qual for o valor remetido. Como todo tributo, há períodos de isenção, suspensão e revisão do índice aplicado.

- IN - Instrução Normativa da RFB 1645/2016 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=74319#1632332.

Anteriormente à Instrução Normativa 1645/2016 da Receita Federal do Brasil, a Instrução Normativa RFB 1611/2016 rezava que eram 25% (vinte e cinco por cento). Cuidado, há muitos sites com a informação desatualizada. No final do capítulo anterior, antes dos links para saber mais, constam algumas alterações e atualizações sobre Imposto de Renda.

O artigo 60 da Lei n.º 12.249/2010 (http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Lei/L12249.htm), na redação dada pela Lei n.º 13.315/2016 (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13315.htm) reza que: "**Até 31 de dezembro de 2019, fica reduzida a 6%** (seis por cento) **a alíquota do imposto de renda retido na fonte incidente sobre os valores** pagos, creditados, entregues, empregados ou remetidos para pessoa física ou jurídica residente ou domiciliada no exterior, **destinados à cobertura de gastos pessoais, no exterior, de**

pessoas físicas residentes no País, em viagens de turismo, negócios, serviço, treinamento ou missões oficiais, **até o limite global de R$ 20.000,00 (vinte mil reais) ao mês**, nos termos, limites e condições estabelecidos pelo Poder Executivo." (Grifo nosso).

Todos esses encargos dificultam o cálculo do valor final da fatura do cartão; principalmente por causa da imprevisível cotação do dólar no dia e, assim, não se tem como saber antecipadamente qual será a taxa de câmbio praticada pela operadora. Nesse valor costuma ainda ser adicionada uma margem de lucro do banco, que varia em cada instituição. Algumas operadoras de cartão de crédito, ainda, cobram taxas adicionais na função "débito" no exterior. Além dos impostos cobrados nestas operações e das taxas pelo serviço, os juros são bem parecidos com os cobrados no crédito rotativo. Explica-se. O saque com cartão de crédito internacional é considerado um empréstimo e tem, portanto, um custo bem alto. Em contrapartida, o cartão de crédito oferece maior segurança contra fraudes e pode ser vantajoso concentrar as despesas nele para acumular milhas ou pontos de programa de fidelidade. Além disso, alguns ainda têm serviços extras, como seguros de viagens. Mas antes de viajar para fora do país, costuma ser necessário liberar o cartão na operadora para compras no exterior; pois mesmo os cartões internacionais estão sujeitos a bloqueios nas centrais. Enfim, é a maneira mais corriqueira de conseguir dinheiro fora do país; porém, a mais cara também.

A remessa de valores para cobrir gastos pessoais de dependentes no exterior, via de regra, não é considerada rendimento e, por isso, a alíquota de Imposto de Renda não é cobrada neste caso.

Ao reservar um hotel ou outro tipo de hospedagem pelo Booking.com ou demais agências físicas ou virtuais, não haverá incidência de imposto quando optar pelo pagamento direto no hotel. O mesmo vale para reservas de qualquer natureza com pagamento no próprio estabelecimento, em espécie (com IOF ao comprar dólar em bancos ou casas de câmbio) ou cartão de crédito (com IOF), já que nesses casos não há remessas de valores para o exterior.

Não há cobrança se for preciso transferir dinheiro para cobrir custos com serviços médicos ou despesas hospitalares fora do Brasil. De igual forma, os gastos com educação.

A compra de medicamentos no Brasil somente é permitida para aqueles que são liberados pela ANVISA - Agência Nacional de Vigilância Sanitária (http://portal.anvisa.gov.br/). Ainda mais, a Anvisa também define quais substâncias são consideradas drogas ilícitas (Lei nº 11.343/2006, parágrafo único do artigo 1º).

- http://www.anvisa.gov.br/hotsite/talidomida/legis/Portaria_344_98.pdf.

No caso das passagens aéreas vendidas por agências de turismo, uma lei permite a isenção do IR (Imposto de Renda) quando o imposto é cobrado nos dois países onde a empresa atua (a chamada "dupla tributação"). A companhia do exterior que opera aqui fica isenta se houver acordo de reciprocidade com o Brasil. Caso contrário, a alíquota é de 15% (quinze por cento).

Também é possível fazer a remessa de moeda estrangeira do exterior por meio de **empresas não financeiras especializadas** em transferências externas, dependendo da legislação de cada país. Para fazer a remessa, o remetente, no exterior, normalmente deve procurar uma instituição que ofereça o serviço de transferência de valores com utilização de cartão internacional.

Outra opção é efetuar a remessa internacional através de uma casa ou agência **corretora de câmbio**. Os bancos têm prestigio e passam uma sensação de segurança maior, mas essa sensação tem um custo, por isso se conferir as tarifas bancárias, constatará que as custas são bem menores com as agências de câmbio. O agente de câmbio é sempre mais arriscado que fazer via banco; geralmente são instituições menores e pode ocorrer de ter alguns agentes trabalhando mesmo sem ser credenciado pelo Banco Central para enviar remessas ao exterior (http://www.bcb.gov.br/pt-br/#!/n/INSTCRED). Por isso, é muito importante consultar a lista do Banco Central para ver se a instituição tem autorização para transferir dinheiro para o exterior. Pode ocorrer de o agente de câmbio vender a moeda estrangeira e

terceirizar o serviço de remessa ao exterior; desde que o terceirizado seja uma das instituições autorizadas pelo Bacen para fazer as transferências, não tem nenhum problema.

Compras ou vendas de moeda estrangeira relacionadas a viagens internacionais, bem como transferências unilaterais (doações, manutenção de residentes, dentre outras), desde que limitadas a US$ 3,000.00 (três mil dólares), também podem ser realizadas em correspondentes contratados por **instituições autorizadas a operar em câmbio**. Qualquer empresa regularmente autorizada a exercer uma atividade comercial pode ser contratada por instituição financeira autorizada a operar em câmbio para ser seu correspondente. Pode-se consultar a lista dos correspondentes em operações de câmbio na página do Banco Central do Brasil, no endereço http://www.bcb.gov.br/?IAMCCCA.

As **agências de turismo**, não conveniadas que detenham autorização do Banco Central para esse fim, podem negociar moeda estrangeira relacionada a viagens internacionais.

Resumindo, é possível fazer a remessa diretamente por meio de **instituição autorizada a operar no mercado de câmbio** ou, no caso de transferências até o equivalente a US$ 3,000.00 (três mil dólares), por meio de **empresas especializadas** contratadas por instituições autorizadas a operar no mercado de câmbio.

As empresas especializadas mais populares são a **Western Union** (https://www.westernunion.com.br) e a **Money Gram** (http://global.moneygram.com/br/ptb); que estão presentes em mais de 200 (duzentos) países, inclusive no Brasil, e várias casas de câmbio têm convênio com elas. A principal vantagem desse tipo de serviço é o fato de não precisar abrir conta em banco. Pelos simuladores disponíveis nos sites, é possível saber qual a taxa cobrada de acordo com o valor que deseja enviar e o país escolhido.

Através da ***Western Union*** (https://www.westernunion.com.br) é possível enviar e receber dinheiro do exterior. Ela funciona como uma corretora de câmbio pela qual é possível realizar operações internacionais

do Brasil ou no exterior. O valor da transação e das taxas variam de acordo com o país de envio e de recebimento. Mas, as taxas são normalmente mais baixas do que às aplicadas aos cartões brasileiros de crédito, débito e pré-pago. É possível que o remetente receba o dinheiro na mesma hora, retirando numa agência da *Western Union*, Banco Bradesco, Banco do Brasil ou em algumas lojas, como a Riachuelo.

- https://www.westernunion.com.br;
- http://www.corretorawesternunion.com.br/;
- http://www.bancowesternunion.com.br/.

Do Brasil, é necessário procurar uma agência da *Western Union* munido de documento de identificação com foto (CNH ou RG juntamente com o CPF), informar o país do destinatário (e, em alguns casos, também é necessário informar o estado) e nome completo do remetente. O mesmo vale para quem quer enviar e está fora do Brasil. No caso, se estiver em viagem, o documento de identificação pode ser o passaporte. Em qualquer operação se pode escolher em qual moeda o remetente irá receber o valor, se na moeda local ou em euros, dólares, etc. Quem vai receber dinheiro via Western Union vai precisar do nome completo, endereço, telefone do remetente e o código da operação (*Money Transfer Control Number*), que é informado para quem envia o dinheiro no momento em que a operação é realizada (fica impresso no comprovante da transferência). No Brasil, além do Banco do Brasil e Banco Bradesco, algumas lojas servem de agência da Western Union para envio e recebimento, como as lojas Riachuelo.

A **Ourominas** (http://www.ouroemoeda.com/ ou http://ourominas.com/), empresa que atua no segmento de compra e venda de moedas estrangeiras e ouro, oferece um produto ágil e prático para a transferência de dinheiro entre países. Sem utilizar cartão de crédito ou conta bancária, usando apenas um documento de identificação com foto e comprovante de residência, amigos e familiares podem transferir a quantia em espécie para mais de 200 países, sem que incida sobre a operação o imposto de 25% (vinte e cinco por cento) para remessas ao exterior. A facilidade é fornecida pela **MoneyGram** (http://global.moneygram.com/br/ptb), uma das maiores empresas de transferência de dinheiro do mundo, da qual a Ourominas é representante no Brasil.

O **Transferwise** (https://transferwise.com/br/) permite fazer operações financeiras, através de sua plataforma, para diversos países do mundo, em mais de 20 (vinte) moedas, com uma comissão de apenas 0,5% (meio por cento). O Transferwise promete enviar dinheiro para o exterior sem pagar impostos. A TransferWise possui conta corrente em vários países onde atua. O que a empresa faz é pegar o seu dinheiro no país de origem como se fosse uma recarga no aplicativo e, posteriormente, ela devolve o seu dinheiro na conta bancária do país de destino através de um depósito nacional. Com isso a pessoa faz uma transferência internacional como se tivesse efetuando um depósito em uma conta no mesmo país. Além de não pagar IOF (Imposto sobre Operações Financeiras) a cotação da moeda é mais próxima da comercial (que é mais barata que a cotação de turismo, por exemplo) e, no geral, o custo para envio pode ser até 8x mais barata.

O ***Small World Financial Services*** (https://www.smallworldfs.com/small-world/bra/pt-pt) permite o envio de dinheiro para mais de 190 países.

O site https://remittanceprices.worldbank.org/pt lista as opções existentes para a remessa de dinheiro entre vários países.

O **Paypal** é o serviço de pagamento online mais usado no mundo. Com ele pode-se fazer compras em qualquer parte do mundo ou até realizar transferência para pessoas físicas tudo isso de forma rápida, fácil, segura e totalmente online.

- https://www.paypal.com/br/webapps/mpp/home.

PayPal e Coinbase fecharam um acordo que permite vender bitcoin e receber dólar diretamente na conta PayPal.

- https://blog.coinbase.com/2016/06/22/coinbase-adds-support-for-paypal-and-credit-cards/;
- https://www.braintreepayments.com/payment-methods/accept-bitcoin.

Outras opções:

- https://transferwise.com/br/;
- http://global.moneygram.com/;
- https://www.remessaonline.com.br/;
- https://www.confidencecambio.com.br/;
- https://www.paypal.com/br/webapps/mpp/home;
- https://www.payza.com/;
- https://www.solidtrustpay.com/;
- http://www.ego-pay.com/;
- https://www.skrill.com/en/;
- https://www.neteller.com/pt;
- https://www.mayzus.com/pt/;
- https://ripple.com/.
- http://www.wmtransfer.com.br/;
- https://c-gold.com/;
- https://www.visa.co.uk/products/v-pay-by-visa/;
- http://transvaloresbrasil.blogspot.com.br/ ou http://portaltransvalores.blogspot.com.br/;
- http://okpay.com.br/;
- https://www.paxum.com/payment/index.php.

As transferências internacionais de recursos, também, podem ser realizadas por intermédio dos **Correios** (ECT - Empresa Brasileira de Correios e Telégrafos). Além disso, recursos do exterior também podem ser recebidos por meio de cartões internacionais.

Os Correios estão autorizados a prestar serviço de transferências financeiras internacionais. O envio e o recebimento de valores são feitos eletronicamente entre o Brasil e os países conveniados. No exterior, o remetente (depositante) deve comparecer à empresa de correios do local onde se encontra para fornecer as informações necessárias. O vale postal dos Correios, isento de IOF, permite enviar até R$ 10.000,00 (dez mil reais) por CPF por dia para 33 países. A opção, porém, exige sacar o dinheiro de uma vez e só nos Correios.

A alternativa do **vale postal dos Correios é isenta de IOF**. A opção, porém, exige sacar o dinheiro de uma vez e só nos Correios, que não têm convênio com países muito procurados por brasileiros, como os EUA (Estados Unidos). O limite para envio de remessas nacionais é de R$ 1.000,00 (mil reais) e a tarifa cobrada varia conforme o valor a ser enviado, até o máximo de R$ 22,75. Já na modalidade internacional, o limite para envio é de até US$ 3,000.00 (três mil dólares) por remessa ou R$ 10.000,00 (dez mil reais) por dia para um mesmo cliente (seja por uma remessa única

ou pelo somatório de várias remessas). Esse limite também pode variar de acordo com o país de destino, sendo estabelecido entre os Correios e seus parceiros. A taxa cobrada é de R$ 35,00 (trinta e cinco reais), mais 1,5% (um e meio por cento) sobre o valor a ser enviado. O saque poderá ser efetuado nas instituições postais conveniadas, que estão presentes em 33 países.

- https://www.correios.com.br/para-voce/correios-de-a-a-z/vale-postal-eletronico-internacional;
- http://www.correios.com.br/para-voce/correios-de-a-a-z/pdf/vale-postal-eletronico-internacional/PasesConveniados.pdf;
- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/manuais/despacho-de-**importacao**/topicos-1/remessa-postal-internacional-rpi-e-remessa-expressa-re/remessa-postal-internacional-rpi/com-pagamento-do-imposto.

Outra possibilidade é comprar a moeda desejada ainda no Brasil e **levar para o destino em espécie**. Transportar dinheiro vivo (consigo ou através de outra pessoa) pode não ser a forma mais segura, mas certamente será mais barata que utilizar o cartão no exterior.

Encontre a casa de câmbio com a melhor cotação no Brasil em https://www.melhorcambio.com/.

Em regra, o dólar é corrente, fácil de trocar e valorizado em qualquer lugar do mundo; mas há exceções. Para os Estados Unidos, a Zona do Euro, a Inglaterra e demais países há uma regra geral, comprar a moeda de destino (dólar, euro ou libra) aqui no Brasil antes da viagem. Dependendo da cotação (até 10% mais cara que a cotação comercial), também podem ser compradas no Brasil o dólar canadense (Canadá), o dólar australiano (Austrália) e o franco-suíço (Suíça); senão deve-se comprar dólares norte-americanos no Brasil para serem trocados pela moeda local no seu destino. A cotação pode ser conferida em vários sites, como, por exemplo, em http://economia.uol.com.br/cotacoes/cambio/. Entretanto, em países (exemplos, Argentina, Chile, Bolívia, México, Colômbia, África do Sul, etc.) cuja moeda não é o dólar, o euro ou a libra, pelo fato dessas moedas de destino terem pouca circulação no Brasil, em regra, deve-se fazer a

conversão de dólares pela moeda de destino no próprio local (não no Brasil). Se a viagem for para um país cuja moeda não seja a que o viajante comprou no Brasil, ele terá que fazer dois câmbios e perderá em torno de 10% (dez por cento). O primeiro câmbio é na compra da moeda no Brasil e o outro no do país de destino para trocar pela moeda local. O real é uma moeda fraca e de pouca circulação no exterior, com o que ao levá-lo em viagens internacionais perde-se até 40% (quarenta por cento) do seu valor de compra; exceto em países vizinhos do Brasil onde quase não há circulação de dólar, euro, libra, dólar canadense, dólar australiano e franco-suíço e, ainda em cidades com grande circulação de turistas brasileiros, o real é até mais valorizado do que o dólar ante aos constantes negócios com brasileiros (exemplo, brasileiros que fazem compras no Paraguai e na Bolívia). Outro detalhe, do mesmo modo que o dólar está em baixa no Brasil, também estará em baixa em qualquer lugar do mundo. Por fim, deve-se evitar as *exchanges* em aeroportos, portos, estações ferroviárias e nas proximidades de atrações turísticas, pois possuem as piores cotações. Aos finais de semana e feriados as cotações tendem a piorar nas casas de câmbio no exterior.

Algumas considerações sobre a compra de moedas:

- **Contrato de câmbio**: é o comprovante da operação de câmbio; ou seja, da compra ou venda de moeda estrangeira. É muito importante solicitar esse documento para a casa de câmbio, pois ele pode ser exigido para comprovar a proveniência lícita do dinheiro ou a origem de eventual falsificação na imigração ou alfândega/aduana. Assim, em caso de cédulas falsas, o contrato de câmbio responsabiliza a casa de câmbio. Mesmo que se tenha comprado menos de R$ 10.000,00 (dez mil reais), é importante colocar o contrato de câmbio junto com os demais documentos de viagem; assim, se alguma autoridade o solicitar, estará prontamente disponível para apresentação.

- **Dólar Comercial**: é a taxa que as grandes empresas utilizam para fazer importação/exportação de mercadorias.

- **Dólar Turismo**: é aquele que as pessoas compram para viajarem. A cotação do dólar turismo é sempre mais alta que a do comercial. Compra de passagens aéreas em companhias estrangeiras, gastos realizados no exterior por meio de cartão de crédito/débito, recarga em cartão pré-pago e aquisição de moeda em espécie seguem a taxa do dólar turismo. Lembrando que as operações de compra/venda de dinheiro em espécie possuem IOF de 0,38% e, no cartão pré-pago (que pode ser feito em bancos ou algumas casas de câmbio), incide um imposto de 6,38%, o mesmo valor que recai sobre o cartão de crédito.

A compra de qualquer moeda estrangeira em dinheiro vivo ou no cartão pré-pago está livre do Imposto de Renda nas casas de câmbio. Mas o consumidor continua pagando o IOF de 0,38% ao trocar reais por outra moeda, desde que seja em espécie. Para cartão pré-pago, o IOF é de 6,38%, como no cartão de crédito.

Para saber o valor total de uma compra ou venda de moeda estrangeira, deve-se levar em consideração não somente a taxa de câmbio, mas também o imposto incidente e eventual cobrança de comissões. Isso porque nem sempre o local que oferece a melhor taxa de câmbio é o que tem o melhor preço final, após considerados imposto e comissões.

- http://www.bcb.gov.br/?TAXCAMFAQ.

Quando compra moeda estrangeira, paga-se a **taxa de câmbio e o IOF**. Buscando facilitar esse cálculo e proporcionar melhor comparação, foi criado o Valor Efetivo Total (VET), que traz em seu valor todos os custos já considerados. Assim, ao comprar ou vender moeda estrangeira, não deixe de perguntar também pelo VET. É obrigação da instituição fornecê-lo, inclusive fazendo constar no contrato de câmbio ou no recibo.

O Banco Central disponibiliza em sua página na internet *ranking* para facilitar a comparação e o acompanhamento do VET médio praticado pelas instituições. Mais detalhes sobre o VET em https://www3.bcb.gov.br/rex/vet/index.asp e http://www.bcb.gov.br/?VETFAQ.

Pode-se adquirir moeda estrangeira mediante a entrega de reais em espécie ou em qualquer instrumento de pagamento em uso no mercado financeiro, até o limite de R$ 10.000,00 (dez mil reais). Acima desse valor, somente mediante débito em conta, transferência bancária ou cheque. As pessoas que ingressarem no país com moeda nacional em montante superior a R$ 10.000,00 (dez mil reais), ou ao seu equivalente em outras moedas, devem apresentar à Receita Federal declaração relativa aos valores em espécie, em cheques e em cheques de viagem que estiverem portando. A falta de apresentação da e-DBV (Declaração Eletrônica de Bens do Viajante) pode acarretar a retenção ou, até, o perdimento dos valores que excederem o limite de R$ 10.000,00 (dez mil reais), assim como a aplicação de sanções penais previstas na legislação brasileira.

- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/viagens-internacionais/porte-de-valores;
- https://www.edbv.receita.fazenda.gov.br/edbv-viajante/pages/selecionarAcao/selecionarAcao.jsf.

Portanto, até R$ 10.000,00 (dez mil reais) em espécie ou o equivalente em moeda estrangeira, não será preciso informar as autoridades sobre o montante carregado. Caso pretenda transportar mais do que isso, será preciso fazer a chamada Declaração Eletrônica de Porte de Valores (e-DPV) e dirigir-se à fiscalização aduaneira, no momento de seu ingresso ou saída, para fins de conferência da declaração. É importante frisar que não há qualquer limite para a quantidade de dinheiro levada para outros países. Em países situados fora da União Europeia, América do Sul e Estados Unidos, as casas de câmbio podem não aceitar o Real. Além disso, elas podem não ter disponível no dia o valor correspondente em moeda local. Vale ressaltar que a e-DBV é por família e não por pessoa. Assim, para não precisar preencher a e-DBV, são R$ 10.000,00 (dez mil reais) no máximo que a família toda pode levar.

- https://www.edbv.receita.fazenda.gov.br/edbv-viajante/pages/selecionarAcao/selecionarAcao.jsf.

Em resumo, o viajante que deixar o país, ou nele ingressar, portando valores superiores ao equivalente a R$ 10.000,00 (dez mil reais), deverá

preencher a referida declaração e entregá-la à autoridade aduaneira (Guichê da Secretaria da Receita Federal), sob pena de perda dos valores excedentes em prol do tesouro nacional; além das sanções criminais cabíveis.

- http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d6759.htm;
- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=16026#128529.

Dependendo do valor existente no exterior, será necessário prestar informações periódicas ao Banco Central por meio da Declaração de Bens e Valores. Desse modo, se a pessoa possuir no exterior, seja em dinheiro ou em bens, quantia igual ou superior a US$ 100.000,00 (cem mil dólares) em 31 de dezembro do ano corrente, conforme consta do artigo 2º da Resolução n.º 3.854 do Bacen (http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=Res&ano=2010&numero=003854):

> "Art. 2º A declaração de que trata o art. 1º, inclusive suas retificações, deve ser prestada anualmente, por meio eletrônico, na data-base de 31 de dezembro de cada ano, quando os bens e valores do declarante no exterior totalizarem, nessa data, quantia igual ou superior a US$ 100.000,00 (cem mil dólares dos Estados Unidos da América), ou seu equivalente em outras moedas.".

Ressalte-se que não se considera apenas o saldo da conta corrente em 31 de dezembro, mas, também, eventuais bens móveis e imóveis que eventualmente esta pessoa venha a possuir no exterior, inclusive investimento, conforme reza o artigo 3º da citada Resolução.

> "Art. 3° A declaração de bens e valores de que trata esta Resolução compreenderá informações relacionadas às seguintes modalidades:
> I - depósito;
> II - empréstimo em moeda;
> III - financiamento;
> IV - arrendamento mercantil financeiro;
> V - investimento direto;
> VI - investimento em portfólio;

VII - aplicação em instrumentos financeiros derivativos; e
VIII - outros investimentos, incluindo imóveis e outros bens.”.

No caso de bens (móveis ou imóveis) deve ser considerado o valor de mercado deste bem, e não o valor efetivamente pago, conforme prescreve o artigo 1º do Decreto-Lei nº 1.060/1969 (http://www.planalto.gov.br/ccivil_03/decreto-Lei/1965-1988/Del1060.htm):

> “Art. 1º Sem prejuízo das obrigações previstas na legislação do imposto de renda, as pessoas físicas ou jurídicas ficam obrigadas, na forma, limites e condições estabelecidas pelo Conselho Monetário Nacional, a declarar ao Banco Central do Brasil, os bens e valores que possuírem no exterior, podendo ser exigida a justificação dos recursos empregados na sua aquisição.
> Parágrafo único. A declaração deverá ser atualizada sempre que houver aumento ou diminuição dos bens, dinheiros ou valores, com a justificação do acréscimo ou da redução.”.

Também não se pode deixar de declarar investimentos que tenham sido realizados no exterior.

Segundo a legislação fiscal dos EUA (Estados Unidos), estrangeiros de alguns países podem pleitear a isenção ou redução na tributação sobre ganho de capital por meio do preenchimento do formulário W-8BEN. O deferimento da isenção ou desconto pode ser efetivado aos investidores que residem fora dos EUA, desde que sejam oriundos de países que tenham acordo de imposto de renda com os EUA, caso do Brasil.

- https://www.irs.gov/uac/form-w-8ben-certificate-of-foreign-status-of-beneficial-owner-for-united-states-tax-withholding.

Entretanto, assim como na operação com BDRs (*Brazilian Depositary Receipts*), os ganhos de capital devem ser declarados junto ao Fisco brasileiro, ao que serão tributados normalmente; pois quando se compra ou vende ações nos EUA, o governo americano envia os dados para o Brasil, o que reforça a necessidade de ter atenção com os valores declarados. Após a repatriação do valor, é necessário gerar uma DARF (Documento de

Arrecadação de Receitas Federais), pagando imposto de 15% (quinze por cento) sobre o rendimento da operação. No cálculo do lucro inclui a flutuação do dólar envolvida durante a operação; ou seja, quem comprou ações com dólar baixo e as vendeu com dólar mais alto, deve incluir o ganho com o câmbio na tributação.

A tributação com os rendimentos (lucros e dividendos) também deve seguir os mesmos procedimentos da operação com BDRs. Caso o investidor seja um norte-americano ou um brasileiro com *green card* (cartão verde), a incidência de impostos varia a depender da finalidade, do dinheiro investido e do tempo de aplicação (se o investimento se destinar, por exemplo, à aposentadoria ou ao pagamento das despesas educacionais dos filhos, pode ser concedido algum desconto.

BDRs - *Brazilian Depositary Receipts* são valores mobiliários emitidos no Brasil, que possuem como lastro ativos, geralmente ações, emitidos no exterior. Por outras palavras, são certificados representativos de ações de empresas estrangeiras, negociados no Brasil. Apesar de que a nomenclatura correta no Brasil seja CDVM - Certificado de Depósito de Valores Mobiliários, a maioria das pessoas utiliza a nomenclatura norteamericana. Os BDRs são disciplinados pelas Instruções 332 e 480 da CVM com suas posteriores alterações. Já os ADRs (*American Depositary Receipt*), pelo contrário, são recibos de depósitos americanos; ou seja, representam ações de empresas brasileiras negociadas no exterior.

- http://www.cvm.gov.br/legislacao/inst/inst332.html;
- http://www.cvm.gov.br/legislacao/inst/inst480.html;
- http://www.portaldoinvestidor.gov.br/menu/Menu_Investidor/valores_mobiliarios/recibos_acoes.html.

Saiba mais sobre BDRs no capítulo seguinte: "ABRIR UMA CONTA BANCÁRIA OU EMPRESA NO EXTERIOR (*OFFSHORE*)".

Retornando à tributação, deve-se apurar o ganho de capital (diferença positiva entre preço de compra e o de venda) em cada operação, tributando-se 15% (quinze por cento) sobre esse valor. Há, ainda, a tributação sobre os

rendimentos (lucros e dividendos), observando-se as alíquotas de uma tabela progressiva. O recolhimento dos tributos deverá ser feito via carnê-leão, até o último dia do mês subsequente.

O Banco Central obriga os residentes no Brasil detentores de ativos (participação no capital de empresas, títulos de renda fixa, ações, depósitos, imóveis, dentre outros) no exterior que totalizem montante igual ou superior ao equivalente a US$ 100.000,00 (cem mil dólares), no último dia de cada ano, a preencherem a Declaração de Capitais Brasileiros no Exterior. Para quem possui montante acima de US$ 100.000.000,00 (cem milhões de dólares) no exterior, a declaração deve ser feita trimestralmente.

Caso o volume de venda de ações não ultrapasse R$ 35.000,00 (trinta e cinco mil reais) no mês, existe a isenção do imposto sobre o ganho de capital; pois é considerado ganho de "pequeno valor". É a mesma regra dos R$ 20.000,00 (vinte mil reais) de isenção para venda de ações no Brasil, só que o limite de isenção para ações no exterior é maior. No momento da venda ou resgate, deve-se calcular a diferença entre compra e venda em dólar americano e converter o valor em real (cotação de compra no site do Banco Central do Brasil no dia do recebimento da venda) para saber o lucro da operação. Ou seja, a incidência de imposto se dará se houver lucro quando calculado usando-se o dólar. Em cima deste lucro, convertido em reais, incidem os 15% (quinze por cento) de impostos a serem pagos com o preenchimento de DARF (Documento de Arrecadação de Receitas Federais).

- Lei 9.250/1995, artigo 22, na redação dada pela Lei n.º 11.196/2005 (http://www.planalto.gov.br/ccivil_03/LEIS/L9250.htm#art22);

- Instrução Normativa da RFB n.º 1585/2015 (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=67494&visao=anotado).

Independentemente da forma utilizada, sempre estão envolvidos o remetente (depositante) do dinheiro e o beneficiário. O remetente é quem faz a remessa do dinheiro. A identificação do remetente deve seguir a legislação do país da remessa. O beneficiário é quem vai receber o dinheiro. Diferentemente das ordens de pagamento do exterior para o Brasil, as ordens de pagamento do Brasil para o exterior devem ser feitas exclusivamente em

moeda estrangeira. A taxa de câmbio deve ser negociada entre o remetente e a instituição no Brasil.

- http://idg.receita.fazenda.gov.br/noticias/ascom/copy3_of_2013/dezembro/dimof-receita-federal-passa-a-exigir-informacoes-sobre-operacoes-cambiais.

O remetente dos recursos do exterior, no momento da remessa, deve fornecer à instituição no exterior (banco ou transferidora de recursos) os dados do beneficiário (nome completo, documento de identidade, endereço residencial, o número do banco, da agência e da conta destinatária dos recursos, se houver).

Se o valor não ultrapassar R$ 10.000,00 (dez mil reais), é possível receber o dinheiro em espécie ou em qualquer instrumento de pagamento em uso no mercado financeiro. A partir desse valor, somente mediante crédito em conta, transferência bancária ou cheque.

Para receber o valor em reais, é sempre necessário o beneficiário apresentar documento de identificação. Em geral, o banco somente solicitará documentação adicional nas seguintes situações: a) operações acima de R$ 10.000,00 (dez mil reais) no caso de ordens de pagamento em reais; ou, b) operações com valor superior ao equivalente a US$ 3,000.00 (três mil dólares) no caso de ordens de pagamento em moeda estrangeira.

Em regra (salvo exceções, imunidades ou taxações zero de forma expressa) incide a cobrança do **IOF** (Imposto sobre Operações de Crédito, Câmbio e Seguro, ou relativas a Títulos e Valores Mobiliários) sobre as movimentações e transferências de dinheiro.

- http://www.receita.fazenda.gov.br/Legislacao/LegisAssunto/Iof.htm;
- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/imposto-sobre-operacoes-de-credito-cambio-e-seguro-ou-relativas-a-titulos-ou-valores-mobiliarios-iof.

O IOF é o Imposto sobre Operações Financeiras de crédito, câmbio e seguro; ou seja, é o valor acrescentado toda vez que se utiliza um cartão

bancário brasileiro, seja de crédito, débito ou pré-pago, para compras e saques no exterior, ou quando realiza a compra de uma moeda estrangeira no Brasil.

Em regra, conforme prescrevem os artigos 1.º e 5.º da Lei nº 8.894/1994 (http://www.planalto.gov.br/ccivil_03/LEIS/L8894.htm), 15 da Lei n.º 9.718/1998 (http://www.planalto.gov.br/ccivil_03/LEIS/L9718.htm) e 6.º, 15, 22 e 29 do Decreto n.º 6.306/2007 (http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2007/Decreto/D6306.htm), **a alíquota máxima do IOF é de 25%** (vinte e cinco por cento). Entretanto, com o Decreto n.º 6.339/2008 (http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6339.htm) ao alterar o inciso II do artigo 22 e, o Decreto nº 8.325/2014, ao acrescentar o artigo 15-B ao Decreto n.º 6.306/2007, **o percentual foi reduzido para 0,38%** (trinta e oito centésimos por cento) e, este último, ainda previu alguns casos de alíquota zero em operações de câmbio. Algumas alíquotas diferenciadas no Decreto n.º 6.306/2007, são: os parágrafos (§) 15 do artigo 7º e 5º do artigo 8º (adicional de 0,38% [trinta e oito centésimos por cento]); os artigos 32 e 32-C (alíquota é de 1% [um por cento]); o artigo 6º (5% [cinco por cento] ao dia); os incisos VII, IX e X do artigo 15-B (6,38% [seis inteiros e trinta e oito centésimos por cento]); o inciso XII do artigo 15-B (6,00% [seis por cento]); o inciso XX do artigo 15-B (1,10% [um inteiro e dez centésimos por cento]); e, os incisos III (2,38% [dois inteiros e trinta e oito centésimos por cento]) e IV (7,38% [sete inteiros e trinta e oito centésimos por cento]) do artigo 22. Outras alíquotas diferenciadas constam dos artigos 30, 31 e 32 (operações com títulos ou valores mobiliários), 32-C (contrato de derivativo financeiro) e 39 (ouro). **Mais informações sobre a legislação tributária estão em** http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/remessas-para-exterior.

No **artigo 15-B, incisos VII e IX, do Decreto n.º 6.306/2007** (http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2007/Decreto/D6306.htm), reza que: "nas operações de câmbio destinadas ao cumprimento de obrigações de administradoras de cartão de crédito ou de débito ou de bancos comerciais ou múltiplos na qualidade de emissores de cartão de crédito decorrentes de **aquisição de bens e serviços**

do exterior efetuada por seus usuários" e "nas operações de câmbio destinadas ao cumprimento de obrigações de administradoras de cartão de uso internacional ou de bancos comerciais ou múltiplos na qualidade de emissores de cartão de crédito ou de débito decorrentes de **saques no exterior** efetuado por seus usuários" (grifos nossos), **a alíquota do IOF é de 6,38%** (seis inteiros e trinta e oito centésimos por cento).

A Instrução Normativa da Receita Federal (IN RFB) nº 1.645/2016 (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=74319#1632332), dispõe sobre a incidência do **Imposto sobre a Renda** Retido na Fonte sobre rendimentos pagos, creditados, empregados, entregues ou remetidos para pessoas jurídicas domiciliadas no exterior nas hipóteses que menciona.

O artigo 60 da Lei n.º 12.249/2010 (http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Lei/L12249.htm), na redação dada pela **Lei n.º 13.315/2016** (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13315.htm) reza que: "**Até 31 de dezembro de 2019, fica reduzida a 6%** (seis por cento) **a alíquota do imposto de renda retido na fonte incidente sobre os valores** pagos, creditados, entregues, empregados ou remetidos para pessoa física ou jurídica residente ou domiciliada no exterior, **destinados à cobertura de gastos pessoais, no exterior, de pessoas físicas residentes no País**, em viagens de turismo, negócios, serviço, treinamento ou missões oficiais, **até o limite global de R$ 20.000,00 (vinte mil reais) ao mês**, nos termos, limites e condições estabelecidos pelo Poder Executivo." (Grifo nosso).

O contribuinte que está planejando se mudar em definitivo tem até o último dia útil de fevereiro do ano seguinte à saída para comunicar a Receita Federal da decisão. O informe é importante, pois é através dele que a Receita verifica quais bens o contribuinte possui dentro e fora do país. Portanto, o contribuinte precisa avisar a Receita Federal da mudança através de uma declaração de saída definitiva do país e do ajuste anual de imposto de renda na condição de **não residente**.

- http://www.receita.fazenda.gov.br/Aplicacoes/ATSDR/IRPFSaida2013/index.asp.

Caso contrário, os rendimentos recebidos tanto no Brasil como no exterior, durante os doze primeiros meses após a saída, poderão ser tributados por ambos os países.

Feita a referida declaração de saída, caso mais tarde volte a residir permanentemente no Brasil, não terá problemas com o Fisco (Receita Federal) para justificar o ganho patrimonial. A rigor, todos os rendimentos do brasileiro, dentro ou fora do país, são, em tese, tributáveis no Brasil. Se o contribuinte sai do país e não informa que perdeu a condição de residente para fins tributáveis, a Receita Federal pode tributar os rendimentos auferidos fora e o país onde mora também poderá tributá-lo.

Ainda mais, a falta da declaração de saída definitiva pode gerar multa ao contribuinte de até 20% (vinte por cento) do imposto devido.

Os brasileiros no exterior, quando se tornam não residentes, passam a ter tratamento diferenciado, similar ao estrangeiro para diversos fins. Não podem mais abrir conta bancária convencional (comum) no Brasil. Passam a precisar de uma CDE (Conta de Domiciliado no Exterior) para manter reais no país e as movimentações acima de R$ 10.000,00 (dez mil reais) precisam ser justificadas. Também não entregam mais a DIRPF (Declaração do Imposto sobre a Renda da Pessoa Física) anual e passam a sofrer tributação diferenciada quanto ao IOF e ao Imposto de Renda.

Os rendimentos recebidos nos primeiros doze meses consecutivos de ausência:

- De fontes situadas no Brasil são tributados como os rendimentos recebidos pelos demais residentes no Brasil;

- De fontes situadas no exterior sujeitam-se à tributação no Brasil nos termos dos artigos 14 a 16 e 19 e 20 da IN SRF nº 208, de 27/09/2002.

Os rendimentos recebidos a partir do décimo terceiro mês consecutivo de ausência sujeitam-se à tributação exclusiva na fonte ou definitiva, nos termos

previstos nos arts. 26, 27, 35 a 45 da IN SRF nº 208, de 27/09/2002.

- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=15079&visao=anotado.

É considerada não residente no Brasil a pessoa física que:

- Não resida no Brasil em caráter permanente;

- Se retire em caráter permanente do território nacional com a apresentação da Declaração de Saída Definitiva do País;

- Na condição de não residente, ingresse no Brasil para prestar serviços como funcionária de órgão de governo estrangeiro situado no País;

- Ingresse no Brasil com visto temporário e permaneça até 183 dias (aproximadamente seis meses), consecutivos ou não, em um período de até 12 meses ou até a obtenção de visto permanente ou vínculo empregatício antes de completar 184 dias em território nacional;

- Se ausente do Brasil em caráter temporário, a partir do dia seguinte àquele em que complete doze meses consecutivos de ausência.

A alienação de bens e direitos situados no Brasil realizada por não residente está sujeita à tributação definitiva sob a forma de ganho de capital, segundo as normas aplicáveis às pessoas físicas residentes no Brasil.

Assim reza a **Lei n.º 9.779/1999** (http://www.planalto.gov.br/ccivil_03/leis/L9779.htm):

"Art. 7º Os rendimentos do trabalho, com ou sem vínculo empregatício, e os da prestação de serviços, pagos, creditados, entregues, empregados ou remetidos a residentes ou domiciliados no exterior, sujeitam-se à incidência do imposto de renda na fonte à alíquota de vinte e cinco por cento.

Art. 8º Ressalvadas as hipóteses a que se referem os incisos V, VIII, IX, X e XI do art. 1º da Lei nº 9.481, de 1997, os rendimentos decorrentes de qualquer operação, em que o beneficiário seja residente ou domiciliado em país que não tribute a renda ou que a tribute à alíquota máxima inferior a vinte por cento, a que se refere o art. 24 da Lei nº 9.430, de 27 de dezembro de 1996, sujeitam-se à incidência do imposto de renda na fonte à alíquota de vinte e cinco por cento.

Art. 9º Os juros e comissões correspondentes à parcela dos créditos de que trata o inciso XI do art. 1º da Lei no 9.481, de 1997, não aplicada no financiamento de exportações, sujeita-se à incidência do imposto de renda na fonte à alíquota de vinte e cinco por cento.".

A **Lei nº 9.430/1996** (http://www.planalto.gov.br/ccivil_03/leis/L9430.htm), por sua vez, prescreve que:

"Art. 24. As disposições relativas a preços, custos e taxas de juros, constantes dos arts. 18 a 22, aplicam-se, também, às operações efetuadas por pessoa física ou jurídica residente ou domiciliada no Brasil, com qualquer pessoa física ou jurídica, ainda que não vinculada, residente ou domiciliada em país que não tribute a renda ou que a tribute a alíquota máxima inferior a vinte por cento.

§ 1º Para efeito do disposto na parte final deste artigo, será considerada a legislação tributária do referido país, aplicável às pessoas físicas ou às pessoas jurídicas, conforme a natureza do ente com o qual houver sido praticada a operação.

§ 2º No caso de pessoa física residente no Brasil:

I - o valor apurado segundo os métodos de que trata o art. 18 será considerado como custo de aquisição para efeito de apuração de ganho de capital na alienação do bem ou direito;

II - o preço relativo ao bem ou direito alienado, para efeito de apuração de ganho de capital, será o apurado de conformidade com o disposto no art. 19;

III - será considerado como rendimento tributável o preço dos serviços prestados apurado de conformidade com o disposto no art. 19;

IV - serão considerados como rendimento tributável os juros determinados de conformidade com o art. 22.

§ 3º Para os fins do disposto neste artigo, considerar-se-á separadamente a tributação do trabalho e do capital, bem como as dependências do país de residência ou domicílio. (Redação dada pela Lei nº 10.451, de 2002).

§ 4º Considera-se também país ou dependência com tributação favorecida aquele cuja legislação não permita o acesso a informações relativas à composição societária de pessoas jurídicas, à sua titularidade ou à identificação do beneficiário efetivo de rendimentos atribuídos a não residentes. (Incluído pela Lei nº 11.727, de 2008)".

"Art. 22. Os juros pagos ou creditados a pessoa vinculada somente serão dedutíveis para fins de determinação do lucro real até o montante que não exceda ao valor calculado com base em taxa determinada conforme este artigo acrescida de margem percentual a título de spread, a ser definida por ato do Ministro de Estado da Fazenda com base na média de mercado, proporcionalizados em função do período a que se referirem os juros. (Redação dada pela Lei nº 12.766, de 2012).

§ 1º No caso de mútuo com pessoa vinculada, a pessoa jurídica mutuante, domiciliada no Brasil, deverá reconhecer, como receita financeira correspondente à operação, no mínimo o valor apurado segundo o disposto neste artigo.

§ 2º Para efeito do limite a que se refere este artigo, os juros serão calculados com base no valor da obrigação ou do direito, expresso na moeda objeto do contrato e convertida em reais pela taxa de câmbio, divulgada pelo Banco Central do Brasil, para a data do termo final do cálculo dos juros.

§ 3º O valor dos encargos que exceder o limite referido no caput e a diferença de receita apurada na forma do parágrafo anterior serão adicionados à base de cálculo do imposto de renda devido pela empresa no Brasil, inclusive ao lucro presumido ou arbitrado.

§ 5º (Revogado). (Redação dada pela Lei nº 12.766, de 2012).

§ 6º A taxa de que trata o caput será a taxa: (Incluído pela Lei nº 12.766, de 2012).

I - de mercado dos títulos soberanos da República Federativa do Brasil emitidos no mercado externo em dólares dos Estados Unidos da

América, na hipótese de operações em dólares dos Estados Unidos da América com taxa prefixada; (Incluído pela Lei nº 12.766, de 2012).

II - de mercado dos títulos soberanos da República Federativa do Brasil emitidos no mercado externo em reais, na hipótese de operações em reais no exterior com taxa prefixada; e (Incluído pela Lei nº 12.766, de 2012).

III - *London Interbank Offered Rate - LIBOR* pelo prazo de 6 (seis) meses, nos demais casos. (Incluído pela Lei nº 12.766, de 2012).

§ 7º O Ministro de Estado da Fazenda poderá fixar a taxa de que trata o caput na hipótese de operações em reais no exterior com taxa flutuante. (Incluído pela Lei nº 12.766, de 2012).

§ 8º Na hipótese do inciso III do § 6º, para as operações efetuadas em outras moedas nas quais não seja divulgada taxa Libor própria, deverá ser utilizado o valor da taxa Libor para depósitos em dólares dos Estados Unidos da América. (Incluído pela Lei nº 12.766, de 2012).

§ 9º A verificação de que trata este artigo deve ser efetuada na data da contratação da operação e será aplicada aos contratos celebrados a partir de 1º de janeiro de 2013. (Incluído pela Lei nº 12.766, de 2012).

§ 10. Para fins do disposto no § 9º, a novação e a repactuação são consideradas novos contratos. (Incluído pela Lei nº 12.766, de 2012).

§ 11. O disposto neste artigo será disciplinado pela Secretaria da Receita Federal do Brasil, inclusive quanto às especificações e condições de utilização das taxas previstas no caput e no § 6º. (Incluído pela Lei nº 12.766, de 2012)"

Já a **Lei nº 9.481/1997** (http://www.planalto.gov.br/ccivil_03/leis/L9779.htm), assim reza:

"Art. 1º A alíquota do imposto de renda na fonte incidente sobre os rendimentos auferidos no País, por residentes ou domiciliados no exterior, fica reduzida para zero, nas seguintes hipóteses: (Redação dada pela Lei nº 9.532, de 10.12.97).

I - receitas de fretes, afretamentos, aluguéis ou arrendamentos de embarcações marítimas ou fluviais ou de aeronaves estrangeiras ou motores de aeronaves estrangeiros, feitos por empresas, desde que tenham sido aprovados pelas autoridades competentes, bem como os pagamentos de aluguel de contêineres, sobrestadia e outros relativos ao

uso de serviços de instalações portuárias; (Redação dada pela Lei nº 13.043, de 2014).

II - comissões pagas por exportadores a seus agentes no exterior;

III - valores pagos, creditados, entregues, empregados ou remetidos para o exterior: (Redação dada pela Lei nº 11.774, de 2008).

a) em decorrência de despesas com pesquisas de mercado, bem como aluguéis e arrendamentos de stands e locais para exposições, feiras e conclaves semelhantes, inclusive promoção e propaganda no âmbito desses eventos, para produtos e serviços brasileiros e para promoção de destinos turísticos brasileiros; (Incluído pela Lei nº 11.774, de 2008).

b) por órgãos do Poder Executivo Federal, relativos à contratação de serviços destinados à promoção do Brasil no exterior; (Incluído pela Lei nº 11.774, de 2008).

IV - valores correspondentes a operações de cobertura de riscos de variações, no mercado internacional, de taxas de juros, de paridade entre moedas e de preços de mercadorias (*hedge*);

V - valores correspondentes aos pagamentos de contraprestação de arrendamento mercantil de bens de capital, celebrados com entidades mercantil de bens de capital, celebrados com entidades domiciliadas no exterior;

VI - comissões e despesas incorridas nas operações de colocação, no exterior, de ações de companhias abertas, domiciliadas no Brasil, desde que aprovadas pelo Banco Central do Brasil e pela Comissão de Valores Mobiliários;

VII - solicitação, obtenção e manutenção de direitos de propriedade industriais, no exterior;

VIII - juros decorrentes de empréstimos contraídos no exterior, em países que mantenham acordos tributários com o Brasil, por empresas nacionais, particulares ou oficiais, por prazo igual ou superior a quinze anos, à taxa de juros do mercado credor, com instituições financeiras tributadas em nível inferior ao admitido pelo crédito fiscal nos respectivos acordos tributários;

IX - juros, comissões, despesas e descontos decorrentes de colocações no exterior, previamente autorizadas pelo Banco Central do Brasil, de títulos de crédito internacionais, inclusive *comercial papers*, desde que o prazo médio de amortização corresponda, no mínimo, a 96 meses;

X - juros de desconto, no exterior, de cambiais de exportação e as comissões de banqueiros inerentes a essas cambiais;

XI - juros e comissões relativos a créditos obtidos no exterior e destinados ao financiamento de exportações.

XII - valores pagos, creditados, entregues, empregados ou remetidos para o exterior pelo exportador brasileiro, relativos às despesas de armazenagem, movimentação e transporte de carga e emissão de documentos realizadas no exterior. (Incluído pela Lei nº 11.774, de 2008).

§ 1º Nos casos dos incisos II, III, IV, VIII, X, XI e XII do caput deste artigo, deverão ser observadas as condições, as formas e os prazos estabelecidos pelo Poder Executivo. (Renumerado do parágrafo único pela Lei nº 13.043, de 2014).

§ 2º No caso do inciso I do caput deste artigo, quando ocorrer execução simultânea do contrato de afretamento ou aluguel de embarcações marítimas e do contrato de prestação de serviço, relacionados à prospecção e exploração de petróleo ou gás natural, celebrados com pessoas jurídicas vinculadas entre si, do valor total dos contratos a parcela relativa ao afretamento ou aluguel não poderá ser superior a: (Redação dada pela Lei nº 13.043, de 2014).

I - 85% (oitenta e cinco por cento), no caso de embarcações com sistemas flutuantes de produção e/ou armazenamento e descarga (*Floating Production Systems - FPS*); (Incluído pela Lei nº 13.043, de 2014).

II - 80% (oitenta por cento), no caso de embarcações com sistema do tipo sonda para perfuração, completação, manutenção de poços (navios-sonda); e (Incluído pela Lei nº 13.043, de 2014).

III - 65% (sessenta e cinco por cento), nos demais tipos de embarcações. (Incluído pela Lei nº 13.043, de 2014).

§ 3º Para cálculo dos percentuais previstos no § 2º, o contrato celebrado em moeda estrangeira deverá ser convertido para Real à taxa de câmbio da moeda do país de origem, fixada para venda pelo Banco Central do Brasil, correspondente à data da apresentação da proposta pelo fornecedor, que é parte integrante do contrato. (Incluído pela Lei nº 13.043, de 2014).

§ 4º Em caso de repactuação ou reajuste dos valores de quaisquer dos contratos, as novas condições deverão ser consideradas para fins de

verificação do enquadramento do contrato de afretamento nos limites previstos no § 2º. (Incluído pela Lei nº 13.043, de 2014).

§ 5º Para fins de verificação do enquadramento das remessas de afretamento nos limites previstos no § 2º, deverá ser desconsiderado o efeito da variação cambial. (Incluído pela Lei nº 13.043, de 2014).

§ 6º A parcela do contrato de afretamento que exceder os limites estabelecidos no § 2º sujeita-se à incidência do imposto de renda na fonte à alíquota de 15% (quinze por cento) ou de 25% (vinte e cinco por cento), quando a remessa for destinada a país ou dependência com tributação favorecida, ou quando o arrendante ou locador for beneficiário de regime fiscal privilegiado, nos termos dos arts. 24 e 24-A da Lei no 9.430, de 27 de dezembro de 1996. (Incluído pela Lei nº 13.043, de 2014).

§ 7º Para efeitos do disposto no § 2º, será considerada vinculada a pessoa jurídica proprietária da embarcação marítima sediada no exterior e a pessoa jurídica prestadora do serviço quando forem sócias, direta ou indiretamente, em sociedade proprietária dos ativos arrendados ou locados. (Incluído pela Lei nº 13.043, de 2014).

§ 8º O Ministro da Fazenda poderá elevar ou reduzir em até 10 (dez) pontos percentuais os limites de que trata o § 2º. (Incluído pela Lei nº 13.043, de 2014)".

As importâncias pagas, creditadas, entregues, empregadas ou remetidas a não residente a título de *royalties* de qualquer natureza e de remuneração de serviços técnicos e de assistência técnica, administrativa e semelhantes sujeitam-se à incidência do imposto na fonte à alíquota de 15% (quinze por cento).

Os rendimentos recebidos de fontes situadas no Brasil, por não residente, relativos a pagamento, crédito, emprego, entrega ou remessa para o exterior de despesas com instalação e manutenção de escritórios comerciais e de representação, de armazéns, depósitos ou entrepostos sujeitam-se à incidência do imposto na fonte à alíquota de 15% (quinze por cento).

Os rendimentos do trabalho, com ou sem vínculo empregatício, e os da prestação de serviços, pagos, creditados, entregues, empregados ou remetidos a não-residente sujeitam-se à incidência do imposto na fonte à

alíquota de 25% (vinte e cinco por cento), ressalvado o disposto no artigo 37 da IN SRF nº 208, de 27/09/2002.

- IN SRF 208/2002 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=15079&visao=anotado.

Os juros, comissões, despesas e descontos decorrentes de colocações no exterior, previamente autorizadas pelo Banco Central do Brasil, de títulos de crédito internacionais, inclusive *commercial papers*, desde que o prazo médio de amortização corresponda, no mínimo, a 96 (noventa e seis) meses, pagos, creditados, empregados, entregues ou remetidos a não residente sujeitam-se à incidência do imposto na fonte à alíquota de 15% (quinze por cento).

Os rendimentos recebidos de fontes situadas no Brasil, por não residente, relativos a pagamento, crédito, emprego, entrega ou remessa de comissões por exportadores a seus agentes no exterior, de receitas de fretes, afretamentos, aluguéis ou arrendamentos de embarcações marítimas ou fluviais ou de aeronaves estrangeiras, feitos por empresas, desde que tenham sido aprovados pelas autoridades competentes; bem assim de aluguel de *containers*, sobrestadia e outros relativos ao uso de serviços de instalações portuárias, sujeitam-se à incidência do imposto na fonte à alíquota zero. Tais rendimentos, se recebidos por residente em país com tributação favorecida, sujeitam-se à incidência do imposto na fonte à alíquota de 25% (vinte e cinco por cento).

Os rendimentos recebidos de fontes situadas no Brasil, por não residente, relativos a pagamento, crédito, emprego, entrega ou remessa para o exterior de despesas relacionadas com pesquisa de mercado para produtos brasileiros de exportação; bem assim aquelas decorrentes de participação em exposições, feiras e eventos semelhantes, inclusive aluguéis e arrendamentos de estandes e locais de exposição, vinculadas à promoção de produtos brasileiros, e de despesas com propaganda realizadas no âmbito desses eventos, sujeitam-se à incidência do imposto na fonte à alíquota zero. Tais rendimentos, se recebidos por residente em país com tributação favorecida, sujeitam-se à incidência do imposto na fonte à alíquota de 25% (vinte e cinco por cento).

Os demais rendimentos pagos, creditados, empregados, entregues ou remetidos a não residente por fontes situadas no Brasil, inclusive a título de juros sobre o capital próprio; bem assim os decorrentes de cessão de direitos de atleta profissional, solicitação, obtenção e manutenção de direitos de propriedades industriais no exterior, aquisição ou remuneração, a qualquer título, de qualquer forma de direito, e os relativos a comissões e despesas incorridas nas operações de colocação, no exterior, de ações de companhias abertas, domiciliadas no Brasil, desde que aprovadas pelo Banco Central do Brasil e pela Comissão de Valores Mobiliários, sujeitam-se à incidência do imposto na fonte à alíquota de quinze por cento, quando não tiverem tributação específica prevista em lei. Tais rendimentos, se recebidos por residente em país com tributação favorecida, sujeitam-se à incidência do imposto na fonte à alíquota de 25% (vinte e cinco por cento). Os juros e outros encargos pagos ou creditados pela pessoa jurídica a seus sócios ou acionistas, calculados sobre os juros remuneratórios do capital próprio e sobre os lucros e dividendos por ela distribuídos, sujeitam-se à incidência do imposto na fonte à alíquota de vinte por cento. As normas referentes aos rendimentos de aplicações financeiras de renda fixa aplicam-se aos juros e a outros encargos referidos neste item, pagos ou creditados pela pessoa jurídica a seus sócios ou acionistas, e sobre os lucros e dividendos por ela distribuídos, observada a legislação vigente à época da apuração.

O tratamento fiscal é aquele pactuado entre o Brasil e o país em questão, com o fim de evitar a dupla tributação internacional da renda, ou o definido na legislação que permita a reciprocidade de tratamento fiscal sobre os ganhos e os impostos em ambos os países. Assim, o imposto relativo aos rendimentos informados em Rendimentos Tributáveis Recebidos de Pessoas Físicas e do Exterior na Declaração de Ajuste Anual pago no exterior pode ser compensado, desde que não sujeito à restituição ou compensação no país de origem, observados os acordos internacionais entre o Brasil e cada país. A invocação de lei estrangeira concessiva de reciprocidade deve ser comprovada pelo sujeito passivo (contribuinte). A prova de reciprocidade de tratamento é feita com cópia da lei publicada em órgão da imprensa oficial do país de origem do rendimento, traduzida por tradutor juramentado e autenticada pela representação diplomática do Brasil naquele país, ou mediante declaração desse órgão atestando a reciprocidade de tratamento

tributário. Entretanto, não é necessária a prova de reciprocidade para a Alemanha, o Reino Unido e os Estados Unidos da América.

O **artigo 98 do CTN** - Código Tributário Nacional (Lei n.º 5.172/1966 - http://www.planalto.gov.br/ccivil_03/leis/L5172.htm), dispõe que: "os tratados e as convenções internacionais revogam ou modificam a legislação tributária interna, e serão observados pela que lhes sobrevenha."

O Brasil firmou com diversos países **Convenção para evitar a dupla tributação em matéria de Imposto de Renda**; e essas convenções são baseadas no Modelo (*Model Tax Convention on Income and on Capital* - Modelo de Convenção de Dupla Tributação Sobre o Rendimento e o Capital) elaborado pela OCDE - Organização para a Cooperação e Desenvolvimento Econômico (http://www.pcn.fazenda.gov.br/assuntos/ocde/sobre-a-ocde e http://www.oecd.org/).

- https://sites.google.com/site/circoletivas/legislacao-complementar/tributacao-internacional/convencao-modelo-da-ocde.

Assim, por exemplo, no Decreto nº 87.976/1982 (http://www.normasbrasil.com.br/norma/decreto-87976-1982_41351.html), que visa evitar a dupla tributação entre o Brasil e a Argentina, os artigos são os mesmos do Modelo de Convenção de Dupla Tributação Sobre o Rendimento e o Capital.

- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/acordos-internacionais/acordos-para-evitar-a-dupla-tributacao/acordos-para-evitar-a-dupla-tributacao.

O Brasil não é membro da OCDE, porém participa do programa de *enhanced engagement* (engajamento ampliado) que lhe permite participar de Comitês da Organização.

A Instrução Normativa RFB nº 1.226/2011 (http://www.normasbrasil.com.br/norma/instrucao-normativa-1226-2011_78401.html) regulamenta o procedimento de contestação da dupla tributação.

Em ditos tratados constam a seguinte cláusula:

> "ARTIGO VII – Lucros das Empresas
> 1. Os lucros de uma empresa de um Estado contratante só podem ser tributados nesse Estado, a não ser que a empresa exerça sua atividade no outro Estado contratante por meio de um estabelecimento permanente aí situado. Se a empresa exercer sua atividade desse modo, seus lucros poderão ser tributados no outro Estado, mas unicamente na medida em que forem imputáveis a esse estabelecimento permanente.".

Veja, ainda, sobre investidores não residentes.

Sobre o conceito de **"lucros das empresas"**, crucial a leitura dos comentários ao artigo 7°, constante do próprio Modelo de Convenção de Dupla Tributação Sobre o Rendimento e o Capital - 1977: "Conquanto não se tenha julgado necessário definir a expressão "lucros" na Convenção, deve entender-se, porém, que este termo empregado no presente artigo e noutros artigos da Convenção tem um sentido amplo e compreende todos os rendimentos auferidos na exploração de uma empresa. Esta acepção geral corresponde à utilização que a legislação fiscal da maior parte dos países membros da OCDE faz da referida expressão".

Como se observa, "lucros" no contexto do artigo 7º, possui sentido amplo, correspondendo a todos os rendimentos decorrentes da exploração da atividade da pessoa jurídica. Ou seja, qualquer rendimento auferido por uma pessoa jurídica na exploração de seu objeto social enquadra-se, perfeitamente, no conceito de lucros.

A amplitude do conteúdo dessa expressão é muito clara nas versões em inglês e em francês do Modelo da OCDE, que são, respectivamente, "business profit" e "bénéfices des entreprises". Ou seja, o lucro corresponde aos rendimentos auferidos no desenvolvimento do negócio da pessoa jurídica.

Assim, os rendimentos recebidos por uma pessoa jurídica na exploração de seu negócio, podem ser considerados como parte do lucro; ou seja, como

lucro daquela pessoa jurídica.

Ressalte-se, ainda, que a expressão “lucros de empresas” abrange, justamente, os rendimentos auferidos na exploração do objeto social da pessoa jurídica; ou seja, os rendimentos das operações por ela desenvolvidas.

Em se tratando de empresa prestadora de serviços localizada em outro país, os rendimentos auferidos com suas atividades incluem-se no conceito de “lucros de empresas”, pois são efetivamente, resultado da exploração do respectivo objeto social.

Em sendo assim, quando os valores são remetidos a outro país com qual o Brasil tem acordo internacional, destinados ao pagamento de serviços prestados, é perfeitamente aplicável o artigo 7° da Convenção, devendo tais rendimentos serem tributados somente no país de residência do beneficiário.

Neste sentido a lição de Alberto Xavier em artigo intitulado “O Imposto de Renda na Fonte e os Serviços Internacionais – Análise de um Caso de Equivocada Interpretação dos arts. 7º e 21º dos Tratados” (RDDT - Revista Dialética de Direito Tributário, nº 49, 1999, página 10 e seguintes):

> “14. Em nossa opinião, a norma do art. 7° que atribui competência exclusiva ao Estado de domicílio, na hipótese de inexistência de estabelecimento permanente, é o “coração” de um tratado contra a dupla tributação. Sem a proteção que ela assegura à liberdade de circulação internacional de mercadorias e serviços, todas as demais cláusulas perdem grande parte do seu sentido.
>
> 15. Klaus Vogel - sem dúvida a mais alta autoridade científica em matéria de tributação internacional – no seu monumental comentário à Convenção Modelo contra a dupla tributação, observa que o art. 7° abrange a mais importante categoria de rendimentos, o “lucro da empresa”, observando que de longe a maior porção do rendimento derivado da atividade econômica internacional entra nesta categoria. E, contrariando expressamente a opinião segundo o qual o art. 7° não se aplicaria aos serviços afirma, com referência ao caso de “lucros de empresas”:

> “Traditionally, this concept is centred around commerce, including banking and finance, and crafts and trades and industry; more recently, the services sector has joined in”
>
> 16. Aliás o próprio art. 7°, no parágrafo correspondente ao § 7° do Modelo OCDE, revela que se aplica aos preços de venda de bens e serviços, como receitas componentes do lucro contábil, ao dispor que “quando os lucros compreenderem elementos de rendimentos especialmente Tratados noutros artigos da presente convenção, as respectivas disposições não serão afetadas pelas deste artigo”.
>
> 17. Trata-se do princípio de prevalência dos regimes especiais ou do caráter residual da noção de lucro de empresa. Assim, se os elementos do lucro, isoladamente considerados, têm um tratamento especial (como é o caso dos dividendos, dos juros e dos royalties) aplicam-se as disposições específicas que lhes respeitam. Se não têm um tratamento especial, como é o caso da venda de bens e serviços, aplica-se o art. 7°.”.

Em resumo, as remessas de valores em pagamento de serviços prestados sem transferência de tecnologia por empresa sediada em país com o qual o Brasil mantém acordo internacional contra a bitributação enquadram-se no “Artigo VII – Lucros de Empresas da Convenção” e não tendo a empresa estrangeira estabelecimento no Brasil, a tributação pelo imposto sobre a renda ocorre exclusivamente no país de residência da estrangeira, não podendo ser exigida a retenção e o recolhimento do Imposto de Renda Retido na Fonte sobre os valores a este título remetidos.

Nesse sentido a sentença da 15ª Vara Federal do Distrito Federal (JFDF), prolatada em 31/01/2013, no processo nº 35352-82.2013.4.01.3400 (http://processual.trf1.jus.br/consultaProcessual/numeroProcesso.php?secao=DF&enviar=ok, aba “Inteiro Teor”).

A maior parte dos **produtos importados pela Internet** está sujeita a uma taxação de 60% (sessenta por cento). A exceção fica por conta dos produtos isentos de impostos e no caso das transações realizadas entre pessoas físicas, nas quais o item custe, segundo a Receita Federal, menos de US$ 50.00 (cinquenta dólares).

Entretanto, o imposto de importação não pode ser cobrado em remessas internacionais de valor até US$ 100.00 cem dólares norte-americanos, desde que o comprador seja pessoa física. Tal isenção é assegurada pelo artigo 2º, inciso II, do Decreto Lei 1.804/1980. Ocorre que, embora referido dispositivo legal imponha expressamente o limite de cem dólares para isenção, a Receita Federal do Brasil tem adotado o valor de cinquenta dólares como limite e, ainda, impõe como requisito adicional que a remessa seja de pessoa física para pessoa física.

- Decreto Lei 1.804/1980 - http://www.planalto.gov.br/ccivil_03/decreto-lei/1965-1988/Del1804.htm.

Para "fundamentar" esse procedimento, a RFB (Receita Federal do Brasil) utiliza o artigo 1º, § 2º, da Portaria MF 156/1999 e o artigo 2º da Instrução Normativa SRF 096/1999, a primeira do Ministério da Fazenda e a segunda da Secretaria da Receita Federal. Contudo, a Receita Federal não pode reduzir o limite da isenção pela metade, à luz do que prescreve o artigo 150, § 6º, da Constituição Federal; o limite de cem dólares estabelecido no Decreto Lei 1.804/1980 somente poderia ser alterado mediante outra lei que regulasse exclusivamente o assunto, o que não aconteceu. Com efeito, deve valer a regra para importações de até cem dólares, independentemente se a venda foi realizada por pessoa jurídica, bastando para tanto que o comprador seja pessoa física.

- Portaria MF (Ministério da Fazenda) n.º 156/1999 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=23977&visao=anotado.

Ou seja, uma Instrução Normativa e uma Portaria não podem se sobrepor a um Decreto-Lei ante o princípio da hierarquia das normas, devendo ser, portanto, desconsideradas. A isenção de imposto se aplica a compras feitas por pessoas físicas, não importando se o remetente é pessoa física ou jurídica.

O limite para importação por pessoa física por meio postal é de até US$ 3,000.00 (três mil dólares) e vale para qualquer mercadoria, inclusive as declaradas como “gift” (presente). A importação por pessoa física com objetivo de revenda é proibida.

- Saiba como recorrer em https://lhc.net.br/wiki/Taxacao_de_Compras_Internacionais_pela_Receita_Federal.

Quando se compra produtos importados, de países como a China ou dos Estados Unidos, pela internet de lojas estrangeiras, não há cobrança dos 6% (seis por cento) de Imposto de Renda, mas do IOF de 6,38%.

Pelos Correios o objeto só pode ter até 1,05m (um metro e cinco centímetros) de dimensão e a soma das suas dimensões (altura + largura + comprimento) não pode ser maior que 2m (dois metros). Já o peso máximo é de 30 kg (trinta quilos); sendo que vai variar o limite de acordo com a modalidade postal contratada pelo remetente.

Detalhe, a legislação brasileira proíbe a entrada de produtos usados no Brasil (o produto é apreendido e a pessoa é multada). A exceção é feita, por exemplo, para instituições beneficentes do exterior que fazem remessas para instituições do gênero no Brasil.

- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/viagens-internacionais/guia-do-viajante/entrada-no-brasil/cota-de-isencao-duty-free-e-bagagem-tributavel;

- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/viagens-internacionais/guia-do-viajante/perguntas-e-respostas.

O Correios possui uma cartilha sobre importação: http://www.correios.com.br/para-voce/recebimento/pdf/cartilha.

A tributação das importações realizadas por pessoas físicas é chamada de Regime de Tributação Simplificado (RTS). Nesse regime, os bens são tributados por uma alíquota única de 60% (sessenta por cento), contemplando o Imposto de Importação, Imposto sobre Produtos Industrializados, PIS e Cofins. O cálculo é feito sobre a soma do valor do produto e despesas com frete e seguro.

Quando há a utilização dos Correios, para bens até US$ 500.00 (quinhentos dólares), o imposto será pago no momento da retirada da mercadoria, na própria unidade de serviço postal. Já para produtos com valor entre US$ 500,00 (quinhentos dólares) e US$ 3,000.00 (três mil

dólares), o comprador deverá fazer a Declaração Simplificada de Importação (DSI) no site do Correios.

- https://www.correios.com.br/para-voce/correios-de-a-a-z/importa-facil;
- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/manuais/despacho-de-importacao/topicos-1/remessa-postal-internacional-rpi-e-remessa-expressa-re/remessa-postal-internacional-rpi/com-pagamento-do-imposto.

Quando a encomenda vem por serviço comum de correio, o comprador recebe uma Nota de Tributação Simplificada (NTS) e um Documento de Arrecadação das Receitas Federais (DARF) com indicação de valor e da agência onde deve pagar o imposto para retirar o desejado produto. Se a pessoa não concordar com o valor, basta ela se dirigir aos correios e preencher um pedido de revisão de lançamentos. Para isso, é importante que a pessoa tenha consigo a nota de confirmação da compra que deve ser apresentada junto ao formulário.

Siscomex, ou Sistema integrado de comércio exterior, é um sistema utilizado pelo governo do Brasil para o controle do comércio exterior, que por um fluxo único, registra atividades, acompanhamento e controla as referidas operações.

- http://www.portalsiscomex.gov.br/;
- https://www.siscomex.gov.br/vicomex/public/index.jsf;
- http://www1.siscomex.receita.fazenda.gov.br/siscomexImpweb-7/login_cert.jsp;
- http://www.aprendendoaexportar.gov.br/artesanato/CartilhaSimplexVersao2.pdf;
- https://www.banrisul.com.br/bob/data/IMPORTAÇÃOFÁCIL.pdf?cache=0;
- http://www.proimportsmotors.com.br/cartilha-de-importacao-nocoes-basicas-para-importar-mercadorias-do-exterior/.

As importações de bens pelos Correios estão sujeitas ao Regime de Tributação Simplificada – RTS, instituído pelo Decreto-Lei 1.804/1980 (http://www.planalto.gov.br/ccivil_03/decreto-lei/1965-1988/Del1804.htm). Esse regime aplica-se às mercadorias de valor aduaneiro de no máximo US$ 3,000.00 (três mil dólares americanos). A base de cálculo do tributo é o valor aduaneiro, que é composto pelo custo da mercadoria + frete + seguro, se houver.

Nem todas as mercadorias vindas do exterior passam pela fiscalização minuciosa da Receita Federal ao entrar no país.

Os Correios esclareceram que todas encomendas que chegam do exterior passam por raio-x onde é feita a triagem para fiscalização da Receita e outros órgãos competentes, como Anvisa e Exército, para verificação de conteúdo ou aplicação de tributos de importação, de acordo com a legislação de cada país. Ao chegarem ao Brasil por São Paulo, Rio de Janeiro ou pelo Paraná, os pacotes são separados e remetidos para um setor especial, onde ficam aguardando vistoria para detalhar se há tributação.

Já a Receita Federal informa que as mercadorias vindas de outros países, como China e Estados Unidos, poderão ficar até 90 dias retidas para análise e investigação.

A Receita Federal e os Correios estão apertando o cerco e aumentando o número de mercadorias tributadas. O sistema está cada vez mais informatizado para que os pacotes sejam taxados automaticamente. Os Correios e a Receita receberão eletronicamente as informações (dados do remetente, destinatário, conteúdo detalhado, valor dos produtos, etc.) sobre as remessas que estão sendo enviadas ao Brasil. Assim, antes mesmo de o pacote chegar ao Brasil, será possível definir o processo aduaneiro a que será submetido, inclusive quanto à necessidade de fazer a verificação intrusiva do pacote, para checagem de documentos, conteúdos, etc. Mesmo no novo processo, toda carga que chegar do exterior continuará passando pelo raio-x, para controle de segurança.

O site http://www.tributado.net/ fornece uma calculadora *on line* para impostos de importação.

Com a PagBrasil (https://www.pagbrasil.com/pb/br/index.html), os comerciantes internacionais podem vender no Brasil e receber os fundos em dólares americanos ou euros nos seus respectivos países.

A conta do EBANX (https://www.ebanx.com/br) é como uma carteira virtual em dólares (US$) que facilita as compras internacionais.

As seguradoras brasileiras não aceitam segurar mercadorias adquiridas no exterior por pessoas físicas, inclusive aquelas de valores mais expressivos, como máquinas, equipamentos e veículos. O seguro pretendido por pessoa física seria, portanto, adquirido por meio de apólice avulsa, um sistema preterido pela maioria das seguradoras. Na falta de seguro, havendo perdas, danos e extravio de produtos, restará ao comprador buscar o ressarcimento dos prejuízos diretamente da empresa responsável por trazer a mercadoria ao Brasil.

A pessoa física, na figura de importador, ao comprar um produto no exterior, deve solicitar ao vendedor que a exportação seja na condição de venda CIP ou CIF, dependendo do meio de transporte, que já vêm com seguro contratado pelo vendedor no exterior. Nessa modalidade, o ideal é que o seguro seja com cobertura ampla, que inclui a garantia contra todos os riscos, tendo o importador como beneficiário.

Saiba mais sobre **câmbio e moedas estrangeiras** (envios e remessas):

- http://www.bcb.gov.br/pre/portalCidadao/cambio/index.asp?idpai=portalcambio;
- http://www.bcb.gov.br/glossario.asp?Definicao=134&idioma=P&idpai=GLOSSARIO;
- http://www.bcb.gov.br/pre/bc_atende/port/taxCam.asp;
- http://www.bcb.gov.br/pre/bc_atende/port/mercCam.asp;
- http://www.bcb.gov.br/Rex/LegCE/Port/rmcci.asp;
- http://www.bcb.gov.br/rex/rmcci/port/rmcci.asp;
- http://www.bcb.gov.br/pre/portalCidadao/cambio/rde.asp?idpai=PORTALBCB;
- http://www.bcb.gov.br/pre/bc_atende/port/expImp.asp;
- http://www.bcb.gov.br/htms/novapaginaspb/iban.asp;
- http://www.bcb.gov.br/rex/atualizacoes/port/cambio20.asp;
- http://www.bcb.gov.br/pre/composicao/corretora_cambio.asp;
- http://www.bcb.gov.br/pre/composicao/Bancos_Cambio.asp;
- http://www.bcb.gov.br/rex/IAMC/Port/Instituicoes/inst_intermediarias.asp;
- http://www.bcb.gov.br/textonoticia.asp?codigo=3072&idpai=NOTICIAS;
- http://www.bcb.gov.br/rex/atualizacoes/port/cambio13.asp;
- http://www.bcb.gov.br/pre/bc_atende/port/envRecMoeEst.asphttp://www.bcb.gov.br/rex/cartilha/cartilha_cambio_envio_recebimento_pequeno_valores.pdf;
- http://acesso.mte.gov.br/data/files/FF8080812CB90335012CCBDACCA8737F/cartilha_cambio_envio_valores.pdf;
- http://sistemas.mre.gov.br/kitweb/datafiles/Retorno/pt-br/file/CARTILHA4_REMESSAS.pdf.

Consulte, ainda, as **normas da alfândega ou aduana**:

- http://idg.receita.fazenda.gov.br/orientacao/aduaneira;
- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/manuais/transito-aduaneiro/topicos/conceitos-e-definicoes;
- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/viagens-internacionais/guia-do-viajante/e-dbv/edbv;
- http://idg.receita.fazenda.gov.br/orientacao/aduaneira/manuais/rtu-regime-de-tributacao-unificada/topicos/documentos-e-formularios/documentos-e-formularios.

ABRIR CONTA BANCÁRIA OU EMPRESA NO EXTERIOR (*OFFSHORE*)

Existem vários motivos para uma pessoa, física ou jurídica, abrir uma conta bancária no exterior. Há vários exemplos históricos da necessidade disso, podendo ser mencionados como exemplos: fugir de perseguições de estados totalitários (nazismo, comunismo, sharia, etc.); fugir de perseguições religiosas (inquisições, sharia, ateísmo, etc.); escapar de confiscos como dos nazistas que bloquearam e apreenderam o dinheiro e bens dos judeus ou como do Plano Collor que bloqueou e confiscou o saldo das cadernetas de poupanças no Brasil; escapar da alta tributação e das tarifas caras dos bancos nacionais; poder sair do país com seu patrimônio para fugir de uma rebelião, guerra civil ou golpe de Estado; simplesmente administrar patrimônio e/ou renda no exterior; possibilidade de diversificação de investimentos em diferentes mercados e moedas; diversificar o risco dos seus investimentos; conseguir crédito (empréstimos e financiamentos), mais fáceis, rápidos, baratos e em maior valor como muitas vezes o governo e empresários brasileiros já fizeram com bancos ingleses; estabelecer um servidor web (hospedagem de site e/ou arquivos); etc.

> "Chamam-se popularmente de *offshores* as contas bancárias e empresas abertas em paraísos fiscais, geralmente com o intuito de pagar-se menos impostos do que no país de origem dos seus proprietários. Como a grande maioria dos países que permitem a criação desse tipo de empresa anônima — ou a abertura desse tipo de contas bancárias anônimas — fica em ilhas, (tais como as Bermudas, Jersey, Ilhas Cayman, etc.), por extensão de sentido, esse tipo de empresa anônima ou de conta bancária anônima passou a ser chamado de *offshore*, embora alguns países continentais, como o Grão-Ducado do Luxemburgo [1] ou o Principado de Mônaco também as permitam, usando esquemas legais diferentes, porém de resultados equivalentes. O termo vem dos tempos dos corsários que saqueavam os mares e depositavam a pilhagem *off-shore* (fora da costa).
>
> Empresas *offshore* (*offshore company*) são entidades situadas fora do país de domicílio de seus proprietários e, portanto, não sujeitas ao regime legal vigente naquele país.

O mesmo ocorre com as contas bancárias *offshore*, que são geralmente abertas em países de legislação de origem britânica, usando-se um conceito jurídico de *trust*. *Trust law*, originário da *common law* inglesa e que foi trazido para a Inglaterra pelos cruzados. O conceito de *trust* refere-se a uma relação em que a propriedade (real ou pessoal, tangível ou intangível) é mantida por uma parte, em benefício de outra. Deriva do conceito islâmico de "waqf" e se refere a um contrato (*trust instrument ou deed of trust*), através do qual uma pessoa física ou jurídica detém a titularidade de um bem (intangível ou tangível), em benefício de outrem. Assim, nos países que adotam a *common law*, os *trustees* (isto é, aqueles que detêm o título de propriedade) são obrigados a manter e administrar a propriedade em benefício de outrem - que é o proprietário de facto. Tal expediente pode ser usado, portanto, quando se pretende proteger ou ocultar a identidade do verdadeiro dono do negócio. Nos países que adotam o Direito Romano, tal artifício é substituído pela criação de fundações, que, formalmente, são proprietárias de bens.

Nos países ditos (paraísos fiscais) ou que permitem a operação desse tipo de *trusts* ou fundações, os bancos têm conhecimento apenas do nome dos trustees (ou seja, dos administradores ou procuradores) das contas ou dos gestores da fundação, ignorando completamente quem seja o real beneficiário do dinheiro depositado. Assim, mesmo que haja determinação judicial, é impossível que esses bancos forneçam informações sobre quem são os proprietários do dinheiro depositado nessas contas." (https://pt.wikipedia.org/wiki/Offshore_(paraíso_fiscal)).

"Evitar o pagamento de impostos não é o mesmo que evasão fiscal. Alguns investidores abrem contas e empresas *offshores* para pagar menos impostos sobre rendimentos financeiros e também para operações de aquisição e fusão de negócios. No entanto, muitos paraísos fiscais trabalham com empresas de fachada e sob o sistema de "trust", que facilitam a dissimulação da real titularidade de contas e empresas *offshore*, favorecendo operações ilegais, como a lavagem de dinheiro. O "trust" é uma entidade criada para administrar operações financeiras e bens em benefício de outrem. Com isso, a identidade do real proprietário de contas e empresas fica resguardada, já que em todos os papéis de movimentação financeira, é o nome do "trust", não do

proprietário, que aparece." (http://www1.folha.uol.com.br/mundo/2016/04/1757632-entenda-o-que-sao-e-como-funcionam-empresas-e-contas-offshore.shtml).

"Quanto maior a carga fiscal existente em certos países, maior é o interesse de empresas e pessoas físicas em fazer investimentos no exterior, atraídos por inúmeros fatores, tais como: moedas fortes, estabilidade econômica e política, isenções fiscais ou impostos reduzidos sobre os rendimentos, segurança, sigilo e privacidade nos negócios, liberdade de câmbio, economia de custos administrativos e eventual acesso a determinados tipos de financiamento internacional, a juros baixos.

Essas zonas privilegiadas existem em várias partes do globo e alguns entusiastas chegam a falar delas como "tax havens" ou "paraísos fiscais". E, para as sociedades comerciais constituídas nessas "zonas livres" convencionou-se dar o nome inglês de "offshore companies". *Offshore* se aplica à sociedade que está fora das fronteiras de um país.

Assim, uma "offshore company" é uma entidade situada no exterior, sujeita a um regime legal diferente, "extraterritorial" em relação ao país de domicílio de seus associados. Mas a expressão é aplicada mais especificamente a sociedades constituídas em "paraísos fiscais", onde gozam de privilégios tributários (impostos reduzidos ou até mesmo isenção de impostos). E isso só se tornou possível quando alguns países adotaram a política da isenção fiscal, para atrair investimentos e capitais estrangeiros. Na América Latina, o Uruguai é um exemplo típico dessa política.

No Uruguai são conhecidas as "SAFI", prontas para serem compradas e mesmo nos Estados Unidos já se considera que as "LLC" constituídas no Estado de Delaware podem operar como "offshore companies", com benefícios fiscais, desde que só façam negócios no exterior.

Pessoas físicas de alta renda formam freqüentemente empresas *holdings* pessoais ou familiares, visando administrar investimentos feitos. Essas *holdings* pessoais proporcionam sigilo, privacidade e segurança, que não desfrutariam no pais de origem e muitas vezes ainda permitem economizar imposto de renda, dependendo do lugar onde são pagos os rendimentos. Nos pagamentos de dividendos, a redução do

nível de impostos retidos na fonte pode ser obtida pela utilização de uma companhia constituída em jurisdição de imposto nulo.

As *holdings offshore* ainda são muito usadas para adquirir e vender patrimônio pessoal, fazer aplicações financeiras e outros negócios particulares, além de permitir a transmissão de heranças sem os custos, discussões e demoras inerentes a um inventário." (http://www.portaltributario.com.br/offshore.htm).

Veja, ainda, infra maiores explicações sobre o que é *offshore*.

Cada país tem o direito de estruturar sua economia para atrair o capital estrangeiro e o investidor pode procurar, pelas vias legais, diminuir o pagamento de tributos. Diminuir o peso dos encargos tributários em seu patrimônio é uma prática conhecida como elisão fiscal; o que é diferente de evasão fiscal, em que a pessoa procura lavar dinheiro e ocultar um patrimônio criado por meio de crimes (corrupção, tráfico de drogas, entre tantos outros). A abertura de uma conta bancária *offshore* não é reservada apenas para os muito ricos que desejam esconder dinheiro de suas operações ilegais, ou que simplesmente tentam pagar menos, ou nenhum, imposto. Elas também são usadas por pessoas que se recusam a deixar todos os seus "ovos em uma só cesta" ou que vivem nos lugares onde jurisdições políticas e legais são instáveis. A ilegalidade da *offshore* começa quando não se declara à Receita Federal a abertura e respectivos valores, a conta e/ou empresa é em nome de terceiros e não se paga os tributos devidos.

- Bê-á-bá do sonegador: http://revistaepoca.globo.com/Revista/Epoca/0,,EDR72181-6009,00.html;
- http://biblioteca.fbtedu.com.br/fiscais-holdings-empresasoffshore;
- http://materiais.portaldeauditoria.com.br/download-holding-familiar;
- http://investidordesucesso.com.br/lp-ebook-como-investir-exterior.html.

Paraíso fiscal consiste numa determinada região (país ou território) com condições fiscais atrativas para investidores estrangeiros, principalmente por ter baixos impostos e total sigilo bancário.

Alguns dos países que tradicionalmente permitem ou permitiam a criação de empresa ou conta bancária anônima são: Andorra, Anguilla, Bahamas, Bélgica, Belize, Bermudas, Cingapura, Delaware nos Estados Unidos, Domínica, Florida, Hong Kong, Ilhas Cayman, Ilhas Marshall, Ilhas Turcas e Caicos, Ilhas Virgens Britânicas, Irlanda, Jersey, Liechtenstein, Luxemburgo, Madeira, Maurícia, Mônaco, Nova Zelândia, Reino Unido, São Vicente e Granadinas, Singapura, Seychelles, Suíça, Panamá, etc.

- http://www.paraisos-fiscales.info/blog/86_lista-paraisos-fiscales;
- http://www.compte-offshore.info/compte-offshore-par-pays/.

Existem várias empresas especializadas na abertura de *offshores*:

- http://pt.sfm-offshore.com/;
- https://www.icd-fiduciaries.com/en/offshore-bank-account/.

Os paraísos fiscais possuem vantagens tributárias diversas, que variam de paraíso fiscal para paraíso fiscal, cujo maior interesse é a isenção da tributação sobre a renda e sobre transferência de herança. Infra as **principais características de um paraíso fiscal**:

- Nível baixo de tributação dos ativos estrangeiros (o Brasil classifica como paraíso fiscal um país ou região com tributação inferior a 20%);

- Regras bastante rígidas de sigilo bancário, dificultando a identificação dos titulares das contas, atraindo assim pessoas ou organizações que não queiram ter seu nome vinculado a certos ativos;

- Segurança e sigilo na constituição, no quadro societário e nos investimentos da empresa que, justamente por isso, acabam por atrair grandes quantias de dinheiro ilícito;

- Baixo controle fiscal, ou seja, não requerem dados verdadeiros para a abertura de contas ou não possuem sistemas de armazenamento desses dados;

- Desnecessidade de prestação de contas: a maioria não exige a prestação de contas às autoridades fiscais locais;

- Proteção patrimonial: possibilita a blindagem patrimonial de bens e direitos;

- Simplicidade na sucessão: possibilita que a sucessão seja previamente planejada, de forma simples e segura, sem burocracia, sem complicações, com baixos (ou nenhum) custos e de maneira rápida;

- Estabilidade política e econômica. Isso protege a empresa de grandes oscilações na economia e na política;

- Liberdade de câmbio: possibilidade dos depósitos e investimentos também serem feitos em moedas estrangeiras (e não apenas na moeda vigente no país), principalmente as mais fortes, como o dólar, o euro e a libra;

- Baixas taxas de juros em empréstimos e financiamentos;

Para investir dinheiro no exterior de forma legal, é necessário que seu dono declare o dinheiro no país onde mora. Enviar dinheiro ao exterior sem declarar às autoridades é crime de evasão fiscal. É possível, portanto, dentro da legalidade efetuar remessas de valores para o exterior; desde que feitas de forma legal (não clandestina) e com fundos provenientes de atividade lícita.

A Instrução Normativa n.º 1.037/2010 da Receita Federal (atualizada pela IN 1658/2016) **lista os países tidos como paraísos fiscais pelo governo brasileiro**.

- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=16002;
- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=77307.

A **CVM** - Comissão de Valores Mobiliários (http://www.cvm.gov.br/) permite a emissão e negociação dos chamados **BDRs** (*Brazilian Depositary Receipts*), que são recibos de **ações de empresas estrangeiras**, usados como porta de entrada para um brasileiro operar no mercado internacional, comprando e vendendo ações de gigantes. O BDR é, portanto, um certificado de depósito de valores mobiliários emitido no Brasil, mas que representa valores mobiliários de companhias abertas com sede no exterior. Os BDRs são divididos entre patrocinados e não patrocinados, sendo que a principal diferença é que, enquanto no primeiro caso a negociação desses papéis no Brasil se deu por força do interesse das próprias empresas, no segundo, foram os bancos e corretoras que trouxeram as ações para serem comercializadas. O único entrave é que a CVM restringe a compra direta desses títulos apenas a "investidores institucionais" (corretoras, fundos de investimento, instituições financeiras e outros administradores de carteira) ou a pessoas físicas com aplicações superiores a R$ 1 milhão (chamados também de "investidores superqualificados"). Quem deseja operar diretamente, nesse caso, não deve se esquecer que tais papéis possuem menor liquidez do que uma "Blue Chip" brasileira (ações de gigantes do mercado nacional, como Vale, Gerdau e Banco do Brasil).

- http://www.bmfbovespa.com.br/pt_br/regulacao/regulamentos-e-manuais/.

Quem não se encaixa na qualificação estipulada pela CVM como "investidor superqualificado", pode entrar em contato com agentes financeiros que trabalhem com esses títulos para aplicar em fundos de BDRs (alguns exemplos: Western Asset FIA BDR NIVEL I ou o XP Global Equity Managers FIM IE, que necessitam de um investimento mínimo de R$ 25.000,00). A vantagem é que não será necessário abrir conta no exterior, tampouco enviar remessas de valores para outros países. A desvantagem é a falta de autonomia para montar um mix (mistura) de investimentos e operá-lo de acordo com seu livre interesse. Nesse caso, será necessário abrir uma conta de corretagem em um banco internacional, seguido da remessa de valor. Através dos *brokers* (intermediário entre um comprador e um vendedor cobrando uma comissão pelo serviço prestado) dessas instituições (sistemas que permitem a negociação direta das ações), é possível realizar operações de compra e venda de ações de empresas norte-americanas.

Os **fundos *off-shore*** investem recursos no exterior, sendo sua sede formalmente localizada no exterior, porém o gestor localiza-se no Brasil. Logo, esses fundos são destinados a investidores que possuem seus recursos no estrangeiro e que desejam ter uma boa oportunidade de remuneração do seu dinheiro referenciado no risco Brasil. Através desses fundos, é possível investir em ativos estrangeiros, como ações americanas, títulos do governo americano, ações europeias e até ativos brasileiros negociados no exterior. Essa é a maneira mais fácil de investir em ativos (aplicar recursos) no exterior, com custo baixo, rentabilidade atraente e possibilidade de diversificação; pois com uma carteira grande é possível comprar diversas ações americanas, como da Apple, Coca-Cola, etc. Porém, o risco cambial faz parte desse tipo de aplicação; pois como uma boa parte dos investimentos são feitos em dólares ou em euro, a cotação da moeda pode tirar parte da rentabilidade, ou aumentá-la. Em razão da localização formal no exterior, não estão submetidos às regras da maioria dos fundos nacionais, somente à regra de câmbio do Banco Central (do Brasil). Entretanto, estão sujeitos às leis de seu país sede; por exemplo, em alguns países, os custos e as taxas de administração são maiores se comparados aos demais fundos nacionais, pois a taxa de custódia cobrada por um banco no exterior é maior do que no Brasil. A tributação nos fundos *off-shore* vai depender da sede onde o fundo está localizado e variam muito de país para país. Dependendo do país, poderão existir benefícios fiscais ou até mesmo a isenção de impostos. Em compensação, existem países onde a carta tributária sobre os rendimentos é alta, inclusive mais alta que a brasileira. As desvantagens são que costumam exigir valores altos para o investimento, não são garantidos pelo fundo garantidor de crédito, os custos e as taxas de administração altas podem afetar a rentabilidade do fundo (sendo indispensável a indagação ao gestor de quais são os custos e taxas no exterior), a variação do dólar pode afetar negativamente a rentabilidade do fundo e a liquidez reduzida em alguns ativos.

Existem 3 tipos de fundos *off-shore*:

- ***Off-shore* renda fixa**; ou seja, que investem os recursos em títulos de renda fixa no exterior, como Bonds e títulos do Tesouro americano.

- ***Off-shore* renda variável**. A carteira é composta, em sua grande maioria, por ações na Bolsa de Valores de outros países e outros títulos de renda variável.

- ***Off-shore* mistos**. Investe-se tanto em renda fixa quanto renda variável.

Saiba mais sobre fundos *off-shore* em:

- http://epocanegocios.globo.com/Revista/Epocanegocios/0,,EDR84363-9560,00.html;
- http://www.negociosedinheiro.com/investimentos-offshore;
- http://ynvestimentos.com.br/2014/01/fundos-de-investimentos-conceito/;
- http://ynvestimentos.com.br/2013/11/fundos-de-indices/;
- http://ynvestimentos.com.br/2013/11/fundos-cambiais/;
- http://ynvestimentos.com.br/2013/11/fundos-da-divida-externa/;
- http://ynvestimentos.com.br/2013/11/fundos-multimercado/;
- http://ynvestimentos.com.br/2013/11/fundos-em-direitos-creditorios-fidcs/;
- http://ynvestimentos.com.br/2013/11/fundos-imobiliarios/;
- http://ynvestimentos.com.br/2013/11/fundos-em-cotas-de-fundos-de-investimentos/;
- http://ynvestimentos.com.br/2013/11/clubes-de-investimentos/.

Um aviso, a Receita Federal do Brasil exige a identificação do beneficiário final das empresas nacionais e estrangeiras que vierem de alguma forma operar no Brasil.

- http://politica.estadao.com.br/noticias/geral,offshore-tera-que-identificar-dono-real,10000014322;
- http://www.itamaraty.gov.br/pt-BR/discursos-artigos-e-entrevistas-categoria/outras-autoridades-artigos/13916-cooperacao-tributaria-internacional-o-estado-de-sao-paulo-26-4-2016;

- http://idg.receita.fazenda.gov.br/sobre/consultas-publicas-e-editoriais/editorial/cooperacao-tributaria-internacional.

Abrir uma conta bancária em outro país, basicamente, exige os mesmos requisitos necessários no Brasil: apresentação de identidade (via de regra, o passaporte) e os comprovantes de renda e de residência. Outros documentos adicionais dependem de país para país e de banco para banco. Nos Estados Unidos, o *Social Security Card* é o documento equivalente ao nosso CPF.

- http://www.listadebancos.com/.

É necessário verificar a necessidade de um selo "apostille". Este selo serve como certificação especial e pode ser necessário em razão de tratado internacional (Convenção da Apostila da Haia).

- http://www.cnj.jus.br/poder-judiciario/relacoes-internacionais/convencao-da-apostila-da-haia.

O cliente brasileiro de um banco estrangeiro, é obrigado a informar anualmente o Banco Central do Brasil sobre os ativos mantidos no exterior caso eles ultrapassem US$ 100.000,00 (cem mil dólares).

O primeiro passo para abrir uma conta bancária no exterior (*offshore*), é a pesquisa de informações.

Portanto, é essencial levantar informações para descobrir quais bancos estão alinhados com seu perfil e atendem aos seus anseios e objetivos.

Por óbvio, a decisão terá que levar em consideração eventual necessidade de poder adentrar, e até mesmo residir, em referido país; além de outros detalhes personalíssimos ou pessoais. Desse modo, ao escolher um banco, deve-se atentar aos detalhes, tais como, por exemplos:

- Quais são as exigências (documentos, informações, formalidades, valores, etc.) para a abertura da conta?
- É possível a abertura de conta à distância? Se sim, qual é o procedimento?
- É possível a abertura de conta para estrangeiros não residentes?

- O banco exige a presença física do cliente para algum ato? Em caso afirmativo, para qual ou em quais condições?
- Qual é o valor mínimo do depósito inaugural? Existe obrigatoriedade de outros depósitos posteriormente?
- Quais são as exigências e o procedimento para o encerramento da conta?
- Quais são as exigências para o saque?
- Quais são os serviços, benefícios e vantagens que o banco disponibiliza?
- Quais são os planos de fidelidade existentes?
- Quais são as obrigações e riscos envolvidos?
- Quais são os serviços que a instituição disponibiliza via Internet, e-mail e telefone?
- Quais são as taxas, tarifas e demais custos que o banco cobra?
- Existem opções isentas de qualquer cobrança?
- Quais são as políticas tributária e de sigilo do país?
- Quais são os tributos e respectivos índices incidentes?
- Quais são as regras e exceções sobre sigilo, privacidade e compartilhamento de informações?
- Há atendimento em português?
- Como está a saúde financeira do banco em questão?
- Qual é a sua reputação da instituição financeira?
- O que é que os clientes dizem do banco?
- Qual é o nível de segurança oferecido pelo banco?
- Quais as quantidades de agências e suas respectivas localidades?
- Quais são os custos envolvidos com a manutenção da conta bancária?
- Quais são as moedas nas quais é possível ter conta?
- Há fornecimento de cartões de crédito e débito? Se sim, quais são eles e os respectivos termos?

- Existem produtos de investimento disponíveis? Se sim, quais são eles e os respectivos termos?
- Quais são os mercados, investimentos e aplicações onde é possível investir?
- Existe a presença de gerente, ou equipe, para orientar nos investimentos e aplicações?
- Há uma corretora associada ou é possível operar diretamente nas bolsas de valores?
- Quais são as condições e termos de empréstimos e financiamentos?
- Quais são as aplicações possíveis e seus respectivos rendimentos?
- Compare a qualidade do serviço e do atendimento.

Uma das características mais importantes que variam de país para país é a necessidade, ou não, de comparecer pessoalmente ao banco em questão. Em alguns países como Hong Kong e Cingapura é requerido que o cliente se apresente ao banco munido de documentos para a abertura da conta. Já os centros financeiros caribenhos, as ilhas da comunidade britânica na Europa (*Jersey* e *Isle of Man*), bem como Suíça, Luxemburgo e Liechtenstein, costumam permitir a abertura à distância. Nesse caso, tudo é resolvido por e-mail, Skype e telefone. Os documentos necessários para se abrir a conta basicamente são o passaporte, comprovante de residência e uma referência bancária, quer seja uma carta do banco ou um extrato de meses anteriores. Além disso, é importante explicar os motivos que o levaram a abrir a conta no exterior. Além do aporte (depósito) mínimo inicial, deve-se ficar atento às outras taxas cobradas, como manutenção de conta, que pode ser cobrada mensal, trimestral ou anualmente; bem como taxas para recebimento e envio de transferências. É comum bancos que exijam maior aporte inicial, como os Private Banks, não cobrem ou cobrem baixas taxas de manutenção, já que eles geram receita através da administração de recursos dos clientes. A disponibilidade de cartões de crédito e débito também é interessante para quem deseja fazer uso desse serviço. Há opções desde os chamados Travel Money, passando pelos cartões mais simples (Classic) até os mais exclusivos e caros, geralmente chamados de Platinum, Infinite ou Black. As bandeiras Visa, MasterCard e American Express, como no Brasil, são as mais encontradas. É importante verificar também os tipos de investimento disponíveis no banco. Os mais simples são aqueles semelhantes à caderneta

de poupança no Brasil, sendo chamados de *savings account*. Também existem certificados de depósito e depósitos a termo. As taxas variam de banco a banco e de moeda a moeda.

- http://www.investidorinternacional.com/2015/02/11/como-abrir-uma-conta-bancaria-no-exterior-parte-1/;
- http://seuguiadeinvestimentos.com.br/como-abrir-conta-em-corretora-nos-eua-em-10-passos/;
- http://www.guiadomilhao.com.br/como-abrir-uma-conta-bancaria-nos-eua/.

Os países que possuem sistemas bancários bem estabelecidos (sólidos) e que contam com bancos ao alcance dos clientes estrangeiros não residentes são Suíça, Liechtenstein, Luxemburgo, Andorra, Mônaco, Áustria, Estônia, Letônia, Ilha de Man, Ilha de Jersey, Ilha de Guernsey, Malta, Gibraltar, Cingapura, Hong Kong, Emirados Árabes Unidos, Bahrain, Ilhas Maurício, Ilhas Cook, Ilhas Seychelles, Panamá, Ilhas Cayman, São Vicente e Granadinas, São Cristovão e Nevis, Aruba, Anguilla, Antígua e Barbuda, Belize, Bermuda, Bahamas e Santa Lúcia.

Outros detalhes importantes são se o banco tem presença mundial e se possui ramificações no Brasil (exemplos, Citibank International Personal Bank e Banco J Safra Sarasin).

Ressalta-se que a abertura de conta bancária no exterior (*offshore*), normalmente, só vale a pena se precisar do banco para outros propósitos, se tem valores elevados, possui empresa ou patrimônio, ou tem negócios ou investimentos para administrar; vez que o envio de dinheiro de um país para outro segue a mesma lógica de uma transferência bancária feita por ordem de pagamento, com a única diferença de que no último caso tanto o destinatário, quanto o remetente, têm conta em instituições financeiras. Portanto, além de bancar os custos do processo em si, o cliente vai arcar com o ônus da abertura de conta e com a cobrança de todas as taxas em moeda estrangeira. Em razão disso, para um estudante de intercâmbio, o melhor é utilizar de ordem de pagamento para receber créditos no exterior. A exceção fica por conta de bancos brasileiros que possibilitam a abertura de conta na mesma instituição no exterior.

Quem tem conta no Banco do Brasil, por exemplo, pode solicitar a abertura de uma conta no **Banco do Brasil Americas**, instituição da qual o BB é acionista e trata como fosse sua filial norte-americana. Trata-se do antigo Eurobank, comprado pelo BB em 2012 (http://www.bbamericas.com/br/ e accountopening@BBAmericas.com).

O **Bradesco** também possui a **Conta Internacional** destinada a brasileiros que estão, temporariamente, no exterior e querem investir seu dinheiro com segurança. As remessas podem ser feitas de qualquer país, por meio de bancos que operam com ordens de pagamento em moeda estrangeira ou por convênios firmados pelo Bradesco.

- https://banco.bradesco/html/classic/produtos-servicos/tipos-de-conta/conta-internacional.shtm;
- https://www.conta-corrente.com/conta-internacional/bradesco-conta-internacional/bradesco-lanca-conta-internacional-com-abertura-pela-internet/.

De modo semelhante, o **Santander** (https://www.santander.com.br/br/pessoa-fisica/santander-select/servicos-internacionais/abertura-de-conta-no-exterior).

Já o banco **Bitinvest** (http://www.bit-invest.com/) aceita Payza (https://www.payza.com/), Perfet Money (https://perfectmoney.is/), OK Pay (https://www.okpay.com/pt/), Payeer (https://payeer.com/en/) e bitcoin.

Os bancos russos (http://www.russobras.com.br/econ/bancos.php), que são mais de 800, podem sofrer sanções e retaliações aplicadas pelos governos americanos e da comunidade europeia ao governo russo. Detalhe, a Rússia e o Irã criarão um banco que não operará com dólares e nem euros, mas rublos e riais, suas respectivas moedas nacionais.

- http://www1.folha.uol.com.br/mercado/2014/03/1428752-visa-e-mastercard-deixam-de-atender-clientes-de-bancos-russos-apos-sancoes.shtml;
- https://jornalggn.com.br/noticia/visa-e-mastercard-deixam-de-fornecer-servicos-a-clientes-de-bancos-russos;
- http://exame.abril.com.br/economia/bancos-russos-recorrem-contra-sancoes-da-uniao-europeia/;

- https://noticias.terra.com.br/mundo/europa/eua-sancionam-tres-bancos-russos-devido-a-crise-na-ucrania,a44de72108387410VgnCLD200000b1bf46d0RCRD.html;
- http://www.jornal.ceiri.com.br/uniao-europeia-nao-quer-divulgacao-do-balanco-dos-bancos-russos/;
- http://pt.euronews.com/2015/03/06/estados-unidos-congelam-ativos-de-dois-bancos-russos;
- http://monitordigital.com.br/ue-proube-5-bancos-russos-de-levantar-capital-nos-mercados-do-bloco/;
- http://expresso.sapo.pt/internacional/uniao-europeia-corta-com-cinco-bancos-russos=f884209.

Liechtenstein (pequeno país encravado entre a Suíça e a Áustria) não é mais um paraíso fiscal (saiba mais ao final do capítulo) para poder esconder dinheiro; entretanto, ainda existem muitas razões para abrir uma conta em Liechtenstein. Apesar dos seus bancos estarem querendo dinheiro, por medo de multas pesadas, eles podem exigir provas da propriedade e licitude do dinheiro e do pretenso cliente estar em dia com os pagamentos de seus tributos (impostos). O sigilo bancário foi uma tradição em Liechtenstein (onde a discrição é um valor importante) e se estendia às empresas *offshore*. Assim, atualmente, pode-se manter o anonimato relativo com tributação (imposto) na fonte, como ocorre na Áustria, Bélgica, Suíça e Luxemburgo. Esta taxa de imposto é negociável e permanece entre as mais baixas. Este é um dos regimes fiscais mais favoráveis no mundo. Em razão de tratados de transparência e cooperação, para abrir uma conta pessoal, será muito mais fácil para quem não for um residente europeu ou dos Estados Unidos. Desde 1990, cada cidadão de um país da União Europeia (https://europa.eu/european-union/index_pt) tem a oportunidade de abrir uma conta *offshore*, desde que declare a existência dessa conta bancária estrangeira. A penalidade fixa é € 750 por conta não declarada, mais a tributação dos rendimentos tributáveis que não tenha sido declarado. Alguns bancos *off-shores* exigem conhecer fisicamente o cliente para poder abrir a conta; já outros oferecem um pouco mais de flexibilidade e permitem a abertura remota. No entanto, exigirão documentos como a cópia do passaporte, comprovante de endereço, um currículo para indivíduos ou um plano de negócios para pessoas jurídicas (pessoas coletivas). A lista de documentos não é exaustiva, podendo ser exigidos muitos documentos adicionais e o processo pode durar cerca de 3 meses. O montante mínimo

para abrir é muito diferente de um banco para outro. Geralmente, de 1000 a $ 2000, nos bancos mais acessíveis. *Le prestataire off-shore* (o prestador de *off-shore*) são as empresas que realizam o trabalho de localização de um banco *offshore* e a intermediação na realização da respectiva abertura da conta; por vezes, mais discretamente e principalmente com taxas mais baratas. Mas a recomendação é não usar nenhum OSP (*Service Provider Offshore*), pois não há nada que eles podem fazer que a pessoa não possa fazer por si mesma contatando os bancos através da Internet e/ou por telefone. Além disso, muitos deles ainda estão vendendo Liechtenstein como um paraíso fiscal e ele simplesmente não é mais! Outro detalhe, por causa da má fama (https://www.falter.at/archiv/wp/ein-anstaendiger-mensch-hat-kein-konto-in-liechtenstein), os bancos desconfiam das intenções dos pretensos clientes estrangeiros e, na dúvida, dizem que não estão abrindo mais contas para estrangeiros; mas basta persistir, de forma educada e sem ser irritante, tal como num jogo de sedução, que a conversa pode mudar.

- Centrum Bank (http://www.centrumbank.li/);
- EFG Bank von Ernst (http://www.efgbankvonernst.com/);
- Volksbank (http://www.volksbank.li/);
- Liechtensteinische Landesbank (https://www.llb.li/);
- Bank Vontobel (https://www.vontobel.com/CH/EN/MiFID-Vontobel-Liechtenstein-AG);
- Lamda Privatbank (https://thebanks.eu/banks/9874);
- Bank Frick & Co. (http://www.bankfrick.li/sites/index.html);
- Banque Pasche (http://www.banquehavilland.com/);
- LGT Bank in Liechtenstein (https://www.lgt.li/de/);
- Raiffeisen Privatbank Liechtenstein (https://www.raiffeisen.li/de/);
- Bank Alpinum (https://www.bankalpinum.com/);
- Valartis Bank (http://www.valartisbank.li/);
- Neue Bank (http://www.neuebankag.li/de/);
- https://en.welcome.li/liechtenstein-banks-27.html.

Para se conseguir dinheiro é preciso efetuar algum trabalho ou vender alguma coisa. Já para ganhar muito mais dinheiro necessário se faz ter dinheiro para poder investir ou empreender. É o ditado: É preciso ter dinheiro para ganhar dinheiro! Mas quem não tem dinheiro, pode conseguir através da coragem de arriscar e pelo uso da inteligência no empreendimento. Uma artimanha russa é transferir gratuitamente valores do cartão de crédito para o cartão de débito, que funciona como uma conta poupança com rendimento diário, deixando estes valores rendendo até o limite de 55 dias para pagar o cartão de crédito. Portanto, quando vence o prazo de pagar o cartão de crédito, eles sacam do cartão de débito apenas o necessário para pagar o cartão de crédito, deixando o lucro como saldo no cartão de débito. Igual procedimento poderia ser feito para levantar valores numa instituição financeira no exterior (fora do Brasil) cujo empréstimo ou financiamento possuem excelentes condições, longo prazo e juros reduzidos para investir em alguma aplicação financeira num banco brasileiro e, assim, quando se chega a data de pagamento, retira-se apenas o suficiente para pagar o empréstimo ou financiamento no exterior.

Outra forma de levanta dinheiro é através de *crowdfunding* (financiamento coletivo ou "vaquinha virtual"): https://cryptostocks.com/ e http://crowdfundingnobrasil.com.br/.

Segundo um artigo do site Insider Pro, os **14 países com os bancos mais seguros do mundo** seriam: Finlândia, África do Sul, Canadá, Nova Zelândia, Austrália, Hong Kong, Noruega, Singapura, Chile, Suécia, Panamá, Luxemburgo, Guatemala e República Checa.

- https://pt-br.insider.pro/investment/2016-10-04/os-14-paises-com-os-bancos-mais-seguros-do-mundo/.

Já segundo um artigo da Forbes (http://www.forbes.com.br/), **os 29 bancos mais importantes do mundo** seriam: Bank of America (https://www.bankofamerica.com/), Bank of New York Mellon (https://www.bnymellon.com/), Goldman Sachs (http://www.goldmansachs.com/), JP Morgan Chase (https://www.jpmorganchase.com/), Morgan Stanley (http://www.morganstanley.com/), Citigroup

(http://www.citigroup.com/citi/), State Street Bank (http://www.statestreet.com/), Wells Fargo (https://www.wellsfargo.com/), Lloyds Banking Group (https://www.lloydsbank.com/), Royal Bank of Scotland (http://personal.rbs.co.uk/), Barclays (https://www.barclays.co.uk/), HSBC (https://www.hsbc.co.uk/), Credit Agricole (https://www.credit-agricole.fr/), Societe Generale (http://www.societegenerale.fr/), BNP Paribas (https://mabanque.bnpparibas/), Populaire (http://www.banquepopulaire.fr/), Deutsche Bank (https://www.db.com/), Commerzbank (https://www.commerzbank.de/), UniCredit (https://www.unicredit.it/), UBS (https://www.ubs.com/), Credit Suisse (https://br.credit-suisse.com/) e Dexia (http://www.dexia.com/).

- http://www.forbes.com.br/listas/2016/03/29-bancos-mais-importantes-do-mundo/#foto22.

A Exame (http://exame.abril.com.br/), por sua vez, lista os **43 maiores bancos do mundo**:

- http://exame.abril.com.br/negocios/dos-43-maiores-bancos-do-mundo-3-sao-do-brasil-veja-lista/.

Entretanto, **os bancos europeus estão passando por uma crise**.

- http://www.correiobraziliense.com.br/app/noticia/economia/2016/09/04/internas_economia,547253/cresce-ameaca-de-bancos-europeus-para-estabilidade-do-sistema-financei.shtml;
- http://exame.abril.com.br/economia/situacao-dos-bancos-europeus-e-pior-que-a-da-crise-de-2008/;
- http://brasil.elpais.com/brasil/2016/02/15/opinion/1455560445_839433.html;
- http://economia.uol.com.br/noticias/bloomberg/2016/07/06/italia-pode-gerar-crise-bancaria-na-europa-diz-socgen.htm;
- http://www.jornaldenegocios.pt/opiniao/economistas/detalhe/resolver_a_crise_bancaria_europeia_em_italia;
- http://www.jornaldenegocios.pt/opiniao/economistas/detalhe/resolver_a_crise_bancaria_europeia_em_italia?ref=mercados_UltimasSite;

- https://gz.diarioliberdade.org/mundo/item/87210-capitalistas-internacionais-se-preparam-para-a-crise-bancaria-italiana-e-para-o-referendo-constitucional.html;
- http://economia.estadao.com.br/noticias/geral,a-fragil-europa-dos-bancos,10000079330;
- http://www.verdeasset.com.br/crise-de-bancos-europeus-ainda-nao-atingiu-fundo-do-poco/;
- http://www.infomoney.com.br/welcome?returnurl=http%3A//www.infomoney.com.br/bloomberg/mercados/noticia/5611863/apos-crise-bancarios-europeus-enfrentam-robos;
- http://economia.uol.com.br/noticias/bloomberg/2016/10/04/apos-a-crise-bancarios-europeus-enfrentam-os-robos-gadfly.htm;
- http://www.trade4life.com.br/a-crise-do-bancos-pos-brexit/;
- http://istoe.com.br/cresce-ameaca-de-bancos-europeus-para-estabilidade-do-sistema-financeiro-mundial/;
- http://outraspalavras.net/outrasmidias/destaque-outras-midias/deutsche-bank-estopim-de-mais-uma-crise-financeira/;
- http://www.empreendedoresweb.com.br/crise-economica-de-2016/;
- http://www.jn.pt/economia/interior/deutsche-bank-pode-ser-origem-de-mega-crise-financeira-5439501.html;
- http://boainformacao.com.br/2016/10/fantasma-do-lehman-brothers-volta-a-assombrar-qual-e-o-risco-da-crise-do-deutsche-para-os-mercados/;
- http://jornaldeangola.sapo.ao/opiniao/artigos/duvidas_no_deutsche_bank__afectam_economia_europeia;
- http://www.jb.com.br/economia/noticias/2016/10/14/wsj-deutsche-nao-e-o-unico-banco-alemao-em-apuros/;
- http://www.hardmob.com.br/cotidiano-cultura-politica/642397-deutsche-bank-iminente-colapso-do-sistema-financeiro-europeu.html;
- https://www.bloomberg.com.br/2016/09/30/deutsche-bank-expoe-deficit-europeu-de-capital/;
- http://24.sapo.pt/economia/artigos/problemas-do-deutsche-bank-sao-sinal-de-crise-sistemica-alerta-economista;
- http://controversia.com.br/2044;

- http://br.wsj.com/articles/SB11010900750673983657304582372741121426680.

Confira a lista das **taxas de juros de diversos países**: http://pt.tradingeconomics.com/country-list/interest-rate.

No site http://www.thebankdirectory.com/index.php existe as relações de vários bancos de diversos países, como, por exemplo, do Paraguai (http://www.thebankdirectory.com/pt/bancos-em-paraguai/ e http://www.info-centro-24.com/bancos-paraguay.html).

LIBOR (*London Interbank Offered Rate*) é a taxa de juros praticada no mercado interbancário de Londres (Inglaterra). É a taxa de juros do mercado internacional utilizada na grande maioria das operações de empréstimos e financiamentos efetuados em moedas estrangeiras, praticada não somente pelos bancos ingleses; mas, também, pela quase totalidades dos grandes bancos internacionais, independente de sua nacionalidade. A Libor é calculada diariamente pela BBA – British Bankers Association (https://www.bba.org.uk/), para empréstimos e financiamentos efetuados em diversas moedas e para diversos prazos, com base no valor de 16 (dezesseis) taxas de depósitos, mas destas 16 apenas 8 (oito) são consideradas para o cálculo do valor médio da Libor. Explica-se, são excluídas as 4 (quatro) mais elevadas e as 4 (quatro) mais baixas. Já a PRIME (*Prescibed Right to Income and Maximum Equity*) é a taxa de juros cobrada pelos bancos norteamericanos dos clientes com as melhores avaliações de crédito.

As pessoas físicas e jurídicas residentes, domiciliadas ou com sede no Brasil podem obter empréstimo de pessoas físicas ou jurídicas residentes, domiciliadas ou com sede no exterior. Os empréstimos externos têm registro obrigatório no Banco Central do Brasil determinado pela Lei 4.131, de 1962, e pela Lei 11.371, de 2006, e devem ser destinados a atividade econômica. A regulamentação sobre o registro desses empréstimos pode ser consultada na Resolução 3.844, de 2010 e na Circular 3.689, de 2013, títulos I e II. Detalhe, é possível a transformação de empréstimo em investimento.

- Lei nº 4.131/1962 - http://www.planalto.gov.br/ccivil_03/leis/L4131.htm;

- Lei nº 11.371/2006 - https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11371.htm;

- Resolução 3.844/2010 do Banco Central do Brasil - http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=res&ano=2010&numero=3844;

- Circular 3.689/2013 do Banco Central do Brasil - http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=circ&ano=2013&numero=3689.

Recorda-se que os empréstimos externos estão sujeitos ao Imposto sobre Operações Financeiras (IOF). Entretanto, as operações de câmbio relativas a ingresso de moeda estrangeira para cobertura de gastos efetuados no País com utilização de cartão de crédito emitido no exterior possuem alíquota zero de IOF (Decreto nº 6.306/2007, artigo 15-B, inciso V - http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/D6306.htm).

A maioria dos empréstimos (créditos consignados, empréstimos pessoais, empréstimo feitos entre pessoas físicas ou cheque especial) é declarada no Imposto de Renda na ficha Dívidas e Ônus Reais. Já os financiamentos de imóveis e de veículos, por se tratar de compra com garantia da dívida (alienação fiduciária), eles são informados na ficha de Bens e Direitos. Portanto, os empréstimos que que não utilizam os próprios bens adquiridos como garantia do respectivo pagamento, são declarados na ficha Dívidas e Ônus Reais. Em ambos os casos e, inclusive, saldos negativos em conta corrente, somente são informados (declarados) como dívidas se forem superiores a R$ 5.000,00 (cinco mil reais). Os empréstimos são declarados com códigos diferentes, de acordo com o tipo de credor:

- Código 11 – Estabelecimento bancário comercial: Todos os empréstimos concedidos por bancos;

- Código 12 – Sociedade de crédito, financiamento e investimento: Empréstimos concedidos por cooperativas de crédito;

- Código 13 – Outras pessoas jurídicas: empréstimos concedidos por empresas, que não forem bancos ou sociedades de crédito;

- Código 14 – Pessoas físicas: Entram todos os créditos concedidos por pessoas físicas, sejam amigos, familiares ou conhecidos;

- Código 15 – Empréstimos contraídos no exterior: Empréstimos concedidos por pessoas físicas ou jurídicas situadas no exterior;

- Código 16 – Outras dívidas e ônus reais: Empréstimos concedidos por credores que não se encaixem nas especificações dos outros códigos.

No campo “Discriminação” da Declaração de Imposto de Renda, é necessário informar o valor do empréstimo; o destino dos recursos (reforma da casa, por exemplo); a forma de pagamento, adicionando o número de parcelas e valores; a natureza da dívida (crédito consignado, por exemplo); e os dados do credor, com nome e número do CPF ou CNPJ.

O verbete ***offshore***, na tradução do inglês para o português, significa “afastado da costa”. Em termos financeiros, designada a empresa que tem a contabilidade num país distinto daquele onde exerce a sua atividade. Em oposição, ***inshore*** é a empresa que operam dentro do território nacional. O termo *offshore* é, também, comumente aplicado às contas bancárias e empresas abertas em "paraísos fiscais" (tradução equivocada de “tax havens”, que significa refúgio fiscal), com o intuito de pagar-se menos impostos do que no país de origem dos seus proprietários ou para fins ilícitos e de crimes do colarinho branco, corrupção, crime organizado, terrorismo, tráfico de drogas, etc. Esse referência pejorativa da palavra *offshore* se deve ao fato de que maioria dos países que são "paraísos fiscais" são ilhas.

De modo semelhante à abertura de conta bancária, para se **constituir uma empresa *offshore***, é preciso estabelecer previamente seus objetivos e os requisitos legais exigidos para sua concretização. Depois disso, a escolha do pais onde será constituída a entidade dependerá de disposições legais vigentes no mesmo, devendo se averiguar, entre outros, os seguintes fatores:

- Proteção ao sigilo e privacidade dos negócios;

- Legislação tributária, prevendo incidência nula ou reduzida de impostos sobre rendimentos e sobre operações de compra e venda de mercadorias;

- Liberdade cambial, sem restrições à compra e venda e à transferência de divisas para qualquer outro território;

- Legislação bancária, permitindo depósitos em moedas fortes;

- Legislação sobre sociedades;

- Qual é o valor do capital mínimo autorizado e integralizado?

- Qual é o número de administradores exigidos e se há possibilidade de haver diretores residentes fora do território?

- Quais são os limites de responsabilidades dos sócios ou acionistas?

- Há possibilidade e viabilidade de emissão de ações ao portador, ou seja, transmissíveis por simples entrega, sem exigência de identificação do proprietário, nem de transferência formal por documento escrito?

O site https://pt.portal.santandertrade.com/internacionalize-se fornece algumas informações sobre ambientes jurídicos, sistemas fiscais e práticas empresariais de 171 países.

Uma **LLC** (*Limited Liability Company*) é uma mistura entre uma empresa e uma parceria. Em geral, são formadas por mais de um membro, onde cada um recebe parte da companhia sob a forma de ações. É um tipo de empresa menos burocrática que a IBC (*International Business Company*). Não é necessário ter diretores ou secretários e um dos membros em geral atua como *manager* (gerente) da companhia. Esse é o tipo de companhia usada para adquirir imóveis nos EUA.

Uma das maiores vantagens da formação de uma Sociedade Anônima (**LLC** – *Limited Liability Company*) no Estado de Delaware, nos Estados Unidos da América (EUA), é que nesse Estado americano não existe

nenhuma restrição aos estrangeiros que querem administrar ou serem proprietários de uma LLC. Não é necessária cidadania americana. Inclusive, não é necessário que o proprietário da empresa esteja presente para o registro da empresa, já que o registro é feito por agentes locais com sede dentro do Estado do Delaware. A LLC pode ser utilizada por estrangeiros que nunca sequer "colocaram os pés" nos Estados Unidos. Essa prática tornou-se um veículo empresarial comum para estrangeiros não residentes nos EUA (Estados Unidos da América), pois reúne todos os benefícios de uma empresa americana para negócios internacionais, com o diferencial de poder abrir uma conta bancária no país. Para indivíduos que precisam manter uma aparência corporativa, ter uma empresa registrada nos USA (*United States of America*) cria credibilidade nos negócios internacionais. Algo a confirmar é se exigisse que só se façam negócios fora dos Estados Unidos. E tudo pode ser feito remotamente através de empresas especializadas, tais como, por exemplo, a Sociedade Internacional (http://www.sociedadeinternacional.com/contato/).

- http://www.paraisos-fiscales.info/blog/95_llc-limited-liability-company;
- http://www.paraisos-fiscales.info/blog/96_constitucion-de-una-limited-liability-company-llc;
- http://www.sociedadeinternacional.com/empresa-offshore-precos/#DelawareLLC.

Uma **IBC** (*International Business Company*) é uma verdadeira empresa internacional. Tem diretores, acionistas, capital social e responsabilidade limitada. Se difere das companhias habituais pelo fato dos diretores e acionistas não necessitarem ser de conhecimento público, não haver incidência de impostos e não poderem exercer atividades comerciais dentro do país onde estão registradas sob a pena perderem esses benefícios. A exigência de balanço e registros financeiros mantidos pela empresa também é pequena. Em geral, é recomendado manter um balanço com as movimentações, mesmo que de maneira simples. Em suma, é uma corporação formada sob a legislação societária de um paraíso fiscal (como Bahamas, Panamá, Ilhas Turks e Caicos).

- http://www.paraisos-fiscales.info/blog/93_ibc-international-business-company;

- http://www.paraisos-fiscales.info/blog/94_constitucion-de-una-sociedad-offshore;
- https://www.investbarbados.org/ibc.php;
- https://www.seychellesoffshore.com/seychelles-ibc-company.php.

Uma ***Trust Company*** (empresa de confiança ou empresa de negócios de fideicomisso) é uma estrutura mais complexa, mas também é aquela que confere a maior proteção, segurança, privacidade e é totalmente livre de impostos. Uma empresa de confiança é um negócio ou empresa que tem um agente fiduciário ou uma relação fiduciária com um outro indivíduo ou empresa. A empresa de confiança supervisiona a gestão de quaisquer ativos de um concedente (o criador da empresa de confiança). As empresas de confiança também atuam como agentes fiscais e agentes pagadores para corporações e governos atuando como executora, tutora ou curadora na administração de acordos de custódia, propriedades e de confiança fundos. Essas empresas muitas vezes são usadas quando um concedente sente que a empresa de confiança pode fazer um trabalho igual ou melhor para gerir os ativos do que uma pessoa individual; ou se o concedente não sabe de qualquer outra pessoa que pode atuar como agente fiduciário. Uma empresa de confiança geralmente é iniciada para fornecer bens ou serviços específicos e o concedente seleciona a empresa de confiança com base em como os produtos ou serviços específicos serão relacionados com os ativos envolvidos. Não se confunde com *holding*, cujo único objetivo é o de gerir as operações de outras empresas para ganhar dinheiro e geralmente são iniciadas por empresários que entendem a relação entre estoque, propriedade da empresa, potencial de lucro e direitos de voto. Uma *Trust Company* tem início quando transfere bens pessoais para a empresa e passa a administração deles para uma instituição financeira que será responsável pela *Trust*. Ao fazer isso, se definirá as regras que essa instituição deve cumprir em relação aos bens transferidos e quem serão os beneficiários da *Trust*. Em caso de qualquer tipo de desavença, a instituição pode ser trocada por outra.

As ***shelf companies*** são verdadeiras “empresas de prateleiras”, isto é, são empresas criadas e colocadas em *stand by* (em módulo de espera). Ficam prontas, porém inativas, aguardando investidores interessados em adquiri-las.

O *World Economic Forum* ou Fórum Econômico Mundial (https://www.weforum.org/) realiza periodicamente um estudo denominado Ranking da Competitividade Global (*Global Competitiveness Report* ou *Competitiveness Rankings*), pelo qual informa o ranking dos melhores locais para investimentos.

- http://reports.weforum.org/global-competitiveness-report-2015-2016/competitiveness-rankings/.

No **Paraguai**, como exemplo, os fatores de produção são amplamente vantajosos ao industrial: imposto único apenas na saída do bem exportado; custo de energia elétrica de cerca de 60% (sessenta por cento) menor do que no Brasil; as despesas trabalhistas são, no mínimo, 35% (trinta e cinco por cento) menores do que no Brasil e sem a intromissão de sindicatos; tributação no salário 65% (sessenta e cinco por cento) menor do que a brasileira; a tributação sobre a renda da indústria pode ser desde zero até cerca de 10% (dez por cento) enquanto no Brasil é, em média, 34% (trinta e quatro por cento); inexistência ou quase nenhuma de tributação para os produtos entrarem na comunidade europeia; infraestrutura competitiva e completa à apenas 11 (onze) km do Brasil; e, um ambiente político estável e favorável ao mercado, com uma economia em crescimento de quase 6% (seis por cento) ao ano.

- http://veja.abril.com.br/economia/o-tigre-guarani-a-transformacao-economica-do-paraguai/;
- http://exame.abril.com.br/economia/brasil-teme-ser-desbancado-pela-china-da-america-do-sul/;
- http://g1.globo.com/bom-dia-brasil/noticia/2016/10/paraguai-e-nova-china-para-industria-brasileira-entenda.html;
- http://www.infomoney.com.br/bloomberg/mercados/noticia/5999440/brasil-teme-ser-desbancado-pela-china-america-sul;
- http://estadominimo.com/primo-pobre-o-paraguai-e-nova-estrela-da-america-latina/;
- http://internacional.estadao.com.br/noticias/geral,paraguai-se-abre-para-restaurar-lacos,10000024492;

- http://www.capitanbado.com/paraguay/frontera/paraguai-torna-se-a-melhor-opcao-latino-americana-para-quem-quer-estudar-medicina-no-exterior/40430;
- http://veja.abril.com.br/economia/paraguai-se-repagina-e-vira-chamariz-para-empresas-brasileiras/;
- http://exame.abril.com.br/economia/por-custos-menores-empresas-brasileiras-se-mudam-para-o-paraguai/;
- http://economia.estadao.com.br/noticias/geral,em-busca-de-custos-menores-empresas-brasileiras-abrem-fabricas-no-paraguai,10000097591;
- http://revistapegn.globo.com/Negocios/noticia/2017/01/pegn-em-busca-de-custos-menores-empresas-brasileiras-abrem-fabricas-no-paraguai.html;
- http://revistapegn.globo.com/Negocios/noticia/2017/01/pegn-em-busca-de-custos-menores-empresas-brasileiras-abrem-fabricas-no-paraguai.html;
- http://destinonegocio.com/br/empreendedorismo/como-abrir-um-negocio-no-paraguai-veja-o-passo-a-passo/;
- http://adlerweb.blogspot.com.br/2015/12/como-abrir-empresa-no-paraguai.html;
- http://www.tucanoprod.com/pt-br/paraguai-autorizacao-de-residencia-permanente/;
- http://destinonegocio.com/br/empreendedorismo/como-abrir-um-negocio-no-paraguai-veja-o-passo-a-passo/;
- http://www.ultimahora.com/abrir-un-negocio-paraguay-lleva-unos-74-dias-y-17-tramites-n77650.html;
- http://portalbrasil.net/americas_paraguai.htm;
- http://www.rediex.gov.py/;
- https://www.paraguay.gov.py/;
- http://www.presidencia.gov.py/;
- http://www.mre.gov.py/;
- https://www.bcp.gov.py/;
- http://www.hacienda.gov.py/;
- http://www.mic.gov.py/;
- https://www.documentos.gov.py/;

- http://www.bacn.gov.py/;
- http://www.cnv.gov.py/.

Porém, o Paraguai possui leis contra a lavagem de dinheiro (http://www.bancontinental.com.py/imagenes/Normas_de_Prevencion_de_lavado_de_dinero.pdf).

A lei nas **ilhas Cayman** é baseada na "Common Law" britânica. A principal lei que regula estruturas societárias é a "Company Law of the Cayman Islands", que é baseada no *Companies Act britânico* de 1948 e pode ser encontrado no "Cayman Islands Companies Law" de 1960, com sucessivas modificações. O tipo de empresa normalmente utilizado para finalidades "offshore" é o "Exempt Company", que, para gozar de isenção fiscal, no ato do registro deve declarar que não desenvolverá atividades no território das Ilhas Cayman. É obrigatório que as sociedades tenham um endereço nas Ilhas Cayman. As sociedades devem ter no mínimo um diretor que pode ser de qualquer nacionalidade e não precisa ser residente nas Ilhas Cayman. O nome de endereço dos diretores fica registrado no Registro Público. Para as sociedades "Exempt" não é necessário apresentar balanços ou fazer qualquer declaração ao Fisco. Podem ser emitidas ações ao portador (ou seja, anônimas). As empresas do tipo "Exempt" recebem do Governo um certificado garantido a total isenção de qualquer imposto sobre capital ou atividades pelo prazo e vinte anos, que pode ser estendido a trinta anos. Existe uma taxa anual de licenciamento e registro variável de 500 a 1.750 USD (dólares americanos), dependendo do montante do capital societário. A Associação dos Banqueiros de Cayman requer que os membros investiguem as origens de todos os depósitos maiores de USD 10,000. Os artigos da Lei de Conduta Criminal (revisão 1999) impõem que qualquer pessoa relate as transações suspeitas que possam ser os frutos de condutas criminais (lavagem de dinheiro). Além da confidencialidade bancaria inerente na "common law", e as provisões da Seção 13 da Lei de Bancos e *Trusts* de 1989 (*Banks and Trust Companies Law* 1989) que fornece uma série de proteções, a Lei de Relacionamento Confidencial de 1976 (*Confidential Relationships - Preservation - Law* 1976) faz com que seja um crime para qualquer pessoa divulgar ou obter intencionalmente ou tentar de obter informações fornecidas sob condição expressa ou implícita de sigilo profissional. A lei impõe uma pena máxima de uma multa de CI$

5,000 (*Cayman Islands dollar* ou dólar das Ilhas Cayman) e/ou até 2 anos de prisão. Entretanto, a Lei de Drogas e Narcóticos (Evidência) de 1984 (*Narcotic Drug - Evidence - USA - Law* 1984) e um tratado mútuo de auxílio legal com os Estados Unidos, fornece mecanismos para que informações bancárias sejam fornecidas ao procurador geral dos Estados Unidos em casos de suspeita de lavagem de dinheiro ou de origem ilícita. O Governo das Ilhas Cayman se comprometeu com a OECD (Organização para a Cooperação e Desenvolvimento Econômico) a introduzir uma troca de informações fiscais. Maiores detalhes mais abaixo.

- https://pt.wikipedia.org/wiki/Common_law;
- http://classroom.orange.com/pt/direito-anglo-saxao_1.html;
- https://jus.com.br/artigos/22816/o-sistema-do-common-law;
- https://jus.com.br/artigos/29419/formacao-historica-e-caracteres-essenciais-do-sistema-juridico-anglo-saxonico;
- http://wp.clicrbs.com.br/direitofundamental/2013/05/08/no-berco-do-common-law-como-funciona-sistema-juridico-britanico/?topo=52,1,1,,171,e171.

Nas **Ilhas Virgens Britânicas** (BVI – *British Virgin Islands*) a lei aplicada é a "Common Law" britânica, com modificações e regras locais específicas. Normalmente as estruturas societárias *offshore* utilizam sociedades do tipo "International Business Company" (IBC). As sociedades devem ter um escritório próprio nas BVI ou usar os serviços de uma empresa de administração autorizada. As IBCs devem ter, pelo menos, um diretor que pode ser de qualquer nacionalidade e não precisa residir nas BVI. Não é obrigatório fazer declarações fiscais ou apresentar balanços às autoridades, mas as empresas devem manter livros contábeis que reflitam sua posição financeira. É permitida (e comum) a emissão de ações ao portador. As IBCs não pagam nenhum tipo de imposto sobre seu capital ou sobre seus lucros auferidos no mundo inteiro, mas não podem desenvolver suas atividades nas BVI. As IBCs devem pagar uma taxa anual de licenciamento e registro variável de 300 a 1.000 USD (dolares americanos), dependendo do capital societário. Não existem leis específicas relativas a confidencialidade e sigilo, mas a lei inglesa, que se aplica nas BVI, impõe a obrigação legal dos profissionais de manter confidenciais os negócios dos próprios clientes. Maiores detalhes mais abaixo.

Na América Latina, o **Uruguai** em razão da total liberdade do câmbio, dos sigilos bancário e profissional e das numerosas vantagens fiscais, possuía o apelido de "Suíça da América do Sul". O Uruguai possui várias zonas francas onde é possível criar empresas específicas (SAZF – *Sociedad Anonima Zona Franca*) com intuitos de *trading* (comércio) ou outros aproveitamentos das zonas francas. Estas empresas têm várias restrições, mas também grandes vantagens fiscais. Existiam, ainda, as empresas "offshore", denominadas de SAFI (*Sociedad Anonima Financiera de Inversion*); que possuía um regime tributário diferenciado para todas as operações realizadas no exterior. Para as SAFIs não existiam os impostos nacionais sobre o faturamento ou sobre os lucros, mas somente um imposto de 0,3% sobre o capital e patrimônio. As SAFIs permitiam a emissão de ações ao portador; ou seja, anônimas. As únicas exigências eram que tivessem um endereço oficial no Uruguai (normalmente o endereço de um contador) e que existisse, pelo menos, um diretor identificado; que poderia ser qualquer pessoa, de qualquer nacionalidade e não precisava ser residente no Uruguai. Após a edição da Lei de Reforma Fiscal (Lei 18.083/2006), não é mais possível abrir SAFIs e as que existiam foram obrigadas a serem transformadas em S.A. (Sociedades Anônimas) normais. E, em junho de 2010, a Receita Federal do Brasil editou a Instrução Normativa n.º 1.037, enquadrando as SAFI's uruguaias como regimes fiscais privilegiados, o que significou que as transações internacionais com essas sociedades se submeteram à tributação na fonte do IR (Imposto de Renda) à alíquota de 25%. O sigilo Bancário no Uruguai é um dos mais rigorosos do mundo (Lei n° 15322/1982).

- https://legislativo.parlamento.gub.uy/temporales/leytemp980702.htm.

Entretanto, **o Uruguai deixou de ser um paraíso fiscal pela OCDE** (Organização para a Cooperação e Desenvolvimento Econômico), porque concluiu 18 acordos de troca de informações.

- http://www.oas.org/juridico/MLA/pt/ury/index.html;
- http://www.oecd.org/countries/uruguay/.

Os mesmos tratados assinados pelo Uruguai foram impostos a vários outros países: Alemanha, Coreia do Sul, Dinamarca, Equador, Espanha, Ilhas Faroe, Finlândia, França, Groelândia, Hungria, Liechtenstein, Malta, México, Noruega, Portugal, Suécia, Suíça, etc.

A legislação uruguaia ainda permite a constituição de sociedades nas quais o controlador permanecia oculto. O CNPJ uruguaio, por causa do Mercosul (http://www.mercosur.int/), permite participar de quase todos os negócios no Brasil, com algumas exceções.

- https://www.presidencia.gub.uy/;
- https://legislativo.parlamento.gub.uy/;
- http://www.mrree.gub.uy/;
- http://www.miem.gub.uy/;
- http://www.uruguayxxi.gub.uy/;
- http://www.dgi.gub.uy/;
- http://negociosnouruguai.com/pt/;
- http://www.contadoresdeluruguay.com.uy/.

Há duas espécies de **sociedades anônimas uruguaias**. Cada uma delas possui especificidades operativas fora do Uruguai, cada qual com seus específicos benefícios tributários:

SAZF - *Sociedad Anónima de Zona Franca* (Sociedade Anônima de Zona Franca). Caracterizada por zonas de livre comércio e industrialização, monitoradas e controladas pelas autoridades uruguaias e administradas pelo Estado e/ou empresários particulares, os quais dispõem das instalações. As sociedades anônimas de zona franca foram criadas para atuar em forma exclusiva nas atividades referentes ao usuário de zona franca. Esse usuário possui o direito de usufruir de exoneração de impostos nacionais (rendas, patrimônio, valor agregado, etc.) sobre as atividades levadas das empresas usuárias e de total isenção de impostos de importação/exportação sobre as entradas e saídas de mercadorias desde a zona franca. Entre as principais

operações realizadas com este tipo de sociedade estão: formação de centros de distribuição e depósitos; *call centers*; prestação de serviços compartidos; fornecimento de serviços financeiros e profissionais; desenvolvimento de *software*; etc.

Sociedade Anônima Local. Com ela é possível realizar atividades no Uruguai, mas também no exterior. Caso não obtenha rendas ou ativo no Uruguai, estará isenta de pagamento de tributos no país. Entre as vantagens da sociedade anônima local está o fato de não estar catalogada como uma sociedade "off-shore". Corriqueiramente, sociedades já constituídas e autorizadas, porém sem atividade prévia, são adquiridas devido à possibilidade de iniciar imediatamente as atividades. Assim que constituída a sociedade, as ações representativas do capital social podem pertencer na sua totalidade a um só acionista. Os acionistas podem ser pessoas físicas ou jurídicas, nacionais ou estrangeiras, residentes ou não no Uruguai. O Diretório (diretoria) poderá estar integrado, conforme determinado no estatuto, por uma ou mais pessoas físicas ou jurídicas, as quais poderão ser nacionais ou estrangeiras, residentes ou não no Uruguai. A diretoria poderá reunir-se no país ou no exterior, com periodicidade estabelecida no estatuto. As assembleias de acionistas deverão ocorrer no Uruguai e devem realizar pelo menos uma Assembleia Ordinária de Acionistas anual. Nesse encontro deverá ser aprovado o balanço e definidas questões relativas à nova diretoria; exceto se o estatuto preveja períodos mais longos para o exercício do cargo de diretor. Empresas multinacionais podem fazer uso de sociedades anônimas uruguaias para realizar operativas de *trading* (comércio), nas quais se utilizaria uma sociedade anônima para participar intermediando em negócios de compra e venda internacional entre países terceiros. O envio da mercadoria não precisa passar pelo Uruguai, se realiza diretamente do país de origem a seu destino final. Pode-se concentrar os lucros na sociedade anônima e reduzir os tributos a pagar através da realização de cobranças e pagamentos no exterior com origens diversas (prestação de serviços, assessorias, comissões...). Através da centralização da tesouraria, há melhora em eficiência no manejo dos fundos, reunindo-os e distribuindo-os em função das necessidades globais de uma área ou de um grupo regional. A titularidade de uma marca ou patente é licenciada a diferentes

sociedades, concentrando as vantagens econômicas na sociedade anônima, reduzindo-se o imposto. É possível a realização de investimentos de diferentes tipos, como bens imóveis no exterior, investimentos de risco, valores de diferentes países, ações, etc. Entretanto, a maior desvantagem de uma formação de empresa no Uruguai é o custo, pois é muito alto quando comparado com outras jurisdições com as mesmas vantagens.

Como norma geral as empresas **panamenhas** pagam impostos somente sobre as atividades, operações e transações efetuadas dentro do território nacional. Se uma empresa opera exclusivamente no exterior não deverá pagar algum imposto além da taxa governamental anual de registro (cerca de 250 USD). Não existe obrigatoriedade para que as empresas constituídas no Panamá manterem escritório no país. Porém é obrigatório que tenham um agente residente, normalmente um advogado, que será responsável com as relações com o governo. Não é obrigatório manter os livros societários no território de Panamá. No caso de não existirem atividades dentro do território do Panamá, também não será necessário apresentar balanços ou declarações ao governo. Para as sociedades panamenhas é obrigatória a existência de, pelo menos, três diretores que podem ser de qualquer nacionalidade e não precisam ser residentes no país. É permitida a emissão de ações ao portador, desde que integralizadas. De acordo com o artigo 89 do Código Comercial da República do Panamá, somente a autoridade judiciária competente do Panamá tem o poder de requerer a cópia de livros fiscais, correspondências ou de outros documentos contábeis. O mesmo artigo prevê que qualquer empresário que fornecer tais documentos para serem usados em procedimentos legais fora da República do Panamá, em cumprimento do pedido da autoridade judiciária diversa da panamenha, deve ser punido com multa de até 10.000 dólares. Desde que os bancos, incluindo as filiais de bancos estrangeiros, na República do Panamá, sejam considerados bancos "merchant" à luz da definição do artigo 89 do Código Comercial, estarão sujeitos a essa multa sempre que fornecerem cópia dos livros contábeis, das correspondências ou de outro documento em violação a esse artigo. Já o artigo 93 prevê que os empresários estão obrigados a manter no território do Panamá os livros contábeis exigidos pela lei, enquanto mantiverem relações comerciais naquele território e por um período de cinco anos sucessivos do término de tal atividade. Outros livros

auxiliares, não exigidos pela lei, e a correspondência devem ser mantidos no território panamenho até que se expire o prazo para não servirem como prova. Além disso, é proibido o transporte dos livros contábeis, da correspondência ou de outra documentação conexa às relações negociais, para fora da República do Panamá. O Panamá e os Estados Unidos, em 11 de abril de 1991, assinaram um TALM (Tratado de Asistencia Legal Mutua) em questões criminais, que exclui expressamente as violações das leis tributarias até que não seja demonstrado que são ligadas ao tráfico de drogas, furtos, crimes violentos, fraudes fiscais ou violação de normas cambiais. As Leis 41 e 42 de 2000 definem "lavagem de dinheiro", que antes era limitada a casos ligados a drogas, incluindo em tal definição os crimes de fraude grave (ou séria), tráfico ilegal de armas e pessoas, terrorismo, sequestro, extorsão, peculato, corrupção de funcionários públicos e roubo ou tráfico internacional de veículos.

O artigo 168 do Código Penal da República do Panamá prevê responsabilidade penal se qualquer pessoa, inclusive os empregados dos bancos, fornecer documentação ou informações de natureza confidencial sem o consentimento da parte interessada ou uma ordem da autoridade competente panamenha. Documentos de natureza confidencial são aqueles legitimamente obtidos e em posse de uma pessoa que não está autorizada por lei a revelar seu conteúdo sem o consenso de quem os tenha fornecido. Segundo o estabelecido pelo artigo 170 do Código Penal, qualquer pessoa que vier a tomar conhecimento de informações confidenciais devido a sua atividade, emprego ou arte, e que revela tais informações sem o consentimento da parte interessada na manutenção do segredo, pode estar sujeita a responsabilidade penal. Tal responsabilidade penal, entretanto, não emerge das disposições deste artigo sempre que as informações sejam reveladas a fim de tutelar um "interesse superior", mesmo se o Código Penal não fornece uma definição precisa da expressão "interesse superior". Da responsabilidade penal pode surgir também uma responsabilidade relacionada às normas dos artigos 119, 120 e 125 do Código Penal e do artigo 1.986 do Código de Processo Penal. Segundo tais artigos, cada empregado ou funcionário de um banco que cometa um crime, ou o próprio banco nos casos em que o crime tenha sido cometido por um de seus dirigentes, administradores ou representantes legais, podem ser considerados conjuntamente responsáveis por todos os danos,

compreendidos os de natureza moral causados à vítima do crime, a sua família ou eventualmente também a uma terceira pessoa. É necessário sublinhar que o artigo 263 deste Código Penal requer que os funcionários e empregados de um banco indiquem e documentem todas as transações bancárias que conheçam e que estejam relacionadas com operações de tráfico de drogas ou lavagem de dinheiro.

Ao determinar a intenção da autoridade da Comissão Bancária de investigar e fiscalizar o sistema bancário, a legislação bancária panamenha (Decreto de Gabinete 238, de 2 de junho de 1970) proíbe explicitamente a tal órgão examinar contas bancárias, valores em custódia, depósitos fiduciários ou documentação relativa às operações específicas de crédito que um cliente pode ter efetuado com um banco que tem licença de operar no Panamá, sem que seja requerida uma ordem do tribunal. A legislação bancária dá poder à Comissão Bancária de impor uma multa de até mil dólare (USD), no caso de qualquer pessoa fornecer informações violando as disposições vigentes, sem prejuízo de uma possível responsabilidade penal e civil advinda como resultado de tal violação. Os bancos que mantêm contas numeradas estão sujeitos a alguns deveres de sigilo adicionais relacionados a tais contas. O artigo 4 da Lei 18 de 1989 (lei das contas numeradas), estabelece pena de detenção de trinta dias a seis meses e/ou uma multa de mil a dez mil dólares a todo dirigente, diretor, gestor de conta ou empregado de um banco que revele ou divulgue a qualquer pessoa estranha ao banco, e não designada na referida conta, informações ligadas à existência, montante ou titularidade da conta. Esta disposição especial estabelece que tais informações privilegiadas são reveladas exclusivamente aos promotores públicos, juízes e magistrados criminais, e impõe ao bancário a obrigação de refutar-se de atender a uma requisição de informações advinda de uma autoridade diferente daquela relacionada aos procedimentos de natureza penal.

A Associação Bancária do Panamá é uma organização ou corporação privada de banqueiros, não oficial, cujos membros são bancos nacionais ou estrangeiros que desenvolvem suas atividades no país. A Associação adotou um código de conduta para as operações bancárias com o objetivo de estabelecer as normas operativas que os bancos membros devem utilizar a fim de evitar casos de lavagem de dinheiro. Recentemente, a Associação

aderiu à Declaração dos Princípios para a Prevenção do Uso Ilegal do Sistema Bancário, emitida pelo Banco das Transações Internacionais na Basiléia, Suíça. Esta é certamente apenas uma declaração de intenções seguida pelos bancos e não um instrumento legal, mas pode ser interessante neste contexto. Seus pontos principais são: 1) Os bancos devem se esforçar para determinar a verdadeira identidade do cliente a fim de assegurar que o sistema financeiro não seja utilizado como canal para fundos de origem ilegal; e, 2) Os bancos devem cooperar com as autoridades nacionais encarregadas de aplicar a lei, nos limites estabelecidos pelos regulamentos nacionais, resguardada a confidencialidade. Caso os bancos venham a saber de fatos que tragam suspeita da existência de dinheiro ou depósitos derivados de atividade ilegal, devem adotar medidas apropriadas, de acordo com a lei, para fechar ou suspender a conta.

Ressalta-se que, **em razão da luta contra o terrorismo empreendida pelos Estados Unidos, com o apoio da União Europeia, depois do atentado nas torres gêmeas (*World Trade Center*) em 11/09/2011, o sigilo e a privacidade, antes absolutas, foram relativizadas.**

Depois do **escândalo "Panama Papers"** (Documentos do Panamá) em 2015, fruto de uma investigação jornalística internacional, que através do vazamento de documentos confidenciais, expôs um esquema mundial de ocultação de dinheiro e patrimônio em paraísos fiscais, muitos desses países não gostaram da má reputação e passaram a rever seus conceitos e, assim, surgiu a onda de maior transparência dos centros *offshore*. O Liechtenstein (pequeno país encravado entre a Suíça e a Áustria), por exemplo, passou a dispensar dinheiro não declarado.

- https://panamapapers.icij.org/.

Outro escândalo que ajudou a extinguir os sigilos bancários e agilizar as colaborações recíprocas entre os países foi o fato do banco HSBC ter ajudado vários milionários a sonegarem impostos. Entre os supostos beneficiados pela ajuda do HSBC suíço a clientes de mais de 200 países estão políticos, empresários, estrelas do esporte, celebridades, além de criminosos e traficantes, segundo a investigação. Uma investigação feita na França revelou que a filial suíça do banco britânico HSBC ajudava clientes

ricos a evadir o pagamento de milhões de dólares em impostos. Quando foram introduzidas novas leis na Europa em 2005 obrigando bancos suíços a recolher impostos de contas não declaradas e repassá-los às respectivas autoridades fiscais, o banco suíço escreveu aos clientes oferecendo formas de contornar os tributos. As informações foram vazadas em 2007 por um ex-funcionário do banco em Genebra, Herve Falciani. O HM Revenue and Customs do Reino Unido recebeu os dados em 2010 e identificou 7 mil clientes britânicos que não pagaram impostos. Na Argentina, a Administração Federal de Receitas Públicas denunciou a filial local do HSBC em novembro de 2014 por supostamente ajudar 4.040 cidadãos do país a evadir impostos. Em 2012, o HSBC pagou uma multa recorde de US$ 1,9 bilhão para pôr fim a investigações americanas em um caso de lavagem de dinheiro ligado ao tráfico de drogas.

Durante muito tempo, a **Suíça** era conhecido por hospedar as contas bancárias de pessoas físicas estrangeiras e empresas *offshore*. Mas o sigilo bancário suíço está extinto desde 2013. A pressão dos americanos pela assinatura suíça ao FATCA (*Foreign Account Tax Compliance Act*), que prevê a troca de informações bancárias com o objetivo de combater a evasão de divisas, levou a Suíça parar de aceitar clientes que não desejam regularizar a sua situação. E, desde 2016, a Suíça passou a entregar informações de clientes brasileiros em banco suíços, mediante pedido das autoridades do Brasil, nos termos do acordo entre os países que integram o Fórum Global, da OCDE - Organização para a Cooperação e Desenvolvimento Econômico (OECD - *Organisation for Economic Co-operation and Development* - http://www.oecd.org/), e do G-20, que trata da troca de informações bancárias para fins fiscais.

Em 2010, por exemplo, a Suíça bloqueou uma conta de US$ 13 milhões de Fernando Sarney, filho do ex-presidente José Sarney.

- http://politica.estadao.com.br/noticias/geral,banco-usado-por-cunha-na-suica-o-denunciou-por-lavagem-de-dinheiro,1772389;
- http://opiniaoenoticia.com.br/brasil/suica-entrega-ao-brasil-investigacao-sobre-contas-de-cunha/;
- http://www.diariodocentrodomundo.com.br/essencial/banco-suico-entrega-documentacao-completa-de-conta-de-eduardo-cunha/;

- http://g1.globo.com/politica/operacao-lava-jato/noticia/2015/09/suica-envia-para-o-brasil-apuracao-sobre-conta-de-eduardo-cunha.html;
- http://brasil.elpais.com/brasil/2015/10/10/politica/1444440579_636689.html;
- http://epoca.globo.com/tempo/noticia/2015/02/lista-das-bcontas-de-brasileiros-no-hsbcb-na-suica.html;
- http://agenciabrasil.ebc.com.br/politica/noticia/2016-01/lista-de-correntistas-brasileiros-do-hsbc-na-suica-deve-ser-entregue-cpi;
- http://exame.abril.com.br/negocios/revista-traz-lista-de-contas-de-brasileiros-no-hsbc-na-suica/.

A Suíça, foi líder indiscutível na gestão das fortunas privadas de clientes estrangeiros, que lhe permitiu atrair durante décadas (desde 1934) todos os que tinham muito dinheiro e queriam fugir do Fisco e das autoridades. Entretanto, outrora famosa pelo seu sistema financeiro impenetrável a tentativas de terceiros em acessar os dados dos clientes, sob forte pressão internacional nos últimos anos, começou já a reunir dados bancários dos clientes estrangeiros no âmbito do intercâmbio automático de informação acordado com os países da Organização para a Cooperação e Desenvolvimento Económico (OCDE). Embora o sistema automático só comece a funcionar em 2018, na prática o país enterrou já o segredo bancário; vez que já começou a dar os primeiros passos para recolher as informações que irá enviar. Explica-se. A partir de 2018, as informações financeiras dentro dos países membros da OCDE serão enviadas, de forma anual e automática, aos Fiscos (Receitas Federais) dos países de origem dos respectivos clientes. Desse modo não será mais preciso aos governos requisitarem informações de pessoas específicas; ou seja, as informações serão de todos os clientes, mesmo quando não existam indícios de ilícito criminal. Detalhe, os cidadãos portugueses já são "denunciados" pela Suíça desde 2013.

Em 2009, o banco suíço UBS aceitou, sob a ameaça de ter sua licença retirada nos Estados Unidos, entregar à Justiça americana o nome de algumas centenas de clientes acusados de fraude fiscal, apesar de não haver na época uma cooperação administrativa.

Ainda em 2009, a Suíça havia sido incluída na "lista cinza" de paraísos fiscais da OCDE, mas foi retirada logo depois após firmar doze convenções internacionais de troca de informações fiscais com países como a França, Estados Unidos, Grã-Bretanha e Espanha.

A **AEOI** é aplicada por 56 países (incluindo todos os países europeus a partir de 2017) e, a partir de 2018, contará com mais 42 países adicionais (http://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/crs-by-jurisdiction/).

O **FATCA** (*Foreign Account Tax Compliance Act*) é um acordo separado que foi criado pelos Estados Unidos com 112 países do mundo (Rússia não assinou).

- https://www.treasury.gov/resource-center/tax-policy/treaties/Pages/FATCA.aspx;
- http://non-fatca-banks.com/.

A partir de 2017, a Suíça, como boa parte dos paraísos fiscais, incluindo os mais opacos, como Panamá, serão obrigados a revelar ao fisco de outros países os dados de clientes com depósitos acima de US$ 250 mil. Estará sendo aplicado, então, o padrão global de troca automática de informações, instituída pela OCDE por solicitação do G-20, fórum informal que reúne os principais países industrializados e economias emergentes, entre as quais o Brasil. O Brasil, em novembro de 2011, durante a cúpula de Cannes do G-20, aderiu ao o acordo da OCDE. Tais normas substituem o padrão anterior pelo qual um país solicita a outro (país) assistência em investigações fiscais ou de interesse da Justiça. Pelo novo padrão, os governos obterão informações de suas instituições financeiras e as trocarão com outros países, sobre diferentes tipos de contas, para frear a evasão fiscal e ajudar as autoridades a identificar quem oculta dinheiro em paraísos fiscais. Será objeto de troca automática dados sobre juros, dividendos, saldos de contas e rendimentos de alguns produtos de seguros, venda de ativos financeiros e outras rendas geradas por ativos ou pagamentos efetuados por meio da conta bancária.

- http://g1.globo.com/economia/noticia/suica-acaba-com-sigilo-bancario-em-2017-e-instituicoes-devem-entregar-clientes.ghtml;

- http://economia.uol.com.br/noticias/efe/2017/01/01/suica-diz-adeus-ao-sigilo-bancario-em-2017.htm.

A implantação em 2017 da troca automática de informações (AEOI - *Automatic Exchange of Information*), significa o desaparecimento do sigilo bancário no mundo. A troca automática de informações (AEOI) é um padrão definido pela OCDE. A MCAA - *Mutual Competent Authority Agreement* (Convenção Multilateral sobre Assistência Mútua Administrativa em Matéria Fiscal ou *Convention Multilatérale concernant l'Assistance Administrative Mutuelle en matière fiscale*) define que autoridade deve recolher, enviar e receber informações para compartilhar. Ter uma conta bancária *offshore* em um país da jurisdição da AEOI (um estado signatário da AEOI), significa o informe automático dessa conta ao fisco do país de residência de seu titular.

Áustria, Bélgica e Luxemburgo escolheram um sistema transitório de imposto retido na fonte por um determinado período. Assim, o sigilo bancário, ainda é relativamente preservado nestes três países. Entretanto, se o cliente não residente negar informações, tentar ficar anônimo ou ocultar do seu fisco de origem, é feita uma retenção na fonte de 35% sobre a receita financeira e o imposto fixo é pago (em parte) ao país de residência do cliente. Por outro lado, se o não residente aceitar a troca de informações com o seu país de residência, a renda vai ser declarada e tributada no seu fisco de origem e a tributação aplicada na Áustria, Bélgica e Luxemburgo será dedutível no fisco do país de domicílio.

Até 2018, os 129 países que participam do Global Fórum, da OCDE, devem adotar o acordo para troca de informações. Apenas países com alto risco econômico e político, que fazem parte da lista do Grupo de Ação Financeira Internacional (GAFI), que visa combater a lavagem de dinheiro e financiamento de terrorismo, não são obrigados a cumprir as novas regulamentações. O GAFI (Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo) ou FATF (*Financial Action Task Force*) é uma organização intergovernamental cujo propósito é desenvolver e promover políticas nacionais e internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo (http://www.fatf-gafi.org/).

- http://www.coaf.fazenda.gov.br/backup/pld-ft/novos-padroes-internacionais-de-prevencao-e-combate-a-lavagem-de-dinheiro-e-ao-financiamento-do-terrorismo-e-da-proliferacao-as-recomendacoes-do-gafi-1.

Mesmo países da América do Sul, que eram usados como paraísos fiscais também estão apertando o cerco.

O **Brasil** possui vários tratados ou convenções internacionais (no mínimo, 108) para evitar a dupla tributação e a evasão fiscal, como, por exemplos, com os seguintes países: África do Sul, Argentina, Áustria, Bélgica, Canadá, Chile, China, Coréia do Sul, Dinamarca, Equador, Espanha, Filipinas, Finlândia, França, Hungria, Índia, Israel, Itália, Japão, Luxemburgo, México, Noruega, Países Baixos (Holanda), Peru, Portugal, República Eslovaca, República Tcheca, Suécia, Ucrânia, etc.

Em setembro de 2015, começou a troca de informações fiscais entre os Estados Unidos e o Brasil. O Decreto nº 8.506, de 24.8.2015 (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8506.htm), oficializou a implementação do FATCA (*Foreign Account Tax Compliance Act*). Em setembro de 2015, tanto os fiscos americano e brasileiro trocaram dados sobre contas bancárias com saldo superior a US$ 50 mil. Portanto, os brasileiros que possuem conta bancária nos Estados Unidos têm as informações de investimentos e rendimentos enviadas à Receita Federal do Brasil pelos bancos americanos. E o inverso também; ou seja, os americanos que possuem conta bancária no Brasil têm as informações de investimentos e rendimentos enviadas à Receita Federal americana pelos bancos brasileiros. A punição para os bancos que não aderem ao acordo é a taxação de 30% de todos os valores remetidos da instituição financeira nos Estados Unidos para qualquer filial estrangeira.

- https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca;

- http://idg.receita.fazenda.gov.br/sobre/consultas-publicas-e-editoriais/editorial/cooperacao-tributaria-internacional;

- http://www.itamaraty.gov.br/pt-BR/discursos-artigos-e-entrevistas-categoria/outras-autoridades-artigos/13916-cooperacao-tributaria-internacional-o-estado-de-sao-paulo-26-4-2016.

Os Estados Unidos já repassaram informações referentes a 25 mil contas de brasileiros em território americano. O mesmo acordo foi assinado por paraísos fiscais como Ilhas Cayman e Ilhas Virgens Britânicas.

Em 23/11/2015 o Brasil assinou um acordo com a Suíça de troca direta de informações financeiras e tributárias.

- http://www.brasil.gov.br/governo/2015/11/brasil-e-suica-firmam-acordo-para-combater-evasao-e-sonegacao;
- http://idg.receita.fazenda.gov.br/noticias/ascom/2015/novembro/brasil-e-suica-tracarao-informacoes-tributarias;
- http://g1.globo.com/economia/noticia/2015/11/brasil-assina-acordo-com-suica-para-troca-de-informacoes-tributarias.html;
- http://www1.folha.uol.com.br/poder/2015/11/1709914-acordo-entre-receitas-do-brasil-e-da-suica-so-abrange-informacoes-futuras.shtml;
- http://www.swissinfo.ch/por/brasil-e-suíça_os-laços-se-estreitam/41932350;
- https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/korruption.html;
- https://www.efd.admin.ch/efd/en/home.html.

A troca de informações está prevista principalmente no âmbito da Convenção Multilateral para Intercâmbio Internacional Tributário (Decreto nº 8.842 de 29/08/2016 - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8842.htm). O acordo entre países membros da OCDE - Organização para a Cooperação e Desenvolvimento Econômico (http://www.oecd.org/) pretende combater o financiamento do terrorismo e crimes de lavagem de dinheiro. Detalhe, até a Suíça aderiu ao OCDE.

- http://www.itamaraty.gov.br/pt-BR/component/tags/tag/15-ocde-organizacao-para-a-cooperacao-e-o-desenvolvimento-economico;
- http://idg.receita.fazenda.gov.br/noticias/ascom/2016/junho/brasil-ratifica-a-convencao-multilateral-e-tera-amplo-acesso-a-informacoes-tributarias-do-exterior;
- http://idg.receita.fazenda.gov.br/noticias/ascom/2016/junho/arquivos-e-imagens-2/convencao-multilateral-texto-em-portugues.pdf;

- https://www.oecd.org/ctp/exchange-of-tax-information/POR-Amended-Convention.pdf;
- http://www.oecd.org/ctp/exchange-of-tax-information/Status_of_convention.pdf.

A IN RFB (Instrução Normativa da Receita Federal do Brasil) nº 1680/2016 trata do Padrão de Declaração Comum (*Common Reporting Standard*) e a IN RFB nº 1681 institui a Declaração País a País. A diretriz básica da OCDE consta da IN RFB nº 1662/2016.

- IN RFB nº 1680, de 29/12/2016 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=79443;
- IN RFB nº 1681, de 29/12/2016 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=79444;
- IN RFB nº 1662, de 30/09/2016 - 2016 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=77848;
- Lei nº 13.043, de 13/11/2014 - http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/Lei/L13043.htm.

A troca de informações inclui, dentre outras informações, saldo bancário, cartão de crédito e posições de investimentos como ações, renda fixa, CDBs, títulos públicos e letras hipotecárias, etc. No caso de *trusts* (confianças), instrumento legal de gestão de ativos, os bancos terão que identificar e informar o beneficiário.

A partir de 2017, mais tardar 2018, é certo que a Suíça, como todos os outros países membros da Comunidade Europeia, irá declarar contas bancárias automaticamente.

Em resumo, dentro do país onde estão instalados ou trabalham, os bancos já denunciavam há décadas seus clientes à Receita Federal local. Agora irão denunciar todos os clientes dos países que fazem parte de diversos acordos internacionais de troca de informações e quebras de sigilos. Detalhe, outras entidades que fazem parte dos sistemas financeiros e de pagamentos também prestam informações periódicas à Receita Federal.

E, pior, não serão somente os bancos, mas os próprios contadores e escritórios de contabilidade também irão denunciar seus clientes.

- http://www.jornalcontabil.com.br/contadores-terao-de-informar-irregularidades-de-clientes-ao-fisco/;
- http://contadores.cnt.br/noticias/tecnicas/2017/01/03/contadores-na-berlinda-profissionais-terao-que-informar-irregularidades-de-seus-clientes-ao-fisco-a-partir-de-2017.html.

Portanto, para complicar ainda mais, o Brasil deve adotar, a partir de julho de 2017, uma nova norma internacional que obriga contadores das empresas e auditores independentes a se reportarem às autoridades competentes quando descobrirem, no exercício de suas funções, desvios de leis e regulamentos, como práticas de corrupção, lavagem de dinheiro e determinação deliberada de não pagar impostos. Trata-se da norma apelidada de Noclar (*non-compliance with laws and regulations*); que traduzida significa não-conformidade com leis e regulações.

- http://www.valor.com.br/empresas/4768369/contador-tera-que-reportar-irregularidade-partir-do-ano-que-vem;
- https://www.cpacanada.ca/en/connecting-and-news/blogs/audit-quality-blog/2016/december/new-noclar-implications-for-canadian-auditors;
- http://www.iaasb.org/projects/noclar;
- http://www.ifac.org/publications-resources/smp-committee-response-iesba-exposure-draft-responding-non-compliance-laws.

Tanto é assim que em breve os cidadãos não precisarão mais fazerem declaração de imposto de renda, mas tão somente irão conferir e aprovar ou retificar o teor da declaração feita (pré preenchida) pelo software da Receita Federal.

- http://www.acifnet.com.br/contribuintes-com-certificado-digital-terao-pre-preenchimento-automatico-da-declaracao-do-imposto-de-renda/;
- http://www.portaltributario.com.br/artigos/dirpfpronta.htm;
- http://economia.estadao.com.br/noticias/geral,declaracao-automatica-do-ir-valera-so-para-1-milhao-de-pessoas-em-2014,173089e.

Além do OCDE existem diversos outros tratados internacionais de fornecimento de informações. Um exemplo recente é a Operação Lava Jato do Ministério Público Federal que conseguiu informações de dezenas de países através de 159 acordos de cooperação jurídica internacional para troca de provas de corrupção e lavagem de dinheiro pelo mundo.

- http://politica.estadao.com.br/blogs/fausto-macedo/em-3-anos-operacao-lava-jato-chegou-a-37-paises/.

Embora muitos países europeus e os da CEE (Comunidade Econômica Europeia) comprometeram-se a respeitar a troca automática de informações, existem alguns países europeus que, até o presente, ainda não assinaram os acordos: Armênia, Azerbaijão, Belarus, Bósnia, Geórgia, Cazaquistão, Macedónia, Moldova, Montenegro, Sérvia, Ucrânia e Vaticano. Entretanto, o IOR - Instituto para as Obras de Religião (http://www.ior.va/), mais conhecido como Banco do Vaticano, é uma instituição financeira ligada a Santa Sé e localizada na Cidade do Vaticano. O IOR diz seguir rigorosas exigências antilavagem de dinheiro (*anti-money laundering*), em linha com os melhores padrões internacionais e que em outubro de 2015, após a revisão de todas as contas, teriam sido encerradas 4.935 contas.

Mais de 100 jurisdições não assinaram o AEOI, o que significa que eles não vão trocar informações automaticamente. No entanto, a falta de acordo AEOI entre estes tribunais não significa que não haverá troca de informações, pois podem ocorrer através de pedidos, administrativos ou judiciais, e serem fornecidas de forma espontânea. Além do que tais países podem ter assinado outro tipo de tratado ou acordo similar.

Em um período mais recente, a Letônia era muito popular com as empresas *offshore*, e numerosas contas bancárias *offshore* foram abertas com os bancos deste pequeno país báltico. Os bancos da Letônia, através de um sigilo bancário ambíguo, permitiam as autoridades locais o acesso às informações bancárias mediante pedido judicial, mas não tiveram essa burocracia para fornecerem acesso a outros países. Assim, os bancos como Rietumu Bank, Baltikums, Pasta Banka ou ABLV, que tinham milhares de clientes europeus cujas contas bancárias gradualmente foram fechando devido à introdução da troca automática de informações.

Na Suíça, a maioria das contas de clientes no exterior já foram fechadas e a Letônia está prestes a fazer o mesmo, só que desta vez, os beneficiários não serão avisados com antecedência.

A Comissão Europeia pretende alargar esta diretiva para outras áreas geográficas e, em particular, aos centros financeiros que atualmente são amplamente favorecidos para abrir a conta bancária *offshore* de uma empresa *offshore* (Hong Kong ou Cingapura, por exemplo).

Algumas **opções para escapar da AEOI/OCDE e FATCA** são:

- Transferir os investimentos para uma jurisdição não signatária da AEOI/OCDE e FATCA. A lista dos países signatários da OEAI e FATCA inclui a maioria da Europa e os países mais desenvolvidos, restando de fora, na grande maioria, apenas países africanos e do médio oriente (como o Líbano), onde não se recomenda fazer investimentos. Exceções interessantes, por enquanto, seriam Taiwan, Tailândia e, quem sabe, África do Sul. Mas, no longo prazo, o AEOI será aplicado globalmente;

- Torna-se residente fiscal em uma jurisdição com impostos baixos (ou zero), ou que não tribute a renda estrangeira: Dubai, Hong Kong, Malta, Singapura e o regime de não residente no Reino Unido. Quem não tem passaporte britânico e não é filho de ingleses, não paga imposto sobre a propriedade que tinha antes de chegar ao Reino Unido (*Overseas*). Basta declarar à HMRC - *Her Majesty's Revenue and Customs* ou Receita de Sua Majestade e Alfândega (http://www.hmrc.gov.uk/) que pretende estabelecer-se no Reino Unido, de forma temporária, e, portanto, deseja optar pelo regime fiscal de não residentes no Reino Unido (conhecidos como *Non-UK* ou *UK Non domicilied*);

- Remover os fundos bancários e investir em ativos não-financeiros, como, por exemplos, imóveis, joias, obras de arte, etc.;

- Transferir a propriedade para não para aparecer como beneficiário;

- Transferir os ativos para uma *Trust Company* (empresa de confiança ou empresa de negócios de fideicomisso) ou uma fundação privada;

- Criar uma parceria limitada da qual não seja o sócio-gerente;

- Usar a propriedade para pagar um contrato de seguro de vida, como, por exemplo, uma apólice de seguro individual de vida com prémio variável;

- Investir em *private equity* (ativo privado) que não dá o controle e não produz rendimentos, mas apenas ganhos a longo prazo. Consiste em investir em empresas que ainda não são listadas em bolsa de valores; ou seja, que ainda estão fechadas ao mercado de capitais. Portanto, trata-se da compra de participação em empresas (tornando-se sócio do negócio) que possuam boas faturações monetárias e que estejam em notável crescimento. Saiba mais em http://www.abvcap.com.br/Download/Guias/2726.pdf;

- Doar a propriedade para filhos e/ou uma instituição de caridade.

- Utilizar uma empresa financeira que possua um CB - *Carte Bancaire* (cartão de banco) com anonimato. O VIABUY MasterCard pré-pago (https://www.viabuy.com/pt/vantagens/internet-e-entretenimento.html), por exemplo, permite fazer compras de forma anônima e segura porque não é vinculado à conta bancária ou ao cartão de crédito, os pagamentos não aparecem em respectivos extratos e não serão enviados extratos para a residência do titular. Os dados pessoais ficam protegidos. É aceito na Google Play Store, Apple App Store, iTunes Store, Xbox LIVE, iTunes Store USA e App Store USA. Ou, ainda, a utilização de cartões de débito anônimo (http://pt.sfm-offshore.com/news/solicite-um-cartao-de-debito-anonimo.html), de preferência, com números descartáveis.

Confira um livro do Sebrae que dá dicas para empreender fora do Brasil:

- http://www.sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/MG/Sebrae%20de%20A%20a%20Z/LIVRO%20REMESSAS_vers%C3%A3o%20eletr%C3%B4nica.pdf.

MICRONAÇÕES E LOCAIS SEM JURISDIÇÃO

Conforme visto no capítulo anterior, estão sendo extintos os paraísos fiscais, com o que as micronações, áreas independentes e territórios internacionais ("terra de ninguém" ou local sem nenhuma jurisdição) são possíveis candidatos para a constituição de novas versões dos paraísos fiscais ou para a localização de computadores servidores (hospedeiros) de sites.

Em águas internacionais ou em espaço aéreo internacional, aplica-se a legislação do país de onde o veículo (embarcação ou aeronave) estiver registrado; mas não em relação a navios de brinquedo e aos drones particulares e sem registro. De modo semelhante, um site ou servidor está sujeito à legislação do país onde está registrado ou hospedado; com isso sites de apostas, casinos, pornografia, pedofilia... estão localizados em países onde tais práticas são permitidas e, de preferência, que não cedam às pressões de outros países para identificar e/ou entregar os responsáveis. A mesma regra se aplica a empresas, bancos, celebração de contratos... se a realização do negócio é feita totalmente *online* (pela internet).

O espaço sideral é, também, tido por território internacional e, assim, os satélites estão vinculados aos respectivos países que os enviaram. Servidores de torrents já cogitaram lançarem seus próprios satélites ao espaço.

- http://www.mkmusic.com.br/mknews/partido-pirata-internacional-quer-lancar-satelite/.

Já que mais nenhum país ou banco quer saber de *offshore*, por que não construir o próprio banco? Ou, até mesmo, criar o próprio país? Apesar de, à primeira vista, parece loucura ou ser impossível, alguns grupos religiosos já fizeram tal coisa. Assim, por exemplo, cerca de 70% da população do Estado norteamericano de Utah são fiéis da Igreja de Jesus Cristo dos Santos dos Últimos Dias, mais conhecidos por mórmons. Os mórmons instalaram-se na região primeiramente em 1847. Em 1849, os mórmons criaram um Estado, nomeado de *Deseret* (mel de abelha, na linguagem do Livro de Mórmon). Ao longo de 1849 e de 1850, os mórmons pressionaram o governo americano a fazer com que Deseret fosse elevado à categoria de Estado. Até que em

1850, o Congresso americano criou o Território de Utah. Salt Lake City é a capital e a cidade mais populosa do estado norte-americano de Utah. A cidade foi fundada em 1847 no Great Salt Lake City por um grupo de pioneiros mórmons liderados por seu profeta, Brigham Young. Salt Lake City abriga a sede de A Igreja de Jesus Cristo dos Santos dos Últimos Dias.

O **Amambay Trust Bank Ltd**, criado em 1995 nas Ilhas Cook, teria sido um banco paraguaio oculto, sem sede e nem equipe, exclusivamente criado para a prática de lavagem de dinheiro, que funcionou até 2000.

- http://desacato.info/paraguai-banco-de-horacio-cartes-e-ligado-a-paraiso-fiscal/.

Existem dezenas, senão centenas, de **micronações** desconhecidas da maioria da população. Infra elencamos algumas.

Liberland (https://liberland.org/) é um território ermo, localizado na margem oeste do rio Danúbio entre a Croácia e a Sérvia, que não foi reivindicado por nenhuma nação após a separação da Iugoslávia, com o que o checo, Vít Jedlicka, em abril de 2015, fincou uma bandeira no local e se autoproclamou presidente da nova República Livre de Liberland.

- http://veja.abril.com.br/mundo/liberland-o-pais-sem-governo-e-sem-cobranca-de-impostos/;
- http://economia.uol.com.br/noticias/bloomberg/2015/07/21/conheca-a-liberlandia-o-lugar-sem-impostos-onde-reina-o-crowdfunding.htm;
- http://www.tvi24.iol.pt/acredite-se-quiser/liberland/este-homem-fundou-um-novo-pais-na-europa.

No primeiro semestre de 2017, seis casas, cada uma com capacidade para doze pessoas, devem ser construídas para receber os primeiros moradores de Liberland.

- https://vimeo.com/178972497;
- http://constitution.ll.land/;
- https://liberlandpress.com/;
- http://liberlandsa.org/;

- http://www.air-liberland.org/.

De modo semelhante, o americano Jeremias Heaton localizou uma área (Bir Tawil) entre o Egito e o Sudão, que não é de nenhum país, e colocou uma bandeira desenhada pela filha de 7 anos e constituiu o **Reino de Sudão do Norte**.

- http://oglobo.globo.com/mundo/homem-acha-territorio-que-nao-de-nenhum-pais-anuncia-reinado-para-que-sua-filha-seja-princesa-13256932;
- http://www.fatosdesconhecidos.com.br/homem-acha-territorio-que-nao-e-de-nenhum-pais-e-anuncia-reinado/;
- http://www.bbc.com/portuguese/noticias/2014/07/140715_territorio_filha_pai.

Sealand (http://www.sealandgov.org/) é uma micronação localizada no Mar do Norte, a 10 km da costa de Suffolk, no sudeste da Inglaterra. O território resume-se a uma grande base naval construída pelo Reino Unido durante a Segunda Guerra Mundial. Outrora chamada de *Rough Towers*, a base foi uma defesa marítima contra ataques alemães, consistindo em duas grandes torres com capacidade para 200 soldados. Foi desativada assim que a guerra acabou. Historicamente, a fortificação pertence ao Reino Unido, mas está localizada fora dos seus domínios territoriais. Como, também, está fora dos domínios territoriais da França, se trata de "terra de ninguém". Desde 1967, a instalação tem sido ocupada pelo então Major britânico Paddy Roy Bates; seus colegas e familiares afirmam que ela é um Estado soberano independente. No começo de janeiro de 2007, o príncipe Michael de Sealand decidiu pôr a ilha artificial à venda por 1 milhão de libras. Em 2007 os administradores do site *The Pirate Bay* anunciaram o interesse em comprar Sealand para hospedar os seus servidores, mas o negócio acabou não se concretizando.

- http://www2.uol.com.br/historiaviva/noticias/sealand_o_menor_pais_do_mundo.html;
- http://www.megacurioso.com.br/bizarro/45604-conheca-sealand-o-menor-pais-do-mundo-video.htm.

Renato Barros, um português de 56 anos, conseguiu estabelecer seu próprio país ao adquirir (por cerca de 45 mil euros em 2000) uma pequena

ilha no porto do Funchal, Ilha da Madeira, Portugal. Nomeou-a **Principado da Pontinha** (http://www.principality-pontinha.com/), ungiu-se príncipe "Renato II, o Justo" e declarou independente em 2007. A ilha já não é, à luz do direito internacional, território português, desde 1903. A Bitcoin é a moeda oficial desde 2015.

- http://www.mdig.com.br/index.php?itemid=32843;
- https://www.noticiasaominuto.com/pais/557232/fundou-o-seu-proprio-principado-na-madeira-e-conta-tudo-no-cinema.

O **Reino de Elleore** (http://www.elleore.dk/) foi criado em 1944, depois que um grupo de professores de Copenhagen decidiu comprar uma pequena ilha ao norte da cidade de Roskilde, na ilha de Zelândia, Dinamarca.

Seborga (http://www.principatodiseborga.com/pds/ e http://seborga.net/), foi fundado na Itália por Giorgio Carbone em 1963 e se autoproclama como independente. Giorgio I, que se autoproclamou príncipe de Saborga, afirma que a região não está na criação da República Italiana em 1946, nem na Unificação da Itália em 1861, por Giuseppe Garibaldi. Então, por Giorgio I, as terras não tinham dono.

Talossa (http://www.kingdomoftalossa.net/index.cgi) foi criado em 1979, por Robert Madison (que na época tinha 14 anos de idade), e afirma que seu território ocupa uma área que se espalha de parte de Milwaukee até uma ilha francesa desabitada, além de uma boa porção da Antártida.

Porto Claro (http://www.portoclaro.com.br/) é uma micronação criada por Pedro Aguiar, em 25 de setembro de 1992, que funcionou tendo por forma de governo uma monarquia entre 1992 e 1998 e, depois, na forma de república, que configura na Internet até hoje.

O **Sacro Império de Reunião** (http://www.reuniao.org/) é uma micronação fundada em 28 de agosto de 1997, que reivindica, como território de referência, a Ilha de Reunião, parte do Arquipélago dos Açores e de Maurício. Seus criadores foram estudantes da Pontifícia Universidade Católica do Rio de Janeiro, e, até hoje, a maioria dos seus "cidadãos" são brasileiros e portugueses.

O **Território Livre de Ely-Chaitlin** é uma das mais antigas micronações do mundo, existente de 1963 até hoje.

O **Reino da Chocônia** (em inglês, Choconya) é uma micronação modelista anglófona.

O **Principado de Zugesbucht** é uma micronação modelista anglófona. O finlandês Ben Lytz e os seus descobriram que o Vaticano é um tipo interessante de Estado e resolveram transpassá-lo para o universo dos micropaíses, criando o Principado de Zugesbucht e a Congregação Católica Sem Dogma (CCSD). Ben se intitulou Príncipe-Cardeal e distribuiu terras aos amigos de outros países.

Na costa de Israel, bem ao sul do Líbano, há um pequeno e distinto pedaço de terra, Eli Avivi constituiu seu próprio país, **Achzivland** (http://pechkin.rinet.ru/vera/).

- http://www.bbc.com/portuguese/noticias/2015/03/150312_homem_pais_israel_rm.

O **Império Aericano** (http://www.aericanempire.com/), reivindica como seu território uma ilha localizada no meio de um lago na Nova Zelândia e, ainda, áreas e outros planetas.

Kugelmugel (http://kugelmugel.eu/) possui como território independente apenas a casa de seu fundador.

- http://www.croynielsen.de/km_eng.htm.

Calsahara (http://travisdmchenry.wixsite.com/calsahara) é uma pequena nação na Califórnia.

Northwest Front (http://northwestfront.org/) é um movimento norte-americano de criação de uma nação ariana. Isso mesmo, neonazistas (aqueles que dizem: Heil Hitler!).

- http://www.vice.com/pt_br/read/esse-cara-quer-fundar-um-pais-ariano.

Asgardia (http://asgardia.space/), um país fora do planeta Terra está recrutando moradores.

- http://exame.abril.com.br/tecnologia/voce-pode-ser-cidadao-do-primeiro-pais-fora-da-terra/.

Os **seasteaders** (http://www.seasteading.org/), uma mistura de *geeks* com *hippies*, querem fundar sua própria nação em ilhas artificiais construídas em águas internacionais.

- http://revistapegn.globo.com/Revista/Common/0,,EMI327319-18478,00-GRUPO+DE+GEEKS+AMERICANOS+PLANEJAM+FUNDAR+COMUNIDADES+EM+ALTOMAR.html;
- http://motherboard.vice.com/blog/silicon-valleys-next-disruption-floating-autonomous-city-states.

Após esses exemplos de micronações, abaixo alguns links contendo explicações de **como qualquer pessoa pode fundar seu próprio país**:

- http://super.abril.com.br/historia/como-fundar-um-pais/;
- http://www.vice.com/pt_br/read/um-guia-pra-voce-fazer-um-pais;
- http://www.mortesubitainc.org/miscelania/textos-diversos/crie-seu-proprio-pais/guia-rapido-para-criar-seu-pais-em-11-passos-simples;
- http://editoramelhoramentos.com.br/v2/titulos/como-construir-seu-pais/;
- https://www.publico.pt/mundo/noticia/kevin-e-presidente-de-um-pais-fazdeconta-e-quer-ser-levado-a-serio-1704183;
- http://pt.wikihow.com/Criar-o-Seu-Próprio-País;
- http://desciclopedia.org/wiki/Deslivros:Criando_o_seu_próprio_país;
- https://www.skoob.com.br/como-construir-seu-pais-358729ed403125.html;
- http://veja.abril.com.br/entretenimento/como-comecar-seu-proprio-pais-investiga-micronacoes/.

Como fazer o seu próprio país usando Ethereum - Alex Van de Sande: http://www.humaritube.com/watch/6Yi57VcQ6Tg.

Confira um mapa mostrando todas as áreas do oceano que não pertencem a nenhum país em http://donutholes.ch/. São as **águas internacionais** ("donut holes"). Neste local poderia-se criar uma ilha artificial, alocar um navio sem bandeira, construir uma cidade submersa ou manter estacionado uma aeronave ou submarino de controle remoto para servir de servidor (computador hospedeiro). Por exemplo, algo como o veículo autônomo submarino FlatFish desenvolvido pela britânica BG Brasil com o SENAI Cimatec e a Empresa Brasileira de Pesquisa e Inovação Industrial (Embrapii). Ou, até mesmo, uma falsa bóia de sinalização ou falsa pilastra de plataforma abandonada para disfarçar suas antenas e placa solar que mandaria energia para o servidor escondido; bem como para facilitar sua localização para fins de proteção e manutenção.

A LOSS - *League of Secessionist States* ou Liga dos Estados Secessionistas (http://www.theloss.org/) é uma espécie de ONU das micronações, que consta com 40 membros. Em https://pt.wikipedia.org/wiki/Lista_de_micronações também há uma pequena lista. Já em https://pt.wikipedia.org/wiki/Lista_de_países_com_reconhecimento_limitado consta uma lista de países com reconhecimento limitado.

O Brasil possui dezenas de reservas indígenas, centenas de terras indígenas tradicionalmente ocupadas e algumas terras dominiais e áreas interditadas pela Funai (http://www.funai.gov.br/index.php/indios-no-brasil/terras-indigenas). Segundo alguns, pelo menos, 216 dessas áreas seriam completamente independentes e desligados do Governo do Brasil.

- https://pib.socioambiental.org/pt/c/terras-indigenas/demarcacoes/localizacao-e-extensao-das-tis.

As delimitações ou demarcações de fronteiras dos países é feita através de trabalho conjunto dos ministérios das relações exteriores dos países fronteiriços (Itamaraty). Os registros brasileiros constam em:

- http://scdl.itamaraty.gov.br/pt-br/historia.xml;
- http://scdl.itamaraty.gov.br/pt-br/fronteiras_da_scdl.xml;

- http://scdl.itamaraty.gov.br/pt-br/marcos_de_fronteira.xml;
- http://scdl.itamaraty.gov.br/pt-br/atas_de_conferencias.xml;
- http://scdl.itamaraty.gov.br/pt-br/centro_de_documentacao.xml.

Portanto, eventual descoberta de alguma falha na linha fronteiriça brasileira que acabe resultando em alguma área sem pertencer a algum país, só pode ser conseguida através do estudo e comparação dos limites reivindicados pelos países envolvidos através de geografo e engenheiro cartógrafo. Nada impede a remota possibilidade de alguma ilha marítima ou dentro de algum rio ter ficado de fora das reivindicações.

- "Fronteiras terrestres e marítimas do Brasil: um contorno dinâmico" - http://www.teses.usp.br/teses/disponiveis/8/8136/tde-03032008-112642/pt-br.php.

ESPÉCIES E TIPOS DE SOCIEDADES E DE ATIVIDADE EMPRESARIAL

O Brasil é o país com a maior taxa de juros; portanto, com o maior rendimento de aplicações bancárias. E, a tributação pelo governo e as tarifas bancárias para as pessoas jurídicas são mais brandas do que para as pessoas físicas. Além do que as pessoas jurídicas (ou simplesmente um CNPJ), possui certos privilégios, facilidades, serviços e linhas de créditos que não são disponíveis para as pessoas físicas (CPF). Portanto, urge estudar quais são as opções existentes para constituir uma pessoa jurídica ou, simplesmente, conseguir um CNPJ.

- http://exame.abril.com.br/economia/juros-brasileiros-continuam-sendo-os-mais-altos-do-planeta/.

A legislação brasileira permite uma grande variedade de formas que o indivíduo pode utilizar para exercer uma atividade econômica; infra elencamos algumas, expondo suas principais características e a respectiva base legal.

A grosso modo, uma **sociedade** é quando se celebra um contrato onde as pessoas (físicas e/ou jurídicas) envolvidas se comprometem, reciprocamente, a contribuir, com bens e/ou serviços, para o exercício da referida atividade econômica (comércio ou prestação de serviços) e a partilharem, entre si, os respectivos resultados.

Independentemente do tipo jurídico adotado, em regra, é necessário que haja ao menos dois sócios, que podem ser tanto pessoas naturais (físicas) e/ou jurídicas (coletivas), e que não precisam ser domiciliadas no Brasil.

No que tange à tributação de empresas, a legislação brasileira tradicionalmente utiliza como critério diferenciador, no estabelecimento de tributos e suas respectivas alíquotas, o porte da empresa, e não o tipo societário sob o qual ela se reveste, não sendo esse específico critério relevante para a adoção de determinado tipo societário. Assim, por exemplo, o Simples Nacional é um regime compartilhado de arrecadação, cobrança e fiscalização de tributos aplicável às Microempresas e Empresas de Pequeno Porte, previsto na Lei Complementar nº 123, de 14 de dezembro de 2006.

Entretanto, o MEI (http://www.portaldoempreendedor.gov.br/) é o regime tributário com menor oneração. Depois dele é que está o simples nacional acima dos tradicionais regimes de tributação através do lucro presumido (Decreto 3.000/1999, artigos 516 a 528; Lei 8.981/1995, artigo 45; Lei 9.430/1996, artigo 26; 9.718/1998, artigo 13, § 1°; e, Lei 12.814/2013) e do lucro real (Lei 9.718/1998, artigo 14; Decreto-lei 1.598/1977, artigo 6º; Lei 8.981/1995, artigo 37, § 1º; e, Decreto 3.000/1999, artigos 246 a 515).

- Portal do Simples Nacional - http://www8.receita.fazenda.gov.br/SimplesNacional/.

Confira a ferramenta de comparação de carga tributária (passagem do SIMPLES para o Lucro Presumido) em http://www.fgv.br/fgvtec/_app/index.aspx.

Sociedade não personificada é aquela que não inscreve seus atos constitutivos no competente registro, provando as relações entre os sócios e com terceiros somente por escrito. A mais comum é a sociedade em conta de participação. Caracteriza-se como uma sociedade "anônima", pois apresenta duas categorias de sócios: 1) ocultos, que não aparecem e nem tratam com terceiros; e, 2) ostensivos, girando os negócios sob a firma individual. Não exige formalidades registradas, como contrato e arquivamento no registro mercantil ou civil.

No ordenamento jurídico brasileiro são previstas duas espécies de sociedades: a sociedade simples e a sociedade empresária (anteriormente denominada sociedade comercial).

A empresa ou o empreendimento como ente econômico, pode ser explorado por uma pessoa física (empresário individual) ou pessoa jurídica (sociedade empresária legalmente registrada). Como sociedade empresária, pessoa jurídica é a sociedade constituída de sócios e legalmente registrada no órgão competente, para explorar atividades de empresa, constituída na sua grande maioria no Brasil como sociedade limitada ou sociedade anônima (companhia).

O estatuto social (utilizado pelas sociedades em ações e entidades sem fins lucrativos; Código Civil, artigo 54) e o contrato social (utilizado pelas

demais sociedades; Código Civil, artigo 997), são as certidões de nascimento da pessoa jurídica.

- http://www.institucional.jucesp.sp.gov.br/empresas_jucesp-orienta.php;
- Código Civil: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

Nos Estados Unidos os documentos equivalentes ao Contrato Social são: *Articles of Incorporation*, *Articles of Organization* e *By-law* (ou *Bylaw*).

A **sociedade simples** versa sobre parcerias entre profissionais prestadores de serviços, onde eles mesmos exercem a atividade para a qual a sociedade existe. Esse tipo de sociedade, portanto, explora prioritariamente atividades de prestação de serviços de natureza notadamente intelectual e/ou cooperativa; ou seja, não corresponde a atividades mercantis e, assim, não possui personalidade jurídica. A sociedade simples é o único tipo societário que admite o sócio de indústria; que é aquele que não contribui com dinheiro para o capital social da sociedade, mas contribui com o seu trabalho. Apesar da restrição constante do Código Civil, artigo 977, há quem sustente que a sociedade simples permita, na mesma sociedade, sócios que sejam casados, entre si, ainda que pelo regime da comunhão universal de bens ou pelo regime da separação obrigatória. Não está sujeita, para efeito de tomada de decisões sociais, à realização de reuniões e, muito menos, ao formalismo das assembleias como ocorre na sociedade limitada, particularmente quando esta for composta por mais de 10 (dez) sócios, com todas as suas regras de convocação e quóruns de instalação e deliberação. Por via de consequência, a sociedade simples pura não está obrigada a manter livros de atas de reuniões ou assembleias, indispensáveis para a sociedade limitada (Código Civil, artigos 1.062, 1.067 e 1.075). Sua contabilidade é mais simplificada, não estando obrigada, como acontece com a limitada, a um sistema de escrituração contábil contendo regras bastante estritas (Código Civil, artigos 1.179 a 1.195), que ensejam ônus. A responsabilidade dos sócios pode ser limitada ou ilimitada, dependendo do que declararem no contrato social. A sociedade simples não se submete ao regime jurídico empresarial pois é entendida como uma sociedade não-empresária; por essa razão não usufrui dos benefícios concedidos às sociedades empresárias como, por exemplo, o regime de falência e recuperação judicial. As sociedades não empresárias

podem constituir-se por vários tipos societários, inclusive aqueles estipulados para as sociedades empresárias; excluindo-se as sociedades por ações (sociedade anônima ou sociedade em comandita por ações) por serem exclusivos e caracterizadores de empresa (Código Civil, artigo 982 e parágrafo único) e a sociedade de propósito específico. E, síntese, a sociedade simples poderá ser constituída sob quatro formas específicas: 1) Sociedade Simples (em sentido estrito ou comum); 2) Sociedade em nome Coletivo; 3) Sociedade em Comandita simples; e, 4) Sociedade Limitada. Existem 3 tipos de sociedades que somente poderão ser caracterizadas como Simples: 1) Consórcio; 2) Sociedades em Conta de Participação; e, 3) Sociedade Cooperativa. A sociedade simples nunca poderá consistir numa sociedade anônima.

- Código Civil: Lei 10.406 de 2002 - http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

Sociedade empresarial é a sociedade entre um ou mais sócios, constituída para um fim comercial (atividades mercantis, atos de comércio ou atividade típica de empresário: produção e/ou circulação de bens e serviços), registrada na Junta Comercial de seu respectivo Estado (Código Civil, artigos 967 e 968) e, portanto, com personalidade jurídica. Por outro lado, não serão consideradas empresárias aquelas que não apresentem elevado grau de complexidade organizacional, bem como as que se dedicarem a atividades intelectuais, de natureza científica, literária ou artística, salvo se tais atividades constituírem elemento de empresa. A constituição de uma sociedade empresária deve atender ao disposto nos artigos 1.039 a 1.092 do Código Civil. De acordo com o Código Civil, existem 7 tipos principais de sociedades empresariais: 1) Sociedade em Nome Coletivo; 2) Sociedade em Comandita Simples; 3) Sociedade Limitada; 4) Sociedade Anônima; 5) Sociedade em Comandita por Ações; 6) Sociedade Individual de Responsabilidade Limitada; e, 7) Sociedade de Propósito Específico. As sociedades que não explorarem atividades de cunho empresarial serão consideradas sociedades simples.

- http://www.institucional.jucesp.sp.gov.br/empresas_manuais.php;
- http://www.sevilha.com.br/abrir/abrir.pdf.

Empresário (Código Civil, artigo 966) é quem exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços. Assim a atividade deve ser habitual, pessoal e com efetiva contratação de empregados. É vinculado a cargo das Juntas Comerciais.

O **Micro Empresário Individual (MEI)** é uma opção para o empresário que exerce a atividade de forma individual, com uma receita bruta de até R$ 5.000,00 no mês ou R$ 60.000,00 no ano. Caso ultrapasse estes valores, passará a constituir o Empresário Individual. O MEI é uma estrutura jurídica mais simples para abertura de uma empresa. Conta apenas de um certificado de condição de microempreendedor; sendo-lhe inaplicável qualquer tipo de contrato ou estatuto social. Também inadmite sócios porque a atividade empresarial está concentrada na figura do microempreendedor e este empresário não possui limitação de sua responsabilidade; ou seja, as obrigações assumidas pelo MEI são obrigações assumidas pela própria pessoa física. Portanto se o MEI (CNPJ) não tiver bens suficientes para responder por suas obrigações financeiras, os bens da pessoa física (CPF) deverão responder pelas dívidas.

- http://www.portaldoempreendedor.gov.br/.

Empresário individual (Código Civil, artigos 966 a 980). O empresário individual é aquele que exerce pessoalmente atividade empresarial e deve ser registrado na Junta Comercial mediante Ficha de Registro de Empresário Individual. A responsabilidade do seu titular se confunde com a da empresa. Seu nome precisa ser o nome do Empresário, podendo conter abreviações, indicando ainda a atividade que irá exercer.

Empresário individual de responsabilidade limitada - Eireli (Código Civil, artigo 980-A). Muito semelhante ao empresário individual, também é registrado na Junta Comercial, mas sob a forma de um pequeno contrato e deve ter o capital social igual ou superior a 100 salários mínimos. Seu nome pode ser escolhido livremente, mas deve indicar a atividade que será exercida e terminar com a expressão “Eireli”. Assim como o MEI essa estrutura é formada apenas pela figura do empresário (pessoa física), com o detalhe de que existe a separação do patrimônio do empresário e o patrimônio da empresa, o que confere a característica de responsabilidade

limitada. O capital social deverá ser de, no mínimo, 100 (cem) vezes o maior salário-mínimo vigente no país.

Sociedade simples (Código Civil, artigos 997 a 1.038). Divide-se em sociedade simples pura, onde o patrimônio pessoal dos sócios pode ser comprometido pelas dívidas contraídas pela empresa, ou poderá ser uma sociedade simples empresária (geralmente limitada), onde o patrimônio do sócio permanece protegido. Caso trate-se de uma sociedade simples pura, seu registro deverá ser feito no Registro Civil de Pessoas Jurídicas. O documento hábil para registro é o contrato social (Código Civil, artigo 997), seu nome pode ser escolhido livremente, sendo sociedade simples, não precisa constar prefixo ou sufixo, mas deve indicar qual a atividade exercida pela sociedade. No caso da sociedade simples limitada seu registro deve ser feito na Junta Comercial. Seu nome pode ser escolhido com razoável liberdade, vez que apenas deverá acrescentar ao final do nome a insígnia "LTDA", devendo ainda o nome indicar a atividade exercida pela sociedade. Aplicam-se, ainda, à sociedade limita os artigos do Código Civil referentes a sociedade empresária limitada (artigos 1.052 a 1.087). Em ambos os casos o capital da empresa divide-se por quotas. A sociedade simples, em comparação à empresária, tem como principais características: a) simplicidade de estrutura; b) presunção de pequeno porte; e, c) atuação pessoal dos sócios superando a organização dos fatores de produção.

Sociedade em nome coletivo (Código Civil, artigos 1.039 a 1044). Somente pessoas físicas podem se associar e respondem, solidária e ilimitadamente, pelas obrigações sociais. Mesmo sendo sociedade, os patrimônios dos sócios não são protegidos, perdendo uma das principais vantagens de ter sócio(s). Seu nome necessariamente deve ser o de um dos sócios, acompanhado da expressão "Cia.", ou pelo nome de todos os sócios, podendo conter abreviações, seguido da mesma expressão. Esta sociedade geralmente é formada por familiares e constitui-se mediante contrato registrado na Junta Comercial.

Sociedade em comandita simples (Código Civil, artigos 1.045 a 1.051). Formada por sócios comanditados, com responsabilidade solidária e ilimitada, e comanditários, com responsabilidade limitada. Conta, portanto, com dois tipos de sócios, os comanditários (que apenas investem recursos na

empresa) e os comanditados (que são os que efetivamente irão operar a empresa). Os primeiros terão sua responsabilidade limitada ao valor investido, deixando assim seu patrimônio seguro. Já os segundos poderão responder com seu patrimônio pessoal por dívidas da empresa. Seu nome, necessariamente será o nome do(s) sócio(s) comanditado(s) seguidos da expressão "Cia". Se em qualquer momento o sócio investidor exercer gerência ou tiver o nome envolvido diretamente nas atividades da empresa, perderá a proteção do seu patrimônio. É uma sociedade contratual e deve ser registrada na Junta Comercial.

Sociedade empresária limitada ou por cotas de responsabilidade limitada (Código Civil, artigos 1.052 a 1.087). Enquanto o capital social não estiver integralizado, todos os sócios respondem solidariamente pela integralização do capital social. Uma vez integralizado o capital, a responsabilidade fica limitada ao montante correspondente ao valor das quotas de cada sócio. Em resumo, responde o sócio pelo valor do capital subscrito somente, mas todos respondem solidariamente pela integralização do capital social. Os sócios, portanto, não responderam pelas dívidas da empresa com o seu patrimônio pessoal; exceto no caso de simulação, fraude, má-fé, etc. O nome pode ser escolhido livremente, mas necessariamente ao seu final deverá conter a expressão Ltda., e deve indicar a atividade realizada pela sociedade também. É constituída por Contrato Social e deve ser registrada na Junta Comercial. É a sociedade mais utilizada no Brasil, pela simplicidade de se operar e pela proteção do patrimônio de ambos os sócios. Seu capital social divide-se em quotas. A sociedade limitada e a sociedade anônima são tipos societários em que a responsabilidade dos sócios é restrita ao valor que despenderam para pagamento do preço de integralização, conforme o caso, de suas quotas ou ações, sem que, em princípio, seus sócios sejam responsáveis; exceto em caso de prática de atos ilícitos, por qualquer quantia além daquela desembolsada para compor o capital social da empresa. A Limitada não precisa publicar suas contas, alterações contratuais ou outros atos constitutivos, exceto no caso de redução de capital, incorporação, cisão ou fusão. Os administradores da limitada não precisam ser brasileiros, mas devem necessariamente ser residentes e domiciliados no Brasil. Em geral, a adoção da sociedade limitada implica maior economia (procedimento mais simples e menos oneroso do que constituir uma S.A. e pode facilmente se transformar numa S.A.) e um certo

grau de sigilo com relação aos negócios da sociedade. Entretanto, o contrato social é público, podendo ser consultado por terceiros.

Sociedade anônima, sociedade por ações ou companhia (Código Civil, artigos 1.088 e 1.089 e Lei nº 6.404/1976). A sociedade anônima possui legislação especial (Lei n.º 6.404/1976) que regula sua constituição, funcionamento e expressa detalhadamente as características deste ripo societário; somente nos casos omissos serão aplicadas às disposições do Código Civil. Por esta razão o Código Civil não cuida de suas particularidades. A formação da sociedade anônima se dá por meio de um estatuto (Lei 6.404/1964, artigos 80 e 81), que requer maiores formalidades que um contrato social. Seus pedaços não são quotas, mas sim ações. O patrimônio de nenhum dos sócios (acionistas) será prejudicado por dívidas contraídas pela empresa. O capital divide-se em ações, obrigando-se cada sócio ou acionista somente pelo preço de emissão das ações que subscrever ou adquirir. Esta sociedade pode ter qualquer nome, desde que precedido pela expressão "Cia." ou finalizado pela expressão "S/A". Seu capital social divide-se em ações. Recomenda-se apenas para empresas de grande porte. As sociedades anônimas (incluindo as sociedades em comandita por ações), independente do seu objeto, serão sempre consideradas sociedades empresárias. As Sociedades Anônimas podem ser abertas ou fechadas conforme seus valores sejam, ou não, admitidos à negociação no mercado de valores mobiliários. Ambas serão constituídas por estatuto, registrado na Junta Comercial. Compete à Comissão de Valores Mobiliários (CVM) a fiscalização e normatização do mercado de valores mobiliários. Em sociedades que devam deliberar sob a forma de Assembleia, esta será de realização obrigatória ao menos uma vez por ano, no decorrer dos quatro meses subsequentes ao término do exercício social. O objetivo desta Assembleia anual de sócios é tomar as contas dos administradores, deliberar sobre o balanço patrimonial e o de resultado econômico da empresa, eventualmente designar administradores, e tratar de outros assuntos de interesse da sociedade. Exige-se a publicação de edital de convocação para a Assembleia Geral em órgão oficial de imprensa e em jornal de grande circulação, por pelo menos três vezes (Lei 6.404/1964, artigo 124); o que gera custos consideráveis para a empresa a cada convocação (Lei 6.404/1964, artigo 283). Porém, as formalidades de convocação referentes a Assembleias de sócios são dispensáveis, sempre que a totalidade dos sócios

comparecer à Assembleia, ou se declarar, por escrito, ciente dos respectivos local, data, hora e ordem do dia. A realização de reunião ou assembleia de sócios, ainda, poderá ser dispensada sempre que todos os sócios decidirem, por escrito, sobre os assuntos que, de outro modo, seriam objeto de deliberação por reunião ou assembleia. A Sociedade Anônima possibilita a elaboração de acordos de acionistas, emissão de debêntures (forma de financiamento por meio de emissão de títulos de dívida da empresa), abertura de capital ao mercado financeiro, oferece uma estrutura de governança mais robusta (a administração da companhia pode ser composta por uma Diretoria e um Conselho de Administração), existe previsão legal que obriga a distribuição de dividendos mínimos obrigatórios, dentre outras regras aplicáveis a este tipo societário. Para se tornar companhia aberta a empresa deve estar constituída na forma jurídica de uma sociedade anônima. A distribuição pública de valores mobiliários pressupõe prévio registro na CVM (Comissão de Valores Mobiliários), a ser solicitado pela companhia emissora. No caso de empresas abrindo capital, além do Registro de Emissão Pública, é exigido o Registro de Companhia Aberta para negociação em Bolsa ou no Mercado de Balcão Organizado. No processo de aumento do capital social, as etapas fundamentais estão discriminadas nas Instruções CVM 13/1980 e 202/1993, que dispõem respectivamente sobre o registro de distribuição pública de ações e sobre o registro de companhia para negociação de seus valores mobiliários em Bolsa de Valores ou no Mercado de Balcão. As informações solicitadas para fins de registro da emissão compõem o Prospecto; documento básico de divulgação sobre a emissão e a companhia (artigos 18 a 22 da Instrução CVM 13/1980). É permitida, durante o processo de registro, a circulação de um Prospecto Preliminar entre os intermediários financeiros. Ao final do processo, o Prospecto definitivo deve estar à disposição dos investidores potenciais.

- Lei 6.404/1976: Lei das Sociedades por Ações - http://www.planalto.gov.br/ccivil_03/leis/L6404compilada.htm;
- "Como abrir o capital da sua empresa no Brasil - http://www.bmfbovespa.com.br/lumis/portal/file/fileDownload.jsp?fileId=8A828D294F270E45014F709C2F7A2821.

Sociedade em comandita por ações (Código Civil, artigos 1.090 a 1.092 e Lei 6.404/1976). Tal como na sociedade em comandita simples, tem os sócios (acionistas) administradores, que podem responder com o seu

patrimônio pessoal sobre as dívidas contraídas pela empresa, e os sócios (acionistas) investidores, que respondem apenas de acordo com o valor investido. Por outras palavras, o capital é dividido em ações, respondendo os sócios ou acionistas, tão-somente pelo preço das ações subscritas ou adquiridas, com responsabilidade subsidiária, solidária e ilimitada dos diretores ou gerentes pelas obrigações sociais. Seu nome poderá ser escolhido livremente, seguido da expressão “em comandita por ações” ou conter necessariamente o(s) nome(s) do(s) sócio(s) administradore(s). É constituída por estatuto e deve ser registrada na Junta Comercial.

Sociedade cooperativa (Código Civil, artigos 1.093 a 1.096 e Lei 5.764/1971). Celebram contrato de sociedade cooperativa as pessoas que reciprocamente se obrigam a contribuir com bens ou serviços para o exercício de uma atividade econômica, de proveito comum, sem objetivo de lucro. Portanto, as cooperativas são sociedades de pessoas, com forma e natureza jurídica próprias, de natureza civil, não sujeitas a falência, constituídas para prestar serviços aos associados, distinguindo-se das demais sociedades e possuindo características peculiares (artigos 3º e 4º da Lei n.º 5.774/1971). Esta sociedade não possui sócios, e sim cooperativados, que podem ter o seu patrimônio comprometido, ou não, pelas obrigações da cooperativa. Seu nome poderá ser escolhido livremente, sem depender de prefixos ou sufixos e deverá ser registrado no Registro Civil de Pessoas Jurídicas, podendo ser um contrato ou estatuto. Pode adotar por objeto qualquer gênero de serviço, operação ou atividade; mas, independentemente de seu objeto, serão sempre consideradas sociedades simples (nunca poderá ser uma sociedade empresária).

- Lei 5.764/1971: Lei das Cooperativas - http://www.planalto.gov.br/ccivil_03/leis/L5764.htm.

Sociedade de propósito específico - SPE (Lei 11.079/2004). Trata-se da sociedade criada para atender a um negócio específico e isolar um ativo das demais atividades realizadas por uma empresa, sendo geralmente utilizado o tipo societário da limitada ou sociedade anônima para este fim. Por outras palavras, é usada para evitar vínculos diretos visando a imunidade de quaisquer problemas com a atividade específica.

- Lei nº 11.079/2004 - http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l11079.htm.

Sociedade em conta de participação (Código Civil, artigos 991 a 996). Não se trata de uma sociedade empresária, nem mesmo de uma pessoa jurídica, pois é uma sociedade não personificada. Não tem razão social e nem o contrato social registrado, mas um contrato de "gaveta" (particular). Sendo uma sociedade despersonalizada e secreta, não pode ter firma ou denominação (Código Civil, artigo 1.162). Chama-se em conta de participação porque é aberta uma conta para indicar as operações realizadas e os resultados. A participação será a divisão dos lucros entre os sócios. Possui características excepcionais próprias, seja por sua despersonalização, seja por seu caráter de sociedade secreta. Não está sujeita à falência ou recuperação judicial (antiga concordata). O sócio ostensivo é o aparente, que comercia e se obriga perante terceiros; já o sócio oculto, é anônimo e desconhecido. A atividade constitutiva do objeto social é exercida unicamente pelo sócio ostensivo, em seu nome individual e sob sua própria e exclusiva responsabilidade, participando os demais dos resultados correspondentes. A responsabilidade, portanto, é apenas do sócio ostensivo. Obriga-se perante terceiro tão-somente o sócio ostensivo. O sócio participante ou oculto obriga-se exclusivamente perante o ostensivo, nos termos do contrato social; que produz efeitos somente entre os sócios e eventual inscrição de seu instrumento em qualquer registro (por ser uma sociedade secreta não pode ser registrado) não confere personalidade jurídica à sociedade. Nada impede, por conseguinte, o registro do ato constitutivo da sociedade no Registro de Títulos e Documentos, para melhor resguardo dos interesses dos contratantes (não afetando em nada terceiros). A falência do sócio ostensivo acarreta a liquidação da sociedade; já falindo o participante, os direitos decorrentes do contrato de sociedade podem integrar o espólio (bens do falecido).

A sociedade ***holding*** não representa um tipo societário diverso daqueles que estão previstos no sistema jurídico brasileiro (sociedade limitada, sociedade anônima, sociedade simples, etc.). Em outras palavras, a *holding* não é um modelo societário diferente; mas, sim uma sociedade com objetivos específicos. Aliás, não se pode deixar de advertir que, com a regulamentação da Empresa Individual de Responsabilidade Limitada

(Eireli), essa também pode assumir, dentro de um contexto empresarial ou familiar, a condição de *holding*.

- http://biblioteca.fbtedu.com.br/fiscais-holdings-empresasoffshore.

Holdings são sociedades não operacionais, que têm seu patrimônio composto de ações de outras companhias. São constituídas para o exercício do poder de controle ou para a participação relevante em outras companhias, visando nesse caso, constituir a coligação.

A *holding* pode possuir vários formatos, senão vejamos:

- ***Holding* pura ou de participações** é aquela que participa de outras sociedades, como cotista ou acionista, tendo como objetivo a detenção de bens, que podem ser não apenas participações em outras sociedades; mas, também, imóveis e outros bens e direitos. Basicamente, o que a *holding* pura faz é repassar aos seus acionistas os dividendos e os juros sobre o capital próprio recebido de suas controladas, após as deduções das despesas próprias da *holding*. Por outras palavras, diz pura porque o seu objeto social restringe-se, apenas, a participação no capital de outras empresas;

- ***Holding* mista** é a que possui atividades secundárias, caracterizando-se pela integralização de bens imóveis ou móveis dos quotistas ou acionistas, fundadores no capital social da pessoa jurídica. Em suma, é mista porque, além da participação no capital de outras empresas, ela exerce a exploração de alguma outra atividade empresarial;

- ***Holding* patrimonial** é uma sociedade que mantém a titularidade de bens e direitos, compreendendo bens móveis, imóveis e propriedade industrial (marcas e patentes) que admita participações em uma ou mais sociedades. A *holding* patrimonial poderá ser constituída sob a forma de sociedade simples ou de sociedade empresária, sendo, no Brasil, são mais comuns e

utilizadas sob a forma de sociedades anônimas e sociedades de responsabilidade limitada;

- ***Holding* familiar** é utilizada pelo empresariado para substituir a propriedade e controle das empresas e bens pessoais do grupo familiar visando a blindagem patrimonial e a minimização de problemas cotidianos, como conflitos familiares, separações, falecimentos, etc. Portanto, objetiva a concentração e proteção do patrimônio familiar através de pessoa jurídica para facilitar a gestão dos ativos com maiores benefícios fiscais (diminuição de impostos federais, imposto de transmissão "causa mortis", etc.) e a proteção patrimonial em diversos casos. Desse modo, uma ou mais pessoas físicas, ao invés de terem patrimônio (bens, propriedades, empresas, investimentos, aplicações, ações, direitos, etc.) em seus próprios nomes, transferem tudo para uma pessoa jurídica, geralmente constituída na forma de uma sociedade limitada e, via de regra, contendo na sua denominação social a palavra empreendimentos, participações ou comercial Ltda., que irá administrar referido patrimônio com menos despesas, encargos e tributos e, ainda, será beneficiada de várias proteções legais contra a dilapidação.

Os **principais objetivos da *holding*** são a "blindagem" do patrimônio, planejamento sucessório e tributário e a contribuição de todos para manutenção da estabilidade financeira e da harmonia familiar (*affectio societatis*). Na *holding* familiar é possível que genitores (doadores ou instituidores) confiram todo o patrimônio pessoal à sociedade, podendo ocorrer a doação das quotas ou ações em favor dos sucessores (filhos) com reserva de usufruto, que elimina a necessidade de inventário ou partilha. Desse modo, quando os pais conferem todo o patrimônio à *holding* familiar, pode ocorrer a doação das quotas ou ações em favor dos sucessores com reserva de usufruto, que elimina a necessidade de inventário ou partilha.

Conforme visto alhures, no ordenamento jurídico brasileiro são previstas duas espécies de sociedade (tipos societários): a sociedade simples e a sociedade empresária. A *holding* patrimonial poderá ser constituída sob

qualquer um deles; todavia, os mais comuns e utilizados no Brasil são as Sociedades Anônimas e as Sociedades de Responsabilidade Limitada.

A sociedade limitada é o tipo societário mais indicado para uma *holding* porque demanda um menor custo para sua constituição e fica dispensada das publicações exigidas nas Sociedades Anônimas e, também, por possuir características de uma sociedade de pessoas, proporciona uma maior proteção ao grupo familiar contra o ingresso de terceiros ao quadro societário. Essa blindagem é caracterizada e representada pelo princípio do *affectio societatis* (sociedade de afeição) que estará expressamente descrito no seu ato constitutivo.

Affectio Societatis significa confiança mútua e vontade de cooperação conjunta a fim de obter determinados benefícios; ou seja, é a união dos sócios para que possa ser alcançado o resultado desejado e, ainda, com os diferenciais de harmonia de vontades e trabalhos somados ao desejo de permanecerem juntos na sociedade.

Para constituição de uma *holding*, seus sócios, que podem ser pessoas físicas e/ou jurídicas (outras empresas), terão que formar o capital social com a integralização de bens ou direitos de sua propriedade, mediante a elaboração de contrato ou estatuto social (conforme a espécie de sociedade) contendo as informações obrigatórias trazidas pela lei e o registro deste no órgão competente (Junta Comercial).

Se a *holding* adotar a forma de sociedade simples, não estará sujeita à falência.

A doação de quotas com reserva de usufruto é o mecanismo que determinará a divisão do patrimônio entre os herdeiros (Código Civil, artigos 1.829 a 1.844) e por consequência conforme as cláusulas de restrições, não permitirá a dilapidação do patrimônio a curto e médio prazo.

Os bens que integralizarão o capital social da *holding* podem ser conferidos pelos valores constantes da declaração de bens do Imposto de Renda ou pelo valor do mercado. Se fizer por valor superior ao da declaração de bens do imposto de renda, a diferença apontada será tributada

pelo imposto de renda da pessoa física, nos termos da Lei nº 9.249/1995, como ganho de capital.

- Lei nº 9.249/1995 - http://www.planalto.gov.br/ccivil_03/leis/L9249.htm.

O doador ou instituidor (normalmente patriarca e/ou matriarca) após a doação das quotas irá se instituir na sociedade como usufrutuário e administrador, permanecendo até a sua morte no total controle do patrimônio pertencente a *holding* patrimonial. Todo ato que envolva a sociedade constituída necessitará obrigatoriamente de sua anuência, sendo inválido qualquer ato praticado pelos herdeiros (normalmente filhos) sem sua autorização. Antes da ocorrência da sua morte é como se nenhuma doação estivesse ocorrida, visto que o patriarca efetuou, tão somente, a doção da nua-propriedade das quotas.

Os administradores da *holding* terão direito a uma retirada mensal a título de "pró-labore" (uma remuneração específica para os administradores). Se o sócio não for administrador receberá tão somente os dividendos (não receberá "pró-labore"). A quantia retirada de "pró-labore" não deve ser elevada, visto que incidirá sobre esses rendimentos o recolhimento de INSS (Instituto Nacional do Seguro Social ou Previdência Social) e Imposto de Renda.

Com a constituição de uma sociedade empresária todo o patrimônio da pessoa física (doador ou instituidor) ou do casal de patriarcas é integralizado no capital social da *holding*. Com isso, o patrimônio que antes era pessoal, ao se tornar da pessoa jurídica, ficará seguro em face das inúmeras situações de responsabilidade por parte de seus sócios, seja de problemas pessoais, seja sobre eventuais outras empresas das quais porventura participem, que possam acabar por provocar medidas como arresto, sequestro ou penhora de bens, busca e apreensão, etc. Com os bens integralizados na pessoa jurídica, portanto, há uma maior proteção do patrimônio familiar. Na presença da *holding*, o que se torna passível de penhora são os frutos e rendimentos que as quotas ou ações irão produzir, ou as próprias quotas ou ações, conforme preceitua o Código Civil (http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm), nos seus artigos 1.026 e 1.031. O CPC - Código de Processo Civil

(http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm), no artigo 861 versa sobre penhora de quotas, no 866 trata da penhora de percentual de faturamento da empresa e, no artigo 867, fala sobre a penhora de frutos (rendimentos) de móvel ou imóvel. Enfim, a constituição de uma *holding* visa propiciar a divisão do patrimônio ainda em vida, evitando a dilapidação após morte dos patriarcas, reduzindo os custos tributários e os desgastes que o processo de inventário causaria ao grupo familiar.

Além do usufruto ainda é possível aos doadores inserirem, no mesmo ato, clausulas de proteção como de inalienabilidade, incomunicabilidade, impenhorabilidade e reversão. O CPC, no artigo 833, inciso I, prescreve que são impenhoráveis os bens inalienáveis e os declarados, por ato voluntário, não sujeitos à execução. Já o Código Civil no artigo 1.911 reza que: "A cláusula de inalienabilidade, imposta aos bens por ato de liberalidade, implica impenhorabilidade e incomunicabilidade".

A cláusula de inalienabilidade tem a função primordial de instituir sobre as quotas doadas uma vedação aos herdeiros; pois ficarão impedidos de alienar as quotas recebidas. Esse gravame sobre as quotas não permite a dilapidação do patrimônio da sociedade após a morte do doador ou instituidor (normalmente patriarca e/ou matriarca), porquanto a cláusula de inalienabilidade das quotas pode ser instituída de maneira vitalícia. Constando a cláusula de inalienabilidade no contrato social, automaticamente o patriarca estará gravando as quotas também com incomunicabilidade e impenhorabilidade.

O gravame da incomunicabilidade é caracterizado por proteger as quotas doadas de futuros casamentos; vez que gravadas com incomunicabilidade as quotas recebidas pelos herdeiros (normalmente filhos) serão exclusivamente de sua propriedade, não se comunicando em um futuro divórcio, mesmo que o herdeiro seja casado sob o regime da comunhão universal de bens. O Código Civil, no artigo 1.668, inciso I, reza que são excluídos da comunhão os bens doados ou herdados com a cláusula de incomunicabilidade e os sub-rogados em seu lugar. No planejamento sucessório através da constituição de uma *holding*, portanto, o patrimônio da empresa será incomunicável com o cônjuge do sócio donatário independentemente do regime de casamento

pactuado. Em resumo, a incomunicabilidade objetiva impedir dos bens e/ou direitos doados se comuniquem com o cônjuge ou o convivente do donatário.

Já a cláusula de impenhorabilidade tem como maior escopo proteger as quotas da sociedade de futuros processos em que os sócios (ou herdeiros), ou a própria sociedade, venha a ser devedora ou executada, protegendo desta maneira a penhorabilidade das quotas. Em suma, os bens e/ou direitos doados não poderão ser penhorados por dívidas dos donatários e nem da própria *holding*. Entretanto, os lucros e dividendos recebidos pelos herdeiros não são protegidos e, assim, poderão ser objetos de penhora sem nenhuma objeção (Código Civil, artigos 1.026 e 1.031 e, CPC, artigos 835 – X, 866 e 905).

Por fim a cláusula de reversão visa, em caso de ocorrer a morte de um dos herdeiros antes do patriarca, que as quotas pertencentes ao herdeiro falecido retornem a ser de propriedade do doador sem nenhum ônus (Código Civil, artigo 547); salvo se renunciar a tal direito em favor dos herdeiros do falecido (normalmente netos do doador ou instituidor).

A constituição de uma EIRELI será extremamente útil e poderá ser utilizada como uma *holding* quando o detentor do patrimônio não possuir herdeiros ou não possuir interesse na elaboração de um planejamento sucessório, desejando somente os benefícios tributários decorrente da constituição de uma empresa administradora de bens imóveis próprios. Desse modo, o proprietário dos imóveis integralizará seu patrimônio no capital da pessoa jurídica constituída, sendo o titular dessa EIRELI e tendo o total controle e gestão sobre a empresa.

De qualquer forma, é necessária a correta atribuição do código CNAE (Classificação Nacional de Atividades Econômicas) para não ocorrer erros de tributação.

- http://www.cnae.ibge.gov.br/;
- http://cnae-simples.net/;
- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/classificacao-nacional-de-atividades-economicas-2013-cnae.

Assim, por exemplo, a *holding* constituída com o escopo de gerenciar o patrimônio imobiliário de determinado grupo familiar e promover o planejamento sucessório deverá ter como objetos sociais:

- 6810-2/01: COMPRA E VENDA DE IMÓVEIS PRÓPRIOS;
- 6810-2/02: ALUGUÉIS DE IMÓVEIS PRÓPRIOS, RESIDENCIAIS E NÃO RESIDENCIAIS.

Porém, existem outras atividades a serem consideradas, tais como, por exemplos:

- 7490-1/04: ATIVIDADES DE INTERMEDIAÇÃO E AGENCIAMENTO DE SERVIÇOS E NEGÓCIOS EM GERAL, SEM ESPECIALIZAÇÃO DEFINIDA;
- 6499-9/01: CLUBE DE INVESTIMENTO; EMPRESA DE;
- 6499-9/01: CLUBES DE INVESTIMENTO.

De acordo com o Código Civil, artigo 977, é expressamente vedado aos cônjuges casados sob o regime da comunhão universal de bens e no da separação obrigatória contratarem sociedade entre si. Logo, os cônjuges casados sob um desses regimes não poderão figurar no quadro societário da *holding*. Sendo assim, cabe explicitar ao final do planejamento sucessório somente os herdeiros deverão compor o quadro societário da *holding*, ficando o(s) doador(es) ou instituidor(es) (normalmente patriarca e/ou matriarca) somente como usufrutuário(s) e administrador(es), tendo deste modo o total controle sobre a sociedade.

Os herdeiros (ou sócios) menores de idade poderão figurar como sócios da *holding* sem nenhum óbice perante a legislação societária. Todavia deverão ser devidamente representados ou assistidos por ambos os pais no contrato social de constituição. Caso possuam até 16 (dezesseis) anos deverão ser devidamente representados. Já no caso de possuírem entre 16 (dezesseis) e 18 (dezoito) anos deverão ser devidamente assistidos.

A autorização do cônjuge no planejamento sucessório é exercida através da outorga uxória, caso o patrimônio seja integralizado pelo patriarca, ou da outorga marital caso o patrimônio seja integralizado pela matriarca. A

cláusula da outorga é essencial para a validade do ato, devendo estar expressamente no contrato, com a devida assinatura do(a) outorgante ao final do contrato. A autorização do cônjuge se dará no momento da integralização do capital social, permitindo a transferência do patrimônio para a pessoa jurídica, e também será inerente a outorga na alteração contratual, no momento da doação de quotas para os herdeiros (ou sócios).

O capital social da *holding* será composto mediante integralização de bens imóveis pertencentes ao doador ou instituidor (normalmente patriarca e/ou matriarca). A propriedade dos imóveis será transferida para a sociedade no momento da constituição da empresa. Os bens móveis, como automóveis, por exemplo, não são recomendados para a integralização, pois essa categoria de bens possui uma elevada taxa de depreciação e risco de envolvimento em acidentes ensejando a responsabilidade civil (dever de indenização por parte da *holding*).

Após o arquivamento perante a Junta Comercial o contrato social deverá ser levado, juntamente com a guia de isenção ou recolhimento do ITBI (Imposto de Transmissão de Bens Imóveis) perante os Cartórios de Registro de Imóveis competentes para ser promovida a averbação transmitindo a titularidade dos bens imóveis para a sociedade.

Conforme a regra do artigo 156, § 2º, inciso I, da Constituição Federal, o ITBI (Imposto sobre a Transmissão de Bens Imóveis) não terá a incidência nas hipóteses de integralização de capital social; salvo quando a atividade preponderante desses bens seja a compra e venda e a locação.

Nesse momento a regra aplicável a situação é a prevista na Lei n.º 8.934/1994, artigo 64, sendo o próprio contrato social documento hábil para efetuar o registro: “A certidão dos atos de constituição e de alteração de sociedades mercantis, passada pelas juntas comerciais em que foram arquivados, será o documento hábil para a transferência, por transcrição no registro público competente, dos bens com que o subscritor tiver contribuído para a formação ou aumento do capital social.”.

- Lei n.º 8934/94 - https://www.planalto.gov.br/ccivil_03/leis/L8934.htm.

Não há incidência de imposto de renda sobre ganho de capital se os bens forem transferidos pelo valor constante da declaração do imposto de renda da pessoa física (Lei nº 9.249/1995, artigo 23). Também não há incidência do imposto de transmissão "inter-vivos" relativo aos imóveis entregues para a formação do capital social ou que resultarem de cisão, fusão ou incorporação, nos termos do artigo 156, § 2º, inciso I, da Constituição Federal.

- Lei nº 9.249/1995 - http://www.planalto.gov.br/ccivil_03/leis/L9249.htm;
- Constituição Federal - http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Posteriormente as quotas sociais dessa sociedade serão transferidas no próprio contrato social aos herdeiros mediante cláusula de doação de quotas, ficando cada quinhão hereditário estabelecido de acordo com a vontade dos doadores.

Concomitantemente, estar-se-á realizando um planejamento sucessório, visando estruturar o patrimônio familiar, evitando disputas futuras quando da abertura do processo de sucessão.

O valor monetário dos bens imóveis que serão transferidos e integralizados no capital social da empresa será o valor constante na Declaração de Imposto de Renda Pessoa Física (DIRPF) do(s) doador(es) ou instituidor(es) (normalmente patriarca e/ou matriarca), do ano-calendário vigente e não pelo valor de mercado do bem. Essa condição gera grande benefício tributário em comparação com o processo de inventário, sendo que caso a sucessão seja realizada perante o Poder Judiciário o patrimônio será reavaliado e tributados pelo valor atual de mercado. Outro grande benefício tributário em relação a integralização pelo valor constante na DIRPF consiste no fato de não ser devido o Imposto de Renda sobre o ganho de capital, haja vista que os bens serão integralizados pelo mesmo valor já declarado anteriormente. A integralização dos imóveis pelo valor constante na Declaração de Imposto de Renda é prevista no Decreto nº 3.000/1999 (Regulamento Imposto de Renda), artigo 132.

- Decreto nº 3.000/1999 - http://www.planalto.gov.br/ccivil_03/decreto/D3000.htm.

Na doação de quotas com reserva de usufruto a tributação do ITCMD (Imposto de Transmissão Causa Mortis e Doação) é segregada, sendo o recolhimento feito em dois momentos. No primeiro momento o recolhimento será feito na instituição do usufruto; ou seja, na doação das quotas da *holding*. No segundo momento, o recolhimento se dará na extinção do usufruto, na ocorrência da causa *mortis*. Caso seja o desejo da família o ITCMD poderá ser recolhido de forma integral, se protegendo de eventual incerteza tributária, haja vista que alíquota aplicada será a do momento da doação.

No Estado de São Paulo, por exemplo, a tributação do ITCMD é regida pela Lei Estadual nº 10.705/2000. A alíquota para o Estado de São Paulo, conforme artigo 16 da referida lei, é fixada em 4%. Em uma doação de quotas no Estado de São Paulo a segregação do recolhimento do ITCMD é feita da seguinte forma: 2/3 no momento da doação e 1/3 na ocorrência do evento morte.

- Lei Estadual SP nº 10.705/2000 - http://www.fazenda.sp.gov.br/itcmd/LEI_10705consolidada.asp.

Os bens que serão transmitidos aos herdeiros numa eventual sucessão não serão mais os imóveis, mas sim as quotas sociais, incidindo neste caso o ITCMD na modalidade causa *mortis*, a alíquota é de 4%, que será calculado sobre o valor nominal das quotas ou sobre o quinhão que for apontado em balanço especial levantado para esse fim.

As vantagens tributárias da *holding* não param por aí. Enquanto que uma pessoa física paga até 27,5% de IR (Imposto de Renda) sobre os valores recebidos de locação (aluguéis), uma *holding*, que optou pelo sistema de apuração com base no lucro presumido, a carga tributária total (IR + CSL + PIS/COFINS) é de aproximadamente 11,33% ou, no máximo, 14,53%, se houver o adicional do imposto de renda (§ 1º, do artigo 3º, da Lei nº 9.249/1995, na redação dada pelo artigo 4º da Lei nº 9.430/1996). Ainda mais, se a empresa adotou o regime do lucro real, este permite a dedução das despesas para o cálculo do IR/CS (Imposto de Renda e Contribuição para o Financiamento da Seguridade Social), sendo ou não a atividade preponderante.

- Lei nº 9.249/1995 - http://www.planalto.gov.br/ccivil_03/leis/L9249.htm.

Sobre a venda, a pessoa física paga 15% sobre o ganho de capital; no caso da *holding* de compra e venda de imóveis, que estiver sendo tributada com base no lucro presumido, a venda dos imóveis em estoque, é tributada a uma alíquota aproximada de 6,73% sobre a receita da venda.

Além disso, os dividendos que forem distribuídos aos sócios pela *holding* estão isentos do imposto de renda.

Ressalta-se que a *holding* que receba aluguéis não pode ser optante do regime de tributação do Simples Nacional (Lei Complementar 123/2006, artigo 17, incisos XIV e XV).

- Lei Complementar 123/2006: http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp123.htm.

Consoante artigo 13 da Lei 9.718/1998, a pessoa jurídica cuja receita bruta total, no ano-calendário anterior, tenha sido igual ou inferior a R$ 78.000.000,00 (setenta e oito milhões de reais), poderá optar pela tributação com base no lucro presumido. Vale frisar que a empresa poderá ser optante pelo lucro presumido caso não se enquadre em nenhum impedimento previsto no artigo 14 da Lei nº 9.718/1998. Conforme regra do artigo 15, inciso III, alínea c, da Lei 9.249/1995 a base de cálculo do Imposto de Renda da *holding* tributada pelo lucro presumido será de 32% sobre a receita bruta.

- Lei 9.718/1998: http://www.planalto.gov.br/ccivil_03/leis/L9718compilada.htm;
- Lei 9.249/1995: http://www.planalto.gov.br/ccivil_03/leis/L9249.htm.

Sobre as receitas oriundas de locações a alíquota é 15% (Instrução Normativa RFB 1515/2014, artigo 2º, § 2º-A). Essa alíquota será aplicada na base de cálculo de 32% sobre a receita bruta apurada (IN 1515/2014, artigo 4º, inciso IV, alínea c). Essa regra está prevista no artigo 8º da Instrução Normativa SRF nº 1515/2014. Levando em consideração que a alíquota é de 15% sobre a base de cálculo de 32% sobre a receita bruta, o custo tributário final é de 4,80%.

- Instrução Normativa da Receita Federal do Brasil n.º 1515/2014: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=58604.

Mesmo a *holding* tendo a incidência de CSLL (Contribuição Social sobre o Lucro Líquido), PIS (Programa de Integração Social) e COFINS (Contribuição para o Financiamento da Seguridade Social), a tributação das receitas pela pessoa jurídica é extremamente vantajosa em comparação com a tributação das receitas operadas pela pessoa física.

Cabe explicitar que artigo 4º da Lei nº 9.430/1996 (ou § 1º, do artigo 3º, da Lei nº 9.249/1995), dispõe que a parcela do lucro real, presumido ou arbitrado, que exceder o valor resultante da multiplicação de R$ 20.000,00 (vinte mil reais) pelo número de meses do respectivo período de apuração estará sujeita a incidência de adicional do Imposto de Renda à alíquota de 10%. Sendo assim, a *holding* que auferir o lucro mensal superior a R$ 20.000,00 (vinte mil reais) ao mês, ou superior a R$ 60.000,00 (sessenta mil) no trimestre terá que apurar o adicional. Todavia os 10% irão incidir tão somente sobre o montante que ultrapassar o limite estabelecido.

- Lei nº 9.430/96: http://www.planalto.gov.br/ccivil_03/leis/L9430.htm.

No tocante a CSLL (Contribuição Social sobre o Lucro Líquido), alíquota da *holding* optante pelo regime de tributação pelo lucro presumido é de 9% aplicada sobre a base de cálculo de 32%, consoante regras dos artigos 3º e 31 da Instrução Normativa SRF nº 390/2004.

- Instrução Normativa SRF nº 390/2004: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=15288.

Levando em conta que a CSLL será tributada pela alíquota de 9% sobre a base de cálculo de 32%, o custo tributário final é de apenas 2,88%.

Na carga tributária da *holding* também irá incidir a tributação de PIS com a sua alíquota fixada em 0,65% sobre a receita bruta, conforme regra dos artigos 2º e 3º da Lei nº 9.718/1998, e COFINS, com a alíquota fixada em 3% também sobre a receita bruta, conforme regra dos mesmos artigos citados.

- Lei nº 9.718/1998: http://www.planalto.gov.br/ccivil_03/leis/L9718compilada.htm.

Na atividade de locação de imóveis, a *holding* terá seus rendimentos tributados pela alíquota de 11,33%. Já em caso da tributação incidente sobre as receitas de aluguéis auferidas por pessoas físicas a tributação é feita através de tabela progressiva, podendo a chegar a 27,5%.

- Lucro Real vs. Lucro Presumido vs. Pessoa Física: qual a forma mais eficiente de pagar impostos sobre locação de imóveis? - http://rexperts.com.br/impostos-locacao-imoveis/;

- http://idg.receita.fazenda.gov.br/acesso-rapido/tributos/irpf-imposto-de-renda-pessoa-fisica#c-lculo-anual-do-irpf.

Diante do supra exposto, notório o grande benefício tributário (significativa redução) que a transferência de bens imóveis para uma pessoa jurídica pode propiciar ao grupo familiar; haja vista que os rendimentos serão tributados pela alíquota de 11,33%, muito menor que os 27,5% incidentes sobre os rendimentos da pessoa física.

E, conforme prescrevem os artigos 138 e 142 do Decreto nº 3000/1999 (Regulamento do Imposto de Renda), a carga tributária para pessoas físicas na ocorrência da venda de um imóvel será de 15% sobre o ganho de capital auferido; ou seja, o valor da venda subtraído do valor informado na Declaração de Imposto de Renda. Já para a *holding* na mesma situação, ao final será de apenas de 5,93%, mais o adicional chegará em torno de 6,73% sobre o valor total da alienação (e não sobre o ganho de capital propriamente dito como na tributação da pessoa física).

- Decreto 3000/1999: http://www.planalto.gov.br/ccivil_03/decreto/d3000.htm.

Ressalta-se que se o imóvel for objeto de alienação é inerente ser segregado do ativo não circulante / investimentos ou do ativo não circulante / imobilizado e ser registrado contabilmente no ativo circulante como estoque, onde permanecerão os imóveis que serão objetos de alienação e deverão respeitar o princípio contábil da continuidade. Caso o imóvel integralizado já seja objeto de alienação em um futuro próximo já convém

classificá-lo na conta do ativo circulante / estoque. Após a transferência do imóvel para o ativo circulante como estoque, este imóvel não poderá continuar auferindo rendimentos oriundos dos aluguéis, sob risco de as autoridades tributárias caracterizarem essa operação de simples lançamento contábil como fraude para redução da incidência tributária. Importante frisar que para essa redução tributária é obrigatória constar no objeto social da empresa a atividade de compra e venda de imóveis.

Conforme consta do artigo 10 da Lei nº 9.249/1995, os lucros ou dividendos, pagos ou creditados pelas pessoas jurídicas tributadas com base no lucro real, presumido ou arbitrado, não ficarão sujeitos à incidência do imposto de renda na fonte, nem integrarão a base de cálculo do imposto de renda do beneficiário, pessoa física ou jurídica. Portanto, os lucros da empresa distribuídos aos sócios serão isentos do pagamento de Imposto de Renda. Ainda mais, a Instrução Normativa RFB 1515/2014, artigo 141, § 3º, caso a tributação seja pelo lucro presumido, permite a distribuição dos lucros ou dividendos de resultados mediante escrituração contábil, mesmo que o período-base não esteja encerrado. Por outras palavras, é possível a distribuição dos lucros mediante balanços periódicos (mensais, trimestrais ou semestrais).

- Lei nº 9.249/1995: http://www.planalto.gov.br/ccivil_03/leis/L9249.htm;
- Instrução Normativa RFB nº 1515/2014: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=58604.

INVESTIMENTOS ESTRANGEIROS NO BRASIL

A Constituição Federal (http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm), no artigo 172, determina que: "A lei disciplinará, com base no interesse nacional, os investimentos de capital estrangeiro, incentivará os reinvestimentos e regulará a remessa de lucros.". E, no artigo 190, prescreve que: “A lei regulará e limitará a aquisição ou o arrendamento de propriedade rural por pessoa física ou jurídica estrangeira e estabelecerá os casos que dependerão de autorização do Congresso Nacional.”.

Já no artigo 222, a CF (Constituição Federal), assim reza:

"A propriedade de empresa jornalística e de radiodifusão sonora e de sons e imagens é privativa de brasileiros natos ou naturalizados há mais de dez anos, ou de pessoas jurídicas constituídas sob as leis brasileiras e que tenham sede no País.

§ 1º Em qualquer caso, pelo menos setenta por cento do capital total e do capital votante das empresas jornalísticas e de radiodifusão sonora e de sons e imagens deverá pertencer, direta ou indiretamente, a brasileiros natos ou naturalizados há mais de dez anos, que exercerão obrigatoriamente a gestão das atividades e estabelecerão o conteúdo da programação.

§ 2º A responsabilidade editorial e as atividades de seleção e direção da programação veiculada são privativas de brasileiros natos ou naturalizados há mais de dez anos, em qualquer meio de comunicação social.

§ 3º Os meios de comunicação social eletrônica, independentemente da tecnologia utilizada para a prestação do serviço, deverão observar os princípios enunciados no art. 221, na forma de lei específica, que também garantirá a prioridade de profissionais brasileiros na execução de produções nacionais.

§ 4º Lei disciplinará a participação de capital estrangeiro nas empresas de que trata o § 1º.

§ 5º As alterações de controle societário das empresas de que trata o § 1º serão comunicadas ao Congresso Nacional.".

A Lei nº 4.131, de 3 de setembro de 1962 (http://www.planalto.gov.br/ccivil_03/leis/L4131.htm), por sua vez, disciplina a aplicação do capital estrangeiro e as remessas de valores para o exterior e dá outras providências.

A Lei n° 10.610, de 20 de dezembro de 2002 (http://www.planalto.gov.br/ccivil_03/leis/2002/L10610.htm), dispõe sobre a participação de capital estrangeiro nas empresas jornalísticas e de radiodifusão sonora e de sons e imagens, e dá outras providências.

O Decreto-Lei nº 37, de 18 de novembro de 1966 (http://www.planalto.gov.br/ccivil_03/decreto-lei/Del0037.htm), dispõe sobre o imposto de importação, reorganiza os serviços aduaneiros e dá outras providências. Já o Decreto-Lei 94, de 30 de dezembro de 1966 (http://www.planalto.gov.br/ccivil_03/decreto-lei/1965-1988/Del0094.htm), versa sobre o Imposto de Renda e dá outras providências.

O estrangeiro não pode adquirir empresas jornalísticas, de radiodifusão sonoro e imagens. Somente podem fazê-lo os brasileiros natos ou naturalizados há mais de 10 (dez) anos ou pessoa jurídica constituída sob as leis brasileiras que tenham sede no país. Essas empresas devem ter pelo menos 70% (setenta por cento) do capital de brasileiro(s) nato(s) e/ou naturalizado(s), que obrigatoriamente exerce(m) a direção da empresa e a responsabilidade pela seleção da programação veiculada e regulada pelo Poder Público.

Nova York mantém-se como principal mercado-alvo no mundo para investimentos em imóveis. Entretanto, o Brasil aparece em segundo lugar na lista dos países com a melhor oportunidade de valorização do preço em 2016. Grupos italianos, russos, portugueses, norte-americanos e espanhóis demonstraram interesse em investir no Brasil.

Já os brasileiros ocupam a terceira posição entre os maiores compradores estrangeiros de imóveis em Portugal.

- http://www.bbc.com/portuguese/internacional-37570236;
- http://istoe.com.br/319466_COMO+COMPRAR+CASA+NO+EXTERIOR/.

Qualquer cidadão pode adquirir imóveis urbanos no Brasil; inclusive os estrangeiros. As únicas restrições existentes por estrangeiros são relacionadas com a compra de imóveis rurais, terrenos de marinha e ao longo das faixas de fronteiras; as restrições não se aplicam no caso de unidade autônoma de condomínios, como a compra de apartamentos em prédio situado em terreno de marinha ou lotes de terreno.

A Constituição Federal, nos termos do artigo 190, estabelece que caberá a legislação infra regular e limitar a aquisição de propriedade rural por pessoa natural ou jurídica estrangeira. Desse modo, a aquisição de imóvel rural por pessoa natural ou jurídica estrangeira é regulada pela Lei 5.709/1971 (http://www.planalto.gov.br/ccivil_03/leis/L5709.htm), seu Decreto regulamentador n.º 74.965/1974 (http://www.planalto.gov.br/ccivil_03/decreto/1970-1979/D74965.htm) e pela Instrução Normativa do Incra (Instituto Nacional de Colonização e Reforma Agrária) n.º 76/2013 (https://www.legisweb.com.br/legislacao/?id=258139).

- http://www.incra.gov.br/institucionall/legislacao--/atos-internos/instrucoes/file/1579-instrucao-normativa-n-76-23-08-13.

Em reforço, a Lei nº 8.629, de 25 de fevereiro de 1993 (http://www.planalto.gov.br/ccivil_03/leis/L8629.htm), dispõe sobre a regulamentação dos dispositivos constitucionais relativos à reforma agrária.

Verifica-se que há dois requisitos para a aquisição de imóvel rural por estrangeiro: a pessoa física ter residência no país e a pessoa jurídica estar autorizada a funcionar no Brasil. Igualmente fica sujeito ao regime estabelecido por esta lei a pessoa jurídica brasileira da qual participem, a qualquer título, pessoas estrangeiras físicas ou jurídicas que tenham a maioria do seu capital social e residam ou tenham sede no Exterior (Lei 5.709/1971, artigo 1º, § 1º). Esta última norma não possui entendimento unânime sobre sua vigência ou aplicação, devendo ser consultado previamente o tabelião do cartório de imóveis correlato para saber a sua posição pessoal; ou seja, se ele vai autorizar ou não a lavratura em questão.

- Lei 5.709/1971 - http://www.planalto.gov.br/ccivil_03/leis/L5709.htm.

Sobre a questão existe uma batalha judicial em andamento:

- http://www.gclaw.com.br/blog/stf-suspende-norma-que-liberava-compra-de-terras-por-estrangeiro/;
- http://www.conjur.com.br/2016-set-13/stf-suspende-parecer-compra-terra-rural-estrangeiro;
- http://www.felsberg.com.br/decisao-do-stf-restabelece-no-estado-de-sao-paulo-as-restricoes-para-aquisicao-de-imovel-rural-por-pessoas-juridicas-estrangeiras-e-equiparadas/.

Independentemente disso, existe um Projeto de Lei (4.059/2012 da Câmara dos Deputados) em trâmite para liberar a compra de propriedade rural por estrangeiros.

- http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548018.

Essa iminente liberação da compra de terras por estrangeiros no Brasil deverá provocar um grande fluxo de investimentos no país; principalmente por parte de fundos em busca de rentabilidade segura e de longo prazo, reaquecendo uma fatia do mercado imobiliário que tem sofrido com a estagnação econômica e a crise política.

Esse recente interesse demonstrado pelo governo federal em mudar a legislação para permitir a compra de terras por estrangeiros está gerando uma movimentação diferente neste mercado de propriedades rurais. Nos últimos meses, grupos estrangeiros têm desembarcado no país e buscado informações sobre a compra de terras, tramites legais, funcionamento das operações entre outros.

Os avanços nas discussões sobre o tema interferem na bolsa de valores. As cinco companhias mais expostas influenciadas com dito projeto de lei são: SLC Agrícola (SLCE3), Vanguarda Agro (VAGR3), BrasilAgro (AGRO3), São Martinho (SMTO3) e Cosan (CSAN3). Destas, a Vanguarda Agro foi a mais beneficiada com uma alta de 50% em apenas quatro sessões. Recorda-se, por oportuno, que o Brasil é o maior produtor mundial de laranja, café, carne bovina e açúcar.

- http://www.valor.com.br/valor-data/commodities/agricolas;
- http://www.agrolink.com.br/cotacoes/;
- http://www.noticiasagricolas.com.br/cotacoes/;
- http://www.integrada.coop.br/cotacoes/bmef_ativos/bm&f_boi_gordo_cafe_arabica_dolar_comercial_milho_soja.xhtml.

Inobstante essa restrição atual de aquisição de terras por estrangeiros, a alienação fiduciária de bem imóvel rural em garantia em favor de pessoa física ou jurídica estrangeira, ou a esta equiparada, não se submete às restrições estabelecidas pela Lei nº 5.709/1971; constituindo essa autorização, entretanto, requisito para consolidação da propriedade no patrimônio dessas pessoas, em caso de inadimplemento da obrigação garantida e consequente de excussão do bem, ou para dação do direito eventual do fiduciante em pagamento da dívida garantida (Lei nº 5.709/1971, Código Civil [http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm], arts. 1.228, 1.361, 1.367 e 1.419, e Lei nº 9.514/1997, arts. 22 e seguintes).

Já em relação aos imóveis urbanos, por não estarem abrangidos por tais normas supra, a sua aquisição por estrangeiros é livre.

Além da assinatura (pessoalmente ou por procuração traduzida) do comprador e de seu cônjuge, para a compra de imóveis no Brasil por estrangeiro são necessários os seguintes documentos:

Passaporte se não residente ou RNE (Registro Nacional de Estrangeiro) se tiver visto de permanência;

- Se pessoa física, CPF (Cadastro de Pessoa Física);
- Se pessoa jurídica, CNPJ (Cadastro Nacional de Pessoa Jurídica);
- Se pessoa jurídica, cópia autenticada de seus atos constitutivos (contrato social);

- Se o comprador pessoa física for casado, Certidão de casamento. Se esta for estrangeira, deverá ser traduzida para o português por tradutor juramentado no Brasil e posteriormente registrada no cartório de títulos e documentos (pode ser realizado por procurador);

- Se o comprador pessoa física for casado, também, será necessário o CPF do cônjuge (que também figurará como adquirente do imóvel);

- Se o comprador pessoa física solteiro, Certidão de Nascimento ou outro documento comprobatório do estado civil, traduzido para o português no Brasil por tradutor juramentado e posteriormente registrada no cartório de títulos e documentos (pode ser realizado por procurador);

- Se o comprador não estiver presente no ato, será necessária procuração pública legalizada na repartição consular brasileira do país de origem do estrangeiro, traduzido para o português no Brasil por tradutor juramentado e posteriormente registrada num Cartório de Títulos e Documentos no Brasil, com plenos e amplos poderes, para comprar, assinar escritura, contratos particulares e resolver qualquer assunto perante os Cartórios de Notas, Registro de Imóveis e Receita Federal para regularização no Brasil do imóvel adquirido em nome do estrangeiro.

Incumbe a um profissional do ramo (Técnico em Transações Imobiliárias ou Corretor de Imóveis inscrito no CRECI - Conselho Regional de Corretores de Imóveis), conferir a documentação e tirar as certidões necessárias para verificar se o imóvel não tem nenhum impedimento legal para venda. A compra de um imóvel somente pode ser feita por escritura pública (feita em qualquer cartório ou tabelionato de notas); documento este que a lei considera hábil para ser registrado no Cartório de Registro Imobiliário. Após a celebração da escritura pública num Tabelionato de Notas (pode ser feita por procurador), qualquer pessoa, independentemente de procuração, pode levar o negócio a registro perante o Cartório de

Registro de Imóveis, a fim de conferir publicidade e eficácia à transferência do imóvel.

Para custear a aquisição, por sua vez, o estrangeiro pode valer-se de diversos procedimentos: envio de ordem de pagamento (em reais ou em moeda estrangeira), em favor do vendedor do imóvel, no banco indicado por este; pagamento direto ao vendedor por meio de conta corrente se o comprador tiver conta bancária no Brasil; transferência internacional via banco; remessa do valor do imóvel ao seu procurador, que, então, realizará a operação de câmbio junto ao agente de câmbio, para, em seguida, pagar o vendedor; etc.

- http://www.caixa.gov.br/internacional/remessas-internacionais/Paginas/default.aspx.

Também é possível efetuar o pagamento, à distância, através de uma conta *escrow*. ***Escrow account***, é uma espécie de conta controlada ou conta de garantia, através da qual o banco responsável (depositário *Escrow*) assegura as partes de só fazer o repasse dos valores após a transação estar comprovadamente concretizada, obedecendo estritamente às formas pré-estabelecidas no contrato *Escrow*. Em uma compra e venda, por exemplo, vendedor, comprador e o agente *Escrow* assinam o contrato *Escrow*. Após a assinatura o comprador depositará sob a guarda do agente *Escrow* o valor relativo à compra do objeto. Em seguida o vendedor executa os serviços necessários para o fornecimento do produto vendido e remete ao comprador para aprovação. Após a aprovação do produto, o comprador comunica o agente *Escrow* de que o produto foi entregue nos termos contratados, momento este em que o agente *Escrow* efetua a liberação dos valores para o vendedor e a negociação é concluída com êxito para ambas as partes.

Há várias maneiras de se investir em ativos brasileiros e nem sempre é necessário abrir uma conta no Brasil ou de enviar dinheiro para o Brasil.

Os investidores não residentes têm, por meio desses métodos abaixo relacionados, acesso aos mesmos produtos disponíveis para os brasileiros, podem aplicar também em fundos de investimento regulados pela CVM

(Comissão de Valores Mobiliários), com trânsito livre entre renda variável e renda fixa.

Adquirir cotas de fundos fora do Brasil, cujos ativos financeiros sejam vinculados a ativos brasileiros. Uma opção é o ETF (*Exchange-Traded Fund* ou fundos negociados na Bolsa) de ações; pois diversificam necessariamente, diminuindo o risco individual (interessante para quem não pode acompanhar o dia a dia do mercado brasileiro). Outra são os fundos de dívida pública (*bonds*), como, por exemplo, o ETF de *Emerging Markets Bond ishares* (contém apenas 3,98% de sua composição em títulos brasileiros, os demais são de outros países). Mas existem fundos que investem exclusiva ou prioritariamente em títulos brasileiros.

Os contratos de opções sobre "Exchange Traded Fund" são instrumentos derivativos criados para mitigar riscos de oscilação de preço; além de servir para criar estratégias especulativas em relação a trajetória de preço e a ampliação a exposição e do potencial de retorno de um investidor, já que o capital inicialmente investido para comprar uma opção é relativamente pequeno.

- http://www.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/renda-variavel/etf/boletim-mensal/;
- http://www.bmfbovespa.com.br/pt_br/listagem/fundos-de-investimentos/etfs-fundos-de-indices/procedimentos-de-listagem/;
- http://www.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/renda-variavel/etf/renda-variavel/etfs-listados/;
- https://www.ishares.com/us/products/239572/ishares-jp-morgan-usd-emerging-markets-bond-etf;
- ETFs DE SEGUNDA GERAÇÃO NO BRASIL - http://cfasociety.org.br/media/uploads/bsk-pdf-manager/policy_brief_for_brazil_160808_mar_br_62.pdf.

Adquirir ADR (*American Depositary Receipts*) de companhias brasileiras, que são negociados nos Estados Unidos (http://topforeignstocks.com/foreign-adrs-list/the-full-list-of-brazilian-adrs/). Basicamente o ADR é uma maneira de se comprar, nos Estados Unidos, ações de companhias brasileiras. As ações são compradas e

custodiadas no Brasil (lastreados em ações reais), mas são emitidos recibos de depósitos dessas ações no exterior.

Abrir a CDE (Conta de Domiciliado no Exterior). Entretanto, os bancos brasileiros não são obrigados a aceitarem não residentes ou estrangeiros. Deve-se, portanto, procurar um que o faça e, ainda, opere no câmbio (não pode ser uma agência qualquer).

- https://www.itau.com.br/securitiesservices/servicos/investidores-nao-residentes/;
- https://www.itau.com.br/securitiesservices/servicos/investidores-nao-residentes/faq/;
- https://banco.bradesco/html/empresas/produtos-servicos/conta-corrente/conta-internacional.shtm.

A Resolução CMN 4373/2014, antiga 2689/2000, permite aos investidores não residentes acessarem os produtos do mercado financeiro e de capitais brasileiro, por meio de operações no ambiente de bolsa de valores ou balcão organizado.

Aplicar diretamente em uma Corretora participante da Bovespa usando um banco no exterior, por meio do cadastro simplificado. Trata-se do Cadastro Simplificado de Investidores Não Residentes, que possui alguns requisitos: a) O investidor ser cliente da instituição estrangeira (banco); b) Essa instituição assumir perante a corretora a obrigação de prestar as informações cadastrais necessárias; c) O órgão de controle do país de residência ter firmado acordo de cooperação com a CVM para troca de informações; d) É necessário nomear um representante no Brasil (muitas vezes, a própria instituição financeira).

- Resolução nº 4.373, de 29/9/2014 - http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=Res&ano=2014&numero=4373 OU http://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48650/Res_4373_v1_O.pdf;
- IN - Instrução Normativa da CVM 419/2005 - http://www.cvm.gov.br/legislacao/inst/inst419.html;

- IN - Instrução Normativa da CVM 505/2011 - http://www.cvm.gov.br/legislacao/inst/inst505.html.

Uma opção de investimento, são os fundos imobiliários resultaram da entrada do ramo de imóveis no mercado financeiro (a exemplo dos REITs - *Real Estate Investment Trust* nos EUA); são como participação em locação de imóveis.

- http://carteirarica.com.br/fundos-imobiliarios/.

Como incentivo à entrada de capitais no país, o não residente, não importando se natural do Brasil ou do estrangeiro, possui incentivos para investir em aplicações financeiras no Brasil.

Várias aplicações possuem isenção de imposto de renda sobre aplicações financeiras, o que é um grande atrativo.

Além dos brasileiros que moram no exterior e que ainda possuem obrigações junto ao Fisco, a Comissão de Valores Mobiliários (CVM) determina que todo investidor estrangeiro deve, obrigatoriamente, além do cadastro na CVM, possuir a inscrição no CPF (Cadastro de Pessoa Física). Para esse grupo, no entanto, o procedimento é facilitado. O MRE - Ministério das Relações Exteriores (http://www.itamaraty.gov.br/) permite que os dois registros sejam realizados simultaneamente, em qualquer instituição financeira autorizada pelo Banco Central. O prazo para ficarem prontos é de 24 horas. Além dos investidores, os estrangeiros podem precisar de CPF para abrir uma empresa no Brasil (independentemente do porte ou do segmento), assim como também para comprar um imóvel ou bens de maior valor.

Investidores Não Residentes (INR's) são pessoas físicas ou jurídicas, inclusive fundos ou outras entidades de investimento coletivo, com residência, sede ou domicílio no exterior e que investem no Brasil. A Resolução do CMN (Conselho Monetário Nacional) nº 4.373/2014 disciplina sobre as aplicações dos INR's no Brasil, nos mercados financeiro e de capitais do país.

- https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=res&ano=2014&numero=4373.

Ainda, de acordo com o artigo 4º do citado normativo, tais investidores estão sujeitos a registro prévio na CVM. Nesse sentido, a Instrução CVM (Comissão de Valores Mobiliários) n° 560/2015 (http://www.cvm.gov.br/legislacao/inst/inst560.html) é a norma que atualmente trata sobre o registro destes investidores na Autarquia. Recomenda-se que os representantes dos INRs tenham pleno conhecimento dessas duas normas.

Detalhe, **o brasileiro é considerado não residente quando entrega sua Declaração de Saída Definitiva do País, ou quando permanece no exterior por período superior a 12 meses consecutivos** (há aqueles que vêm ao Brasil uma vez por ano para evitarem perder a condição de residentes). O brasileiro no exterior, quando se tornam não residente, passa a ter tratamento diferenciado, similar ao estrangeiro para diversos fins: a) Não pode mais abrir conta bancária comum no Brasil; passando a precisar de uma **CDE (Conta de Domiciliado no Exterior)** para manter reais no país (e as movimentações acima de R$ 10.000,00 têm de ser justificadas); b) Não entrega mais DIRPF (Declaração do Imposto sobre a Renda da Pessoa Física) anual; e, c) Passa a sofrer tributação diferenciada quanto a IOF e Imposto de Renda.

O ingresso de investidor não residente nos mercados financeiro e de capitais no Brasil continua sujeito aos mesmos requisitos estabelecidos pela Resolução CMN n° 2.689 (revogada pela Resolução nº 4.373, de 29/9/2014), quais sejam: a) ser titular de conta individual ou participante de conta coletiva (conhecida como “conta ônibus”); b) constituir representante legal e custodiante no Brasil (usualmente a instituição custodiante atua como representante legal do investidor); c) obter registro na CVM; e d) obter cadastro de pessoa física ou pessoa jurídica perante o Ministério da Fazenda. A Resolução CMN n° 4.373 trouxe mais responsabilidades para o representante legal, que, em nome do investidor não residente, deve ter poderes para receber citações, intimações e notificações relativas a procedimentos judiciais ou administrativos instaurados com base na legislação e regulamentação dos mercados financeiro e de capitais, relacionados a operações objeto do contrato de representação, dentre outras

atribuições que conferem maior relevância ao papel por eles representado. Além disso, a CVM passou a exigir que o representante seja necessariamente instituição financeira ou instituição autorizada a funcionar pelo Bacen. O registro do investidor não residente na CVM, por sua vez, ficou mais simples, passando a ser concedido automaticamente mediante protocolo dos documentos exigidos, ante a previsão anterior de manifestação expressa no prazo de 24 horas. O registro pode ser suspenso pela Superintendência de Relações com Investidores Institucionais (SIN) em caso de constatação de que o investidor não residente não cumpre qualquer dos requisitos normativos.

- Resolução 4.373/2014 - http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=Res&ano=2014&numero=4373.

A Gerência de Registros e Autorizações (GIR), da Superintendência de Relações com Investidores Institucionais (SIN), da Autarquia, é a área da CVM responsável pela análise de pedidos de registro e demais atividades cadastrais dos INR's. De acordo com a Resolução CMN nº 4.373/2014, o representante de investidor não residente deverá ser instituição financeira ou instituição autorizada a funcionar pelo Banco Central do Brasil e deverá solicitar previamente seu registro como representante de investidor não residente à CVM (Comissão de Valores Mobiliários). Para tanto, deverá enviar o pedido de registro, assinado e digitalizado, para o endereço eletrônico gie-internet@cvm.gov.br. No pedido deverá ser informada a pessoa física (fornecer nome completo, CPF e endereço de e-mail) que será responsável na instituição pela representação de investidores não residentes perante a CVM. Após a efetivação do registro do representante no cadastro da CVM, será enviada automaticamente, ao endereço de e-mail do responsável, a senha de acesso aos Sistemas mantidos pela CVM e disponíveis em seu website (CVMWeb e SIE-WEB), com a qual o representante poderá efetuar o registro dos investidores, manutenção cadastral e o envio dos informes à CVM. O próprio representante do investidor não residente fará o registro do investidor na CVM, através dos sistemas CVMWeb e SIE-WEB. Para isso, deverá dispor de senha de acesso aos sistemas mencionados, que foi fornecida ao responsável na instituição quando de seu registro na CVM. O registro do investidor é feito no sistema SIE-WEB, através da inserção das informações cadastrais previstas na

Instrução CVM n° 560/2015. Após a realização desse cadastro, o investidor deve ser incluído em uma conta coletiva ou constituir uma conta própria, para que possa realizar investimentos no mercado. Além do registro, o representante poderá realizar outras atividades no sistema SIE-WEB, tais como: consulta de investidores registrados; alteração de dados cadastrais e denominação do investidor; cancelamento de registros (contas próprias e coletivas, além de inclusões em conta coletiva); confecção de relatórios dos participantes de conta coletiva; etc. Quando se tratar de constituição de conta própria ou coletiva, o representante deverá informar à CVM, assim que disponível, o número do Registro Declaratório Eletrônico (RDE) da carteira, comunicando tal número via e-mail para o endereço eletrônico gie-internet@cvm.gov.br. O representante dos INR's deverá enviar dois informes à CVM: um informe mensal (até o décimo dia útil após o fim do mês a que se refere) com informações sintéticas (classe de ativos) sobre cada investidor representado, e um informe semestral (até o décimo-quinto dia útil após o fim do semestre a que se refere), com os dados analíticos da carteira desses investidores, ou seja, com discriminação de cada ativo detido. Os informes devem ser enviados dentro do sistema CVMWeb, também acessado através de *login* (entrar) e senha, a partir da senha master do responsável por INR's da instituição representante de cada investidor. Os informes poderão ser entregues através do envio de um arquivo padrão XML (*eXtensible Markup Language*) disponibilizado no CVMWeb, a partir do qual o representante faria o *upload* dos arquivos de todos seus representados. Conforme estipulado no art. 23 da Instrução CVM nº 560/2015, o representante está sujeito à multa diária, no valor de R$ 500,00 (quinhentos reais), em virtude do descumprimento dos prazos previstos na Instrução para entrega de informações periódicas.

- Instrução CVM nº 560/2015 - http://www.cvm.gov.br/legislacao/inst/inst560.html.

Uma importante inovação das novas regras diz respeito à realização por investidores não residentes de operações fora de mercados organizados. A antiga Resolução CMN nº 2.689 (revogada pela Resolução nº 4.373, de 29/9/2014) continha restrições a essas operações, que dependiam, em sua maioria, de aprovação específica da CVM. Tais restrições foram sendo suavizadas pelas práticas de mercado e por decisões da própria CVM, o que fez com que a Autarquia ampliasse o rol de operações permitidas

independentemente de qualquer aprovação pelo regulador. Dessa forma, não dependem de autorização prévia da CVM as seguintes operações: a) subscrição; b) bonificação; c) conversão de debêntures e outros títulos em ações; d) subscrição, amortização ou resgate de cotas de fundos de investimento regulados pela CVM; e) resgate ou reembolso, nos casos previstos em lei; f) pagamento de dividendos em valores mobiliários; g) cessão ou transferência de cotas de fundos de investimento abertos, nas hipóteses previstas na regulamentação específica da CVM; h) cessão gratuita ou onerosa de proventos devidos e ainda não pagos a investidor não residente, que objetive o encerramento de conta de custódia; i) cessão gratuita de recibos de subscrição, na qualidade de cedente ou cessionário; j) transação judicial, decisão judicial, arbitral ou administrativa; k) alienação de valores mobiliários cuja autorização para negociação em mercado organizado tenha sido cancelada ou suspensa; l) alienação de ações em decorrência do exercício de direito ou por força de obrigação estipulada em acordo de acionista que tenha sido celebrado e arquivado na CVM há mais de seis meses; m) oferta pública de distribuição de valores mobiliários; n) oferta pública de aquisição de ações (OPA) nos casos em que a CVM autorize que a oferta se realize por procedimento diverso do leilão em mercado organizado, nos termos da regulamentação específica; e o) opção de venda para os acionistas remanescentes em OPA. A cessão de direito de subscrição, apesar de aceita pela CVM em decisões da Diretoria Colegiada no passado, não integrou o rol de operações indicadas expressamente na Instrução CVM nº 560. Contudo, não nos parece razoável supor que a cessão de direito de subscrição fora de mercado organizado seja proibida, dado o contexto da nova regra.

A CVM também consolidou seu entendimento em relação às transferências de posições entre investidores não residentes oriundas do exterior. Passaram a ser admitidas, sem necessidade de aprovação prévia, as transferências em decorrência de fusão, cisão, incorporação, incorporação de ações e sucessão *causa mortis*, bem como demais operações societárias que não resultem na modificação dos titulares finais dos ativos e na alteração do total dos ativos financeiros e valores mobiliários pertencentes, direta ou indiretamente, a cada um dos investidores envolvidos na operação. Tais transferências devem ser informadas à CVM pelo representante legal do investidor não residente, juntamente com o informe mensal.

A nova regulamentação criou rol expresso de informações periódicas que devem ser prestadas pelo representante legal do investidor não residente à CVM, em bases mensais e semestrais. A entrega dessas informações passou a ser exigida no formato previsto na Instrução CVM n° 560 a partir de 1° de janeiro de 2016.

No que se refere aos DRs - *Depositary Receipts* (certificados emitidos no exterior por instituição depositária, representativos dos ativos depositados em custódia específica no Brasil) a alteração mais relevante trazida pelas novas regras foi a ampliação dos ativos que podem constituir lastro desses instrumentos.

De acordo com a Resolução CMN n° 4.373, os DRs podem ser lastreados em quaisquer valores mobiliários emitidos por companhias abertas brasileiras, e não apenas em ações como previsto na regulamentação anterior. No caso de instituições financeiras e demais instituições de capital aberto autorizadas a funcionar pelo Bacen, também em títulos de crédito elegíveis a compor o Patrimônio de Referência, possibilitando, dessa forma, a emissão de DR lastreados em instrumentos de dívida.

- https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48650/Res_4373_v1_O.pdf.

Além disso, a regulação trouxe mecanismos para facilitar a participação dos investidores não residentes que possuem DR lastreados em ações no processo decisório das companhias. A Instrução CVM n° 559 ampliou o prazo mínimo de convocação de assembleia geral de companhia emissora de DR de quinze para trinta dias de antecedência de sua realização. Além disso, o direito de voto das ações que são lastros para os DR deve ser exercido pelos depositários na forma instruída pelos titulares dos certificados, ou em seu melhor interesse, caso os contratos relativos ao programa de DR impeçam o voto instruído.

- Instrução CVM 559 - http://www.cvm.gov.br/legislacao/inst/inst559.html.

Por fim, ressalta-se que a Resolução CMN n° 4.373 reafirmou a obrigatoriedade de realização de operações simultâneas de câmbio ou

transferência internacional em reais, sem entrega efetiva dos recursos e independentemente de prévia autorização do Bacen, nas seguintes hipóteses: a) conversão de haveres de investidor não residente em investimento nos mercados financeiro e de capitais; b) transferência de aplicação de investidor não residente por meio do mecanismo de *Depositary Receipts* para a modalidade de investimentos estrangeiro diretos (IED); e, c) transferência de aplicação de investidor não residente por meio do mecanismo de *Depositary Receipts*, para aplicação nos mercados financeiro e de capitais no país; e (iv) transferência de aplicação de investidor não residente nos mercados financeiro e de capitais, para a modalidade de investimentos estrangeiro diretos (IED) e vice-versa. As transferências de aplicação de investidor não residente nos mercados financeiro e de capitais no país para aplicação por meio do mecanismo de *Depositary Receipts*, contudo, não está sujeita a tal obrigatoriedade, conforme indicado na Circular Bacen n° 3.752.

- Resolução CMN 4.373 - https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=res&ano=2014&numero=4373;
- Circular Bacen 3.752 - https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=Circular&data=2015&numero=3752.

As Leis n.ºs 4.131/1962 e 11.371/2006 determinam o registro no Banco Central do Brasil dos capitais estrangeiros ingressados no país. Desse modo, o investimento de capital estrangeiro em pessoas jurídicas no Brasil está sujeito a Registro Declaratório Eletrônico (RDE) do Bacen (Banco Central do Brasil), através do módulo de Investimento Estrangeiro Direto (IED) do Sistema do Banco Central (Sisbacen).

- Lei 4.131/1962 - http://www.planalto.gov.br/ccivil_03/leis/L4131.htm;
- Lei 11.371/2006 - https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11371.htm;
- Instrução Normativa da Receita Federal 1634/2016 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=73658.

Cademp é o cadastro de pessoas físicas ou jurídicas residentes e não residentes no País, mantido no Banco Central. Para o registro de capitais

estrangeiros no RDE - Registro Declaratório Eletrônico (http://www.bcb.gov.br/pre/portalCidadao/cambio/rde.asp?idpai=PORTALBCB), é necessário que os titulares envolvidos, pessoas físicas ou jurídicas, residentes e não residentes no país, bem como seus representantes, estejam cadastrados no Cademp. O cadastramento no Cademp é efetuado pelo próprio interessado ou por seu representante, diretamente no Sisbacen (http://www.bcb.gov.br/pt-br/#!/n/SISBACEN e https://www3.bcb.gov.br/sisbacenweb/). Para acesso ao Sisbacen, deve ser realizado um credenciamento de usuário especial, de acordo com as instruções do site do Bacen (http://www.bcb.gov.br/).

- http://www.bcb.gov.br/ftp/infecon/RDE/RDE-Cademp.pdf.
- http://www.bcb.gov.br/ftp/infecon/RDE/ManualRDE-IED.pdf.

As pessoas jurídicas estrangeiras não obrigadas à inscrição no Cadastro de Empresas (Cademp) do Banco Central do Brasil (Bacen) e nem ao Registro de Investidores Estrangeiros da Comissão de Valores Mobiliários (CVM), devem preencher a Ficha Cadastral de Pessoa Jurídica (FCPJ), no programa CNPJ para o Evento 107 (Inscrição de Pessoa Jurídica Domiciliada no Exterior) e transmiti-la via Internet através do programa Receitanet.

A RENAI - Rede Nacional de Informações sobre o Investimento (http://investimentos.mdic.gov.br/) é um instrumento pelo qual o Governo Federal busca disseminar informações sobre investimentos produtivos no Brasil.

De modo geral, as regras para investidores não residentes representam um movimento dos reguladores no sentido de acompanhar a evolução dos mercados financeiro e de capitais, conferindo maior flexibilidade aos investidores, ao mesmo tempo em que aumentam a transparência das operações.

Saiba mais em:

- http://www.portaldoinvestidor.gov.br/;
- http://www.investexportbrasil.gov.br/#;

- http://www.cvm.gov.br/.

A Bovespa possui uma guia para os investimentos estrangeiros (http://www.bmfbovespa.com.br/pt_br/regulacao/investimento-estrangeiro/). De igual modo, o Banco Central do Brasil (http://www4.bcb.gov.br/pec/gci/port/guia.asp).

Saiba mais no Portal do Investidor (http://www.portaldoinvestidor.gov.br/) e no site (http://portal.anbima.com.br/) da ANBIMA (Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais). Confira, ainda:

- Guia para investidores estrangeiros - Citi Corretora: https://www.citicorretora.com.br/sites/arquivos/downloads/guiaportfolio.pdf;

- Manual do emissor - Anexos - BM&FBovespa: http://www.bmfbovespa.com.br/lumis/portal/file/fileDownload.jsp?fileId=8AA8D09753A65AFD0153AA777E780DE0.

Infra a legislação específica para os investidores não residentes:

- Resolução nº 4.373, de 29/9/2014, do Banco Central do Brasil (http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=Res&ano=2014&numero=4373), dispõe sobre aplicações de investidor não residente no Brasil nos mercados financeiro e de capitais no País e dá outras providências;

- Instrução 555/2014 da CVM (http://www.cvm.gov.br/legislacao/inst/inst555.html), dispõe sobre a constituição, a administração, o funcionamento e a divulgação das informações dos fundos de investimento;

- Instrução CVM 578/2016 (http://www.cvm.gov.br/legislacao/inst/inst578.html) dispõe sobre a constituição, o funcionamento e a administração dos Fundos de Investimento em Participações;

- Instrução CVM 579/2016 (http://www.cvm.gov.br/legislacao/inst/inst579.html) dispõe sobre a elaboração e divulgação das demonstrações contábeis dos Fundos de Investimento em Participações;

- Instrução CVM nº 560/2015 (http://www.cvm.gov.br/legislacao/inst/inst560.html), dispõe sobre o registro, na CVM, de investidor não residente no País, de que trata a Resolução CMN 4.373/2014 e dá outras providências;

- Ofício-Circular CVM/SIN/n° 2/2014 (http://www.cvm.gov.br/legislacao/circ/sin/oc-sin-0214.html), apresenta aos representantes o novo sistema de registro de investidor não residente e seu manual de operação;

- OFICIO-CIRCULAR/CVM/SIN/Nº 4/2015 - Alterações na legislação sobre Investidores Não Residentes (http://www.cvm.gov.br/export/sites/cvm/legislacao/circ/sin/anexos/oc-sin-0415.pdf);

- Ofício-Circular CVM/SIN/n° 3/2016 (http://www.cvm.gov.br/legislacao/circ/sin/oc-sin-0316.html), apresenta aos representantes o novo padrão XML do Informe Mensal de Investidores Não Residentes e orientações para preenchimento do documento;

- Dúvidas sobre os atos normativos podem ser enviadas para o e-mail: gie-internet@cvm.gov.br.

OBTENÇÃO DE DOCUMENTOS PESSOAIS E ABERTURA DE EMPRESA NO BRASIL

O **CPF (Cadastro da Pessoa Física)** é um banco de dados sobre as propriedades, bens, valores, fontes de renda e demais informações financeiras dos contribuintes (seja nacional ou estrangeiro, residente ou não) para fins de arrecadação tributária; portanto, trata-se do registro da pessoa física junto à Receita Federal do Brasil.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/assuntos-relacionados/perguntas-e-respostas;
- http://www.bcb.gov.br/pre/bc_atende/port/investimento.asp.

Enfim, para fins de arrecadação e fiscalização tributária, o governo brasileiro através do CPF centraliza, arquiva, compara e analisa todas as informações fornecidas pelo próprio contribuinte (declarações sobre renda e bens), por todas as pessoas (físicas e jurídicas) que celebraram negócios (pagaram ou receberam valores e/ou compraram ou forneceram bens e/ou serviços) com o contribuinte, por intermediários de negócios, por instituições financeiras, por outros órgãos públicos e através de demais fontes de informações e sistemas da Receita Federal. Desse modo, o CPF versa sobre as finanças da pessoa física no Brasil (se for pessoa jurídica, o documento será o CNPJ (Cadastro Nacional de Pessoa Jurídica) e, portanto, é necessário para poder realizar alguma transação de negócios; ou seja, adquirir, alugar, vender ou simplesmente fornecer algum bem, serviço ou valor. Em suma, o CPF é necessário para o estrangeiro que vier ao Brasil para residir (mesmo que provisoriamente ou a trabalho) ou, mesmo que sem residir ao Brasil, nele realizar investimentos, investir na bolsa de valores, abrir conta bancária, constituir ou adquirir participação numa empresa ou comprar imóvel ou qualquer bem de grande valor.

Em resumo, todos os residentes no exterior, sejam brasileiros ou estrangeiros, que possuam bens ou direitos no Brasil, devem se inscrever perante a Secretaria da Receita Federal do Brasil.

Os brasileiros, que tenham de 16 a 25 anos e possuam Título de Eleitor regular, podem solicitar o CPF pela internet através do preenchimento de um

formulário eletrônico.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/atos-cadastrais/inscricao-no-cpf/inscricao-de-residentes-no-brasil-ou-no-exterior;

- https://www.receita.fazenda.gov.br/Aplicacoes/ssl/ATCTA/CPF/InscricaoPublica/inscricao.asp.

Nos demais casos, somente em agências da Receita Federal ou através de entidades públicas conveniadas.

- http://idg.receita.fazenda.gov.br/interface/agendamento;

- http://idg.receita.fazenda.gov.br/interface/agendamento/atendimento-realizado-por-instituicoes-conveniadas;

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/conveniados-e-parceiros/entidades-publicas-conveniadas;

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/conveniados-e-parceiros;

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/juntas-comerciais-conveniadas-para-inscricao-e-alteracao-do-cnpj/relacao-das-juntas-comerciais-conveniadas;

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/juntas-comerciais-conveniadas-para-inscricao-e-alteracao-do-cnpj/inscricao-e-alteracao-do-cnpj-2013-orientacoes.

O registro no CPF, em síntese, será obrigatório para os residentes no exterior que possuam: imóveis, veículos, embarcações, aeronaves, participações societárias, contas correntes bancárias, incluindo as contas de não residentes e aplicações nos mercados financeiros e de capitais.

Note-se que o estrangeiro não será considerado residente no Brasil para fins de tributação apenas pela inscrição no CPF. A simples inscrição do estrangeiro no CPF não o caracteriza como residente e, consequentemente, não o sujeita às normas tributárias aplicáveis aos mesmos. A inscrição não criará imediatamente uma obrigação tributária de recolhimento de quaisquer tributos; salvo se o estrangeiro possuir rendimentos tributáveis pelo fisco brasileiro, caso em que os tributos devidos deverão ser recolhidos na fonte.

Sem prejuízo, a inscrição no CPF criará obrigações acessórias ao estrangeiro, que deverá apresentar a Declaração Anual de Isentos – DAI. A obrigatoriedade de apresentação da Declaração de Ajuste Anual do Imposto de Renda é atribuída somente as pessoas físicas residentes no país (IN SRF - Instrução Normativa da Secretaria da Receita Federal do Brasil nº 1445/2014).

- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=50127#1389855.

Os estrangeiros podem tirar CPF (Cadastro da Pessoa Física) de forma automática em representações brasileiras no exterior.

- http://www.itamaraty.gov.br/pt-BR/relacoes-bilaterais;
- http://www.portalconsular.mre.gov.br/.

O estrangeiro interessado em conseguir um CPF pode preencher um formulário (http://www.receita.fazenda.gov.br/Aplicacoes/Atcta/CpfEstrangeiro/fcpf.asp) em inglês, espanhol ou português, disponível na página da RFB - Receita Federal do Brasil (http://www.receita.fazenda.gov.br/Aplicacoes/Atcta/CpfEstrangeiro/default.htm). Depois de imprimir o formulário, deve-se procurar uma representação do Ministério das Relações Exteriores com os documentos pessoais necessários. Entregar o formulário, acompanhado de cópia dos documentos pessoais, em uma repartição consular brasileira (consulado ou embaixada com setor consular), para fins de conclusão da solicitação. A repartição consular brasileira processará a solicitação e informará o número de inscrição no cadastro CPF ao interessado. O solicitante poderá acompanhar o andamento de seu pedido no sítio da RFB, nas versões em português, espanhol ou inglês.

- http://www.receita.fazenda.gov.br/Aplicacoes/ATCTA/CPF/ConsultaAndamento.asp.

Dentro do prazo de 90 dias, o solicitante poderá: a) emitir o Comprovante de Inscrição no CPF por meio de serviço disponível no sítio

da RFB; e, b) em caso de incorreção nos dados cadastrais, requerer a retificação, sem ônus.

- http://www.portalconsular.mre.gov.br/regioes/europa/portugal/faro/cpf/inscricao-no-cpf.

Para o estrangeiro obter o CPF será preciso fotocópia autenticada do passaporte (página da foto) e os seguintes dados: nome completo, nome completo dos pais (pai e mãe), escolaridade, profissão, nacionalidade, estado civil, endereço, código postal, nº do passaporte, data e local de nascimento.

Para que o estrangeiro possa tirar o CPF no Brasil, o mesmo precisará possuir alguns documentos em mãos para a apresentação no momento da solicitação do Cadastro de Pessoa Física. O documento que é essencial para que o estrangeiro possa realizar o CPF no Brasil é o RNE (Registro Nacional de Estrangeiro) ou outro documento que possa confirmar a validade de sua identificação no país de origem, além de que a CIE - Cédula de Identidade de Estrangeiro, também pode ser aceita pelo órgão responsável por emitir o CPF. Em substituição aos documentos acima, é possível, também, apresentar o passaporte ou protocolo de RNE, caso o estrangeiro ainda não o possua, identificando estar em processo de realização. Além dos documentos citados acima, é essencial que o estrangeiro também apresente, no momento da solicitação de seu CPF, os documentos de identificação com validade em seu país de residência com tradução juramentada, sem a necessidade de indicar filiação. Para tirar o CPF, o estrangeiro interessado deverá comparecer pessoalmente ao órgão responsável, assim como agências do Banco do Brasil, Internet e diretamente na Receita Federal; além de ser possível que o representante legal do indivíduo compareça ao local para a solicitação. Ainda que o indivíduo compareça nos órgãos citados acima como válidos para o cadastramento de CPF, o estrangeiro que está situado no Brasil somente poderá concluir a retirada de sua solicitação ao apresentar-se em alguma das unidades da Receita Federal. A convocação para o comparecimento será enviada por correspondência, sendo que o estrangeiro deverá portar os documentos indicados e o protocolo de atendimento para finalizar o processo e obter seu CPF.

Através do Decreto Legislativo 148, de 12 de junho de 2015 (http://www2.camara.leg.br/legin/fed/decleg/2015/decretolegislativo-148-6-julho-2015-781175-convencao-147469-pl.html), do Decreto (federal) nº 8.660, de 29/01/2016 (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8660.htm) e da Resolução do CNJ (Conselho Nacional de Justiça) nº 228 de 22/06/2016 (http://www.cnj.jus.br/busca-atos-adm?documento=3139), o Brasil aderiu à **Convenção sobre a Eliminação da Exigência de Legalização de Documentos Públicos Estrangeiros** (Convenção de Haia). A única formalidade que pode ser exigida para atestar a veracidade da assinatura, a qualidade e a autenticidade será o selo ou carimbo dado pela autoridade competente do país donde o documento é originário. Esta formalidade não pode ser exigida caso as leis, os regulamentos, os costumes que vigorem no país onde se celebrou o ato afaste, simplifique ou dispense o ato da legalização. Desse modo, os documentos estrangeiros, uma vez apostilados no exterior, também estarão aptos a produzir efeitos no Brasil, junto às autoridades, órgãos e instituições interessadas. Não haverá mais envolvimento do Ministério das Relações Exteriores (ou de suas representações no exterior) no processo. Importante ressaltar que eventuais formalidades, no Brasil, podem ser exigidas, como a tradução para o português por profissional (Tradutor Juramentado) residente no Brasil. A apostila confere validade internacional ao documento, que poderá ser apresentado nos 111 países que já aderiram à Convenção. Contudo, a "legalização única" não exime o solicitante de apurar junto ao país ou à instituição destinatária do documento eventuais exigências adicionais, a exemplo de traduções.

- http://www.cnj.jus.br/poder-judiciario/relacoes-internacionais/convencao-da-apostila-da-haia/atos-normativos;
- https://www.hcch.net/en/instruments/conventions/status-table/?cid=41;
- https://www.hcch.net/pt/instruments/conventions/specialised-sections/apostille.

Principais normas sobre o CPF:

- Lei nº 4.862, de 29 de novembro de 1965 (http://www.planalto.gov.br/ccivil_03/LEIS/L4862.htm), artigo 11;
- Decreto-Lei nº 401, de 30 de dezembro de 1968 (http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del0401.htm), artigos 1º e 2º;

- Decreto nº 3.000, de 26 de março de 1999 (http://www.planalto.gov.br/ccivil_03/decreto/d3000.htm), parágrafo 1º do artigo 33;

- IN (Instrução Normativa) da SRF (Secretaria da Receita Federal) n.º 1548, de 13 de fevereiro de 2015, incisos de I a VI do artigo 3º (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=61197);

- IN SRF (Instrução Normativa da Secretaria da Receita Federal) n.º 1634, de 6 de maio de 2016 (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=73658#1624555);

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/assuntos-relacionados/legislacao;

- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/copy_of_cpf-cadastro-de-pessoas-fisicas.

Em Portugal, o NIF - Número de Identificação Fiscal (também referido como Número de Contribuinte) é o equivalente ao CPF (Cadastro de Pessoas Físicas) do Brasil. Entretanto, em Portugal não há distinção entre contribuinte pessoa física e jurídica (CPF e CNPJ) no nome dessa inscrição; ou seja, ambas (pessoas físicas e pessoas jurídicas) possuem NIF. Enquanto que no Brasil pode-se inserir o número de CPF na carteira de identidade (RG), em Portugal o número do NIF é registrado no cartão único, que une o bilhete de identidade (BI) às demais informações da pessoa. O estrangeiro residente em Portugal deve estar registrado no SEF - Serviço de Estrangeiros e Fronteiras (http://www.sef.pt/); no Brasil o órgão competente é a Polícia Federal (http://www.pf.gov.br/).

- http://www.nif.pt/como-pedir-um-nif/;

- https://www.portaldocidadao.pt/web/autoridade-tributaria-e-aduaneira/numero-de-identificacao-fiscal-pessoa-singular.

Na Itália o equivalente do CPF é o *Codice Fiscale*, que é solicitado na *Agenzia dell'Entrate* (http://www.agenziaentrate.gov.it/).

Nos Estados Unidos da América (EUA), o equivalente do CPF é o número do seguro social (SSN - *Social Security Number*), que é emitido pela *Social Security* (http://www.socialsecurity.gov/ssnvisa). No site da seguridade social americana (http://www.ssa.gov/ssnumber/) é informado

quem pode ter um e quais são os documentos necessários para quem deseja ou precisa tirar o SSN. Com ele é possível comprar coisas financiadas, ter cartão de crédito, comprar carro, casa e outras coisas mais. Com ele a pessoa passa a ter um *Credit Score*, indispensável para a compra de qualquer imóvel ou bem a ser financiado no país. Sem ele, o indivíduo tem que comprar a maioria das coisas à vista. Antes da quebra do mercado imobiliário americano, casas eram financiadas sem SSN. Com o *Tax ID* também é possível abrir conta em alguns bancos e até ter *Credit Score*. O *Tax ID* é um documento que pode ser tirado por qualquer pessoa; inclusive imigrantes ilegais. Estrangeiros nos Estados Unidos só podem obter o SSN com a devida permissão do antigo Serviço de Imigração (INS - *Immigration and Naturalization Service*), que foi desmembrado em três novas entidades: Serviços de Imigração e Cidadania dos Estados Unidos (USCIS - *United States Citizenship and Immigration Services*; https://www.uscis.gov/), Imigração e Alfândega (ICE - *Immigration and Customs Enforcement*; https://www.ice.gov/) e Costumes e Proteção de Fronteiras (CBP - *Customs and Border Protection*; https://www.cbp.gov/) - dentro do recém-criado Departamento de Segurança Interna (DHS - *Department of Homeland Security*; https://www.dhs.gov/). Um *Tax ID Card* (ITIN - *Individual Taxpayer Identification Number*, *Taxpayer Identification Number*, *Tax Identification Number*, *Federal Taxpayer Identification Number*, Número de Identificação Fiscal Individual, Número de Identificação do Contribuinte ou Número Federal de Identificação Fiscal), é um número de processamento de imposto que somente está disponível para alguns não-residentes e residentes estrangeiros, seus cônjuges e dependentes que não podem obter um SSN nos EUA (https://www.irs.gov/individuals/international-taxpayers/taxpayer-identification-numbers-tin#ptin).

O procedimento de retirada do CPF e do registro de investidor estrangeiro é simultâneo e pode ser feito em qualquer instituição financeira autorizada pelo Banco Central do Brasil.

O Certificado Digital funciona, basicamente, como um Documento Eletrônico de Identidade.

O **e-CPF** é o Cadastro de Pessoa Física de forma eletrônica, que garante a autenticidade e a integridade na comunicação eletrônica entre pessoas

físicas e a Receita Federal no Brasil. Com este documento digital, a pessoa detentora poderá realizar serviços, assinar ou autenticar e-mails de forma digital e ser utilizado na Receita Federal. O documento funciona vinculado ao CPF, mantendo-se o mesmo número. Dentre suas aplicações, o e-CPF serve para entregar declarações de renda e demais documentos eletrônicos com aposição de assinatura digital; tais como, por exemplos, na assinatura digital de contratos em geral (bancários, de câmbio, etc.).

O processo para a emissão de certificado digital (e-CPF) tem a fase da validação presencial do titular do certificado, que nesse momento haverá a apresentação dos documentos de identificação legalmente aceitos e necessários, original e cópia, conforme o Certificado Digital solicitado.

Em resumo, os documentos são: cédula de identidade (RNE - Registro Nacional de Estrangeiro para o estrangeiro domiciliado no Brasil, Passaporte para o não domiciliado no Brasil e, talvez, seja aceita a Permissão Internacional para Dirigir); CPF (Cadastro de Pessoa Física) válido e com situação regular junto à Receita Federal do Brasil (RFB); comprovante recente (expedido há no máximo 90 dias) de residência em nome do solicitante ou declaração emitida pelo titular; e, duas (2) vias do Termo de Titularidade, gerado após o preenchimento do Formulário de Solicitação para Certificado Digital, que deverão ser assinadas somente na presença do Agente de Registro. Já para pessoa jurídica exige-se: Ato Constitutivo devidamente registrado no órgão competente; Ata de Eleição devidamente registrado no órgão competente (nos casos em que os Sócios e/ou Diretoria sejam eleitos em Ato separado); CNPJ - Comprovante de Inscrição e Situação Cadastral impresso no dia da validação e com situação cadastral válida (Ativa); e, documentos do(s) representante(s) legal(is) da(s) empresa(s).

Pode-se contatar alguma agência da Caixa Econômica Federal (http://www.caixa.gov.br/) no exterior (http://www.caixa.gov.br/atendimento/Paginas/default.aspx#encontre) para se informar se ela pode emitir o Certificado Digital. De modo semelhante, deve-se, também, consultar qualquer banco brasileiro no exterior (https://pt.wikipedia.org/wiki/Lista_de_bancos_do_Brasil), seja público ou

privado, para indagar se eles estão habilitados a emitirem certificados digitais.

Como o Ministério das Relações Exteriores (http://www.itamaraty.gov.br/) é uma das Autoridades Certificadoras da Raiz da ICP-Brasil, também pode contatar uma de suas representações consulares no exterior (http://www.itamaraty.gov.br/pt-BR/relacoes-bilaterais) e perguntar se eles mesmos ou algum conveniado no local está habilitado a emitir certificado digital.

Pelo fato de que a empresa Digitalsign (https://www.digitalsign.pt/pt), que é portuguesa, através da Digitalsign Certificadora (https://www.digitalsigncertificadora.com.br/pt), que é brasileira, tornou-se a 12ª AC (Autoridade Certificadora) de 1º nível da ICP-Brasil, talvez seja possível um cidadão português conseguir emitir um certificado digital ICP-Brasil em Portugal. Melhor ainda, a Pronova (http://www.pronova.com.br/) atende em Portugal para emissão de Certificados Digitais padrão ICP-Brasil. Portanto, Portugal é o primeiro país a contar com uma Autoridade Certificadora brasileira, credenciada para emitir certificados digitais padrão ICP-Brasil internacionalmente.

- http://www.pronova.com.br/pronova-a-sua-certificadora-digital-no-brasil-e-em-portugal.

A obtenção do **RNE (Registro Nacional de Estrangeiro)** é feita através do acesso ao portal online da Polícia Federal (http://www.pf.gov.br/). O estrangeiro deve preencher o formulário de requerimento corretamente, devendo solicitar a opção que mais se adequa à sua situação: anistia, substituição, emissão ou renovação de documento, para em seguida poder agendar data, hora e local do atendimento. Informações erradas podem retardar o pedido e dificultar a emissão do documento. Ao finalizar o pedido, deve-se salvá-lo e imprimir a GRU (Guia de Recolhimento da União); que corresponde a taxa de emissão do documento. Para a emissão da 2ª via da identidade para estrangeiros, o valor cobrado na GRU é pouco mais elevado; a menos em casos de roubo, com apresentação do Boletim de Ocorrência para recorrer do valor. A identificação para os estrangeiros tem validade de até nove anos, devendo ser renovada antes de sua expiração, e caso o estrangeiro se ausente por pelo menos dois anos ou mais do território

nacional, este terá o seu registro cancelado. A renovação também é feita através do formulário de requerimento disponível no portal da Polícia Federal, devendo o estrangeiro optar pela opção adequada a sua situação, e caso o documento expire antes de sua renovação, o mesmo deverá pagar uma multa.

- http://www.pf.gov.br/servicos-pf/estrangeiro/registro-e-emissao-renovacao-de-cedula-de-identidade-de-estrangeiro/requerer-registro-renovacao-e-anistia.

CNPJ é a sigla de **Cadastro Nacional da Pessoa Jurídica**. Trata-se de um cadastro (banco de dados) administrado pela Receita Federal do Brasil que registra as informações das pessoas jurídicas (independentemente da finalidade ou objeto social e, inclusive, até as sem personalidade jurídica como condomínios, órgãos públicos, fundos, etc.) e das equiparadas para fins fiscais (pessoas físicas que exploram em nome individual atividades com intuito de lucro), que são obrigadas a se inscreverem antes de iniciar as suas atividades.

O CNPJ é obrigatório para todas as empresas brasileiras e para empresas estrangeiras que queiram investir no país.

Contar com um CNPJ permite que a empresa emita nota fiscal, faça compras e até contrate outros serviços. Embora vise a identificação perante a Receita Federal, o CNPJ é usado em aberturas de contas jurídicas, financiamentos, na elaboração de contratos e nos mais diversos fins.

O CNPJ é fornecido pela Receita Federal e o pedido só pode ser feito online, necessidade de se fazer o download ou instalar qualquer programa para as solicitações.

O **DBE - Documento Básico de Entrada** (https://www38.receita.fazenda.gov.br/redesim/welcome.html) é um documento que é utilizado para praticar qualquer ato em diversas circunstâncias perante o CNPJ. Ou seja, quando uma pessoa deseja atuar como profissional, seja em qualquer área do mercado como pessoa jurídica, ela deve dar entrada ao processo de Documento Básico de Entrada no CNPJ. A inscrição do Microempreendedor Individual (MEI) será realizada exclusivamente através da sua formalização no Portal do Empreendedor

(http://www.portaldoempreendedor.gov.br/); ou seja, o MEI está dispensado da apresentação do DBE e do Protocolo de Transmissão.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj;
- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/solicitacao-de-atos-perante-o-cnpj-por-meio-da-internet/inscricao-de-primeiro-estabelecimento-matriz;
- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/juntas-comerciais-conveniadas-para-inscricao-e-alteracao-do-cnpj/inscricao-e-alteracao-do-cnpj-2013-orientacoes;
- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/coleta-online-programa-gerador-de-documentos-do-cnpj-cnpj-versao-web.

No site da Receita Federal (http://idg.receita.fazenda.gov.br/) é possível realizar consulta pública de CNPJ e obter as seguintes informações: data de abertura, nome da empresa, título ou nome fantasia (se tiver), código e descrição da atividade econômica principal (CNAE), código e descrição das atividades econômicas secundárias (se tiver), código e descrição da natureza jurídica, endereço e situação cadastral junto à Receita Federal.

- http://www.receita.fazenda.gov.br/PessoaJuridica/CNPJ/cnpjreva/cnpjreva_solicitacao2.asp.

Já o **CNE - Cadastro Nacional de Empresas** (http://cne.smpe.gov.br/) contém dados cadastrais de empresas nacionais e estrangeiras em funcionamento no país e possibilita a pesquisa de seis opções de relatórios com informações como: endereço, capital social, data de início da atividade, filiais de empresas estrangeiras, bloqueios, livros mercantis, atual situação do empreendimento, filiais nos Estados, natureza jurídica e outros dados empresariais. Dito cadastro é utilizado pelo governo federal para a formulação de políticas públicas e o planejamento das empresas.

O **CadSinc** - Cadastro Sincronizado Nacional (https://www16.receita.fazenda.gov.br/Cadsinc/) representa a integração dos procedimentos cadastrais relativos às Pessoas Jurídicas e demais entidades no âmbito das Administrações Tributárias da União, dos Estados, do Distrito

Federal, dos Municípios e dos demais órgãos e entidades que participem do processo de formalização e legalização de empresas - denominados convenentes.

As **pessoas jurídicas domiciliadas no exterior que estão obrigadas à inscrição no CNPJ** são:

I - Aquelas que possuem no Brasil:

a) imóveis;
b) veículos;
c) embarcações;
d) aeronaves;
e) contas-correntes bancárias.

Nesta regra não estão obrigadas à inscrição no CNPJ as pessoas jurídicas que possuam ou adquiram:

a) direitos relativos à propriedade industrial (marcas e patentes);
b) investimentos estrangeiros através do mecanismo de certificados representativos de ações ou outros valores mobiliários (Depositary Receipts) emitidos no exterior, com lastro em valores mobiliários depositados em custódia específica no Brasil.

II – Aquelas que realizam ou contratam no Brasil as seguintes operações, estando obrigadas à inscrição no Cadastro de Empresas (Cademp) do Banco Central do Brasil (BACEN):

a) aquisição de bens intangíveis com prazo de pagamento superior a 360 dias;
b) financiamentos;
c) financiamento à importação;
d) arrendamento mercantil externo ("leasing");
e) arrendamento simples, aluguel de equipamentos e afretamento de embarcações;
f) importação de bens sem cobertura cambial destinados à integralização de capital de empresas brasileiras;

g) empréstimos em moeda concedidos a residentes no País;

h) investimentos (participações societárias em pessoas jurídicas brasileiras).

III – Aquelas que realizam no Brasil exclusivamente aplicações no mercado financeiro ou no mercado de capitais, estando obrigadas à inscrição no Registro de Investidores Estrangeiros da Comissão de Valores Mobiliários (CVM).

A inscrição de pessoas jurídicas domiciliadas no exterior no Cadastro Nacional da Pessoa Jurídica (CNPJ) poderá ser formalizada com o deferimento de sua inscrição no Cadastro de Empresas (Cademp), por ocasião da realização de operações sujeitas a registro no Banco Central do Brasil, tais como investimentos externos e empréstimos em moeda. Será atribuído a tais pessoas jurídicas número de CNPJ provisório. Estas deverão encaminhar à Secretaria da Receita Federal (SRF) os documentos necessários à obtenção da inscrição definitiva (ato constitutivo ou instrumento equivalente e procuração com poderes especiais) no prazo de 180 dias, contados da inscrição através do software Cademp, sob pena de cancelamento da inscrição provisória.

A **inscrição, alteração de dados cadastrais e a baixa no CNPJ** serão formalizadas, obrigatoriamente, por meio dos seguintes documentos: a) Documento Básico de Entrada do CNPJ ou protocolo de transmissão da FCPJ; e, b) Ficha Cadastral da Pessoa Jurídica acompanhada, no caso, do registro de inscrição da sociedade e do quadro de sócios ou administradores (QSA).

Uma das primeiras coisas a fazer para a criação de uma pessoa jurídica ou a criação de um CNPJ, é definir a correta atividade (ou área de atuação) a ser prestada pela empresa através de catálogo classificatório (http://www.cnae.ibge.gov.br/) denominado CNAE (Classificação Nacional de Atividades Econômicas). Depois disso deve-se apurar qual será o tipo societário da empresa ou a forma jurídica do CNPJ. Ambos procedimentos ainda se restringem aos atos preparatórios mentais, estratégicos e iniciais para poder-se começar a rascunhar ou esboçar a criação da pessoa jurídica ou da confecção do CNPJ.

- http://www.crcrs.org.br/arquivos/livros/cartilha_sebrae_empresa.pdf.

Para cada tipo de empresa, a Receita Federal possui uma lista de documentos exigidos (confira o link infra); o que evidencia a necessidade de saber identificar corretamente o tipo de empresa a ser aberta, além do que se declarar uma atividade e desempenhar outra, a empresa pode sofrer com problemas de fiscalização tributária em geral, pois os tipos de tributos e as respectivas alíquotas variam de acordo com a atividade, o tipo de empresa, o quadro societário, o faturamento, etc.

- http://www.receita.fazenda.gov.br/PessoaJuridica/CNPJ/tabelas/DocumentosEventos.htm.

Tal como as pessoas físicas precisam previamente possuir uma certidão de nascimento antes de poder ter um CPF, as empresas (pessoas jurídicas) precisam ante ter um NIRE (Número de Identificação do Registro da Empresa); que é um documento que depende de um Contrato Social, Ficha de Cadastro Nacional e Registro na Junta Comercial do Estado. Por outras palavras, sem essa documentação prévia não existe uma pessoa jurídica ou razão social para poder pedir CNPJ.

A elaboração de Contrato Social e os demais atos dependem da ajuda de um profissional especializado, tanto em contabilidade quanto em direito.

A pessoa jurídica é entidade criada pela união de pessoas, podendo ser: sociedade, associação, fundação, organização religiosa ou partido político. Nasce com o registro no órgão público competente (Junta Comercial ou Cartório, conforme o caso). Possui vida própria e isolada das pessoas que a constituíram; ou seja, possui personalidade distinta da de seus membros.

Após a confecção do documento de constituição da empresa, deve-se realizar o registro na Junta Comercial ou cartório, a inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) e vai até o alvará de funcionamento.

O registro de uma empresa que exercerá atividade empresária (finalidade econômica ou de lucro) e de cooperativas é feito na Junta Comercial do Estado; caso contrário, será no Cartório de Registro de Pessoa Jurídica.

Antes de fazê-lo, porém, é preciso verificar se há alguma empresa registrada com o nome pretendido. Todas as juntas comerciais oferecem esse tipo de consulta pela internet.

O ideal é consultar o site da Junta Comercial do Estado em que a empresa será localizada para saber qual é o procedimento e quais são os documentos que devem ser apresentados. De igual modo, em não se tratando de registro na Junta Comercial, deve-se identificar e contatar qual é o Cartório de Registro de Pessoa Jurídica do município.

- http://www.institucional.jucesp.sp.gov.br/empresas_manuais.php;
- http://www.institucional.jucesp.sp.gov.br/empresas_jucesp-orienta.php.

Em geral, os **documentos necessários para o registro na Junta Comercial** são:

a) Requerimento Padrão (Capa da Junta Comercial), em uma via;

b) Contrato Social ou Requerimento de Empresário Individual ou Ata de Assembleia Geral de Constituição e Estatuto, em três vias (quatro vias, no caso de empresário);

c) Cópia autenticada do documento de identidade do titular ou dos administradores;

d) Original, ou cópia autenticada, de procuração, com poderes específicos e se por instrumento particular, com firma reconhecida, quando o requerimento, a alteração contratual ou a declaração de que trata o caso a seguir (ingresso de administrador) for assinada por procurador. Se o outorgante for analfabeto, a procuração deverá ser passada por instrumento público;

e) Cópia autenticada da identidade do signatário do requerimento;

f) Aprovação prévia de órgão governamental competente, quando for o caso. Ou seja, para empresa de serviços aéreos, de telecomunicações,

corretoras de câmbio, de títulos e valores mobiliários, distribuidora de valores etc. (Instrução Normativa DNRC nº 32, de 19/04/1991);

g) FCN (Ficha de Cadastro Nacional) modelo 1 e 2, em uma via;

h) Pagamento de taxas por meio de Guia de Recolhimento (JC) e DARF (CNE).

Na Ficha de Cadastro Nacional, além dos dados cadastrais da empresa, são informados os códigos de atividade econômica, de acordo com as constantes na Tabela CNAE (Classificação Nacional de Atividades Econômicas). Esses mesmos códigos devem ser informados também para os demais órgãos e entidades responsáveis por inscrições fiscais, emissão de alvarás e concessão de licenças.

Através do Decreto Legislativo 148, de 12 de junho de 2015 (http://www2.camara.leg.br/legin/fed/decleg/2015/decretolegislativo-148-6-julho-2015-781175-convencao-147469-pl.html), do Decreto (federal) nº 8.660, de 29/01/2016 (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8660.htm) e da Resolução do CNJ (Conselho Nacional de Justiça) nº 228 de 22/06/2016 (http://www.cnj.jus.br/busca-atos-adm?documento=3139), o Brasil aderiu à **Convenção sobre a Eliminação da Exigência de Legalização de Documentos Públicos Estrangeiros** (Convenção de Haia). A única formalidade que pode ser exigida para atestar a veracidade da assinatura, a qualidade e a autenticidade será o selo ou carimbo dado pela autoridade competente do país donde o documento é originário. Esta formalidade não pode ser exigida caso as leis, os regulamentos, os costumes que vigorem no país onde se celebrou o ato afaste, simplifique ou dispense o ato da legalização. Desse modo, os documentos estrangeiros, uma vez apostilados no exterior, também estarão aptos a produzir efeitos no Brasil, junto às autoridades, órgãos e instituições interessadas. Não haverá mais envolvimento do Ministério das Relações Exteriores – ou de suas representações no exterior – no processo. Importante ressaltar que eventuais formalidades, no Brasil, podem ser exigidas, como a tradução para o português por profissional (tradutor juramentado) residente no Brasil. A apostila confere validade internacional ao documento, que poderá ser apresentado nos 111 países que já aderiram à Convenção.

Contudo, a "legalização única" não exime o solicitante de apurar junto ao país ou à instituição destinatária do documento eventuais exigências adicionais, a exemplo de traduções.

- http://www.cnj.jus.br/poder-judiciario/relacoes-internacionais/convencao-da-apostila-da-haia/atos-normativos;
- https://www.hcch.net/en/instruments/conventions/status-table/?cid=41;
- https://www.hcch.net/pt/instruments/conventions/specialised-sections/apostille.

Registrada a empresa, ela recebe o NIRE (Número de Identificação do Registro de Empresa), que consta em etiqueta afixada no ato constitutivo.

Para o **Microempreendedor Individual**, a formalização é feita de forma gratuita pela Internet no endereço www.portaldoempreendedor.gov.br. Após o cadastramento, a inscrição na Junta Comercial, o CNPJ, INSS e Alvará Provisório de Funcionamento são obtidos imediatamente gerando um documento único que é o Certificado da Condição de Microempreendedor Individual (CCMEI).

A formalização de empresários não enquadrados como MEI, bem como das demais naturezas jurídicas (no que diz respeito à inscrição fiscal no Estado, na prefeitura municipal e em outros órgãos e entidades) depende da legislação de cada Estado e Município. Mas algumas obrigações são comuns às leis das unidades federativas. É preciso ter registro na prefeitura ou na administração regional da cidade onde ela vai funcionar, no Estado, na Receita Federal e na Previdência Social (INSS - Instituto Nacional do Seguro Social).

Dependendo da atividade, pode ser necessário também o registro na Entidade de Classe, na Secretaria de Meio-Ambiente e em outros órgãos de fiscalização.

Toda empresa, obrigatoriamente, tem uma única e exclusiva **razão social**.

Razão social, denominação social ou firma empresarial é o nome constante do registro da empresa; ou seja, é o nome dado à pessoa jurídica, que consta em documentos legais ou oficiais, contrato social, notas fiscais

emitidas e recebidas, contratos em geral, escrituras e outros tipos de documentos, tal como o nome civil da pessoa física é o que consta de sua Certidão de Nascimento e é utilizado em todos os seus documentos, formalidades e contratos. Em regra (na maioria das vezes) a razão social é constituída de três partes: uma designação específica fruto da criatividade, o ramo principal de atividade e o enquadramento fiscal ou tipo societário da empresa. Infra alguns exemplos das terminações (parte final) de uma razão social:

- Ltda. - Abreviação de "limitada", quando há um número limitado de sócios;

- S.A. - Abreviação de "sociedade anônima", aplicado para empresas de capital aberto, ou seja, negociados em bolsa de valores;

- EPP - Abreviação de "Empresa de Pequeno Porte", obrigatório para as "limitadas" optantes pelo Simples (faturamento entre R$ 120 mil e R$ 1,2 milhão por ano-calendário fiscal);

- ME - Abreviação de "Microempresa", obrigatório para as optantes pelo Simples (faturamento menor do que R$ 120 mil por ano-calendário fiscal);

- MEI - Abreviação de microempreendedor individual, para quem registra o CNPJ nesse enquadramento, com faturamento de até R$ 60 mil por ano.

Portanto, antes da definição da razão social urge saber qual será: a) setor ou ramo de atividade (comercial, industrial, rural, prestação de serviços, etc.); b) o tipo societário ou forma jurídica (empresário, sociedade comercial, sociedade civil, sociedade limitada, sociedade anônima, EIRELI, cooperativa, etc.); c) o porte ou tamanho levando-se em conta o faturamento (receita bruta) e o número de empregados (MEI - Microempreendedor Individual, ME - Microempresa, EPP - Empresa de Pequeno Porte, etc.); e d) qual será o regime tributário (Lucro Real, Lucro Presumido, Simples Nacional, etc.); vez que tais questões interferem na formação da razão

social, chegando ao ponto de até impor que a razão social seja o nome civil (firma individual), completo ou abreviado, do empresário (individual) seguido do seu CPF. Ainda mais, alguns desses itens restringe ou repercute em outro item.

- http://www.institucional.jucesp.sp.gov.br/downloads/guia_basico_colidencia_jan2012.pdf;
- https://www.juntacomercial.pr.gov.br/arquivos/File/legislacao/in_116_2011.pdf.

Já o **nome fantasia**, nome comercial ou nome de fachada é o nome popular, nome social ou nome de guerra da empresa, tal como um apelido, podendo ser a própria razão social ou uma abreviação desta; bem como pode ser totalmente diferente. A finalidade do nome fantasia é facilitar a divulgação, a cativação e a memorização do nome da empresa e dos seus produtos e/ou serviços. Detalhe, é possível registrar um nome fantasia no contrato social, na Junta Comercial e no cartório. Entretanto, para fins de marca registrada (registro de propriedade intelectual), deve ser registrado junto ao INPI — Instituto Nacional da Propriedade Industrial (http://www.inpi.gov.br/).

Outro detalhe é a necessidade de pesquisa prévia do nome empresarial na junta comercial para saber se alguém já é titular desse nome; já em relação ao nome fantasia, no INPI, tal pesquisa não precisa ser prévia. Também é importante a verificação na prefeitura municipal sobre a possibilidade de exercício da atividade desejada no endereço almejado.

Algumas juntas comerciais e cartórios de pessoas jurídicas possuem convênio com a Receita Federal e fazem a emissão do CNPJ integrada com o registro da empresa.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/cartorios-de-registro-civil-das-pessoas-juridicas-conveniados-para-inscricao-no-cnpj/relacao-de-cartorios-conveniados-1/relacao-de-cartorios-conveniados.

Em se tratando de **empresário individual**, não existem duas pessoas (uma física e outra jurídica) dotadas dos seus respectivos patrimônios. Explica-se. O comerciante individual, também conhecido como empresário individual ou

firma individual, não é pessoa jurídica (é incorreto, pois, o termo: “pessoa jurídica individual”); mas sim, mera pessoa física que exerce o comércio. Portanto, o empresário individual não é pessoa jurídica apesar de possuir CNPJ. Ele apenas é equiparado à pessoa jurídica para fins de facilitação para a prática dos atos da empresa. Portanto, empresário individual é pessoa física; logo, o seu patrimônio pessoal, em sua totalidade se confunde com o empresarial e por conta disso responde ilimitadamente pelos débitos do empresário. Dessa forma, o CNPJ do empresário individual tem o condão exclusivo de equiparação à legislação tributária.

O empresário individual que exerce atividade econômica em nome próprio e, por isso, tem sua firma individual arquivada na Junta Comercial e se inscreve no CNPJ/MF não é pessoa jurídica; mas, pura e simplesmente a ela é equiparado pela legislação do imposto de renda. Não há autonomia jurídica e nem exsurge personalidade jurídica individual; pois o empresário individual é pessoa natural que exerce a atividade empresarial em nome próprio. Portanto, empresário é a própria figura do empreendedor que se registra no órgão público (Junta Comercial). Isto é, exerce os negócios em seu próprio nome. É o próprio sujeito de direitos e obrigações no exercício das atividades econômicas.

A figura do empresário individual é pessoa natural, sendo a sua "personalidade jurídica" mera ficção do direito tributário. O CNPJ é apenas um cadastro fiscal do Ministério da Fazenda. Muitos entes despersonalizados possuem CNPJ porque são equiparados a uma pessoa jurídica, apenas para fins fiscais. Só isso.

Recorda-se que os sócios de uma sociedade empresária não são empresários. Quando pessoas naturais unem seus esforços para, em sociedade, ganhar dinheiro com a exploração empresarial de uma atividade econômica, elas não se tornam empresárias. A sociedade por elas constituída, uma pessoa jurídica com personalidade autônoma, sujeito de direito independente, é que será empresária, para todos os efeitos legais. Os sócios da sociedade empresária são empreendedores ou investidores, de acordo com a colaboração dada à sociedade (os empreendedores, além de capital, costumam devotar, também, trabalho à pessoa jurídica, na condição de seus administradores, ou as controlam).

A circunstância de constar ao lado da firma individual a indicação “ME” (Microempresa) indica apenas que se trata de microempresa. Microempresa é tão somente regime tributário facultado às empresas (firma individuais ou pessoas jurídicas) que tenham auferido Faturamento Bruto Anual não superior a um determinado teto. Praticamente, qualquer tipo empresarial mercantil (exceto as Sociedades Anônimas e Comandita por Ações), que esteja dentro do faturamento previsto em lei, inclusive o Empresário Individual, poderão se enquadrar como Microempresa. Não há, portanto, porque se confundir microempresa com empresário individual.

ME é a sigla para Microempresa; ou seja, empreendimentos que visam o lucro e que apresentam um faturamento anual de até R$ 360.000,00. (Lei Complementar 123/2006, artigo 3º, inciso I). Ressalta-se que o único critério é simplesmente o faturamento do empreendimento. E o enquadramento é efetuado mediante declaração para essa finalidade (Instrução Normativa n° 103/2007, revogada pela Instrução Normativa DREI 11/2013). Por outras palavras, ME não é tipo societário ou de empresa, mas meramente a quantidade (porte) de faturamento do empreendimento.

- Lei Complementar 123/2006 - http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp123.htm;

- http://drei.smpe.gov.br/legislacao/instrucoes-normativas/titulo-menu/pasta-instrucoes-normativas-em-vigor-05/in_11_2013.pdf.

Urge apontar as diferenças entre **Eireli** (Empresário Individual de Responsabilidade limitada) e empresário individual. O Eireli está previsto no Código Civil (CC), artigo 980-A enquanto que o empresário individual está definido no artigo 966 do Código Civil. A pessoa física que exerce atividade econômica sem sócios pode abrir uma Eireli. A principal diferença é que em caso de dívidas, o patrimônio pessoal do empresário não será usado para o cumprimento das obrigações. Resumindo, há uma separação dos bens pessoais dos da empresa. O capital social mínimo exigido para a abertura de uma Eireli é de 100 (cem) salários mínimos. Assim como na Eireli, a pessoa física (empresário individual) não precisa de sócios para abrir a sua empresa. Porém, em caso de dívidas, seus bens privados serão usados para os devidos pagamentos aos credores. Isso

também vale para dívidas pessoais, em que bens da empresa podem ser usados para quitá-las. Se o empresário for casado em comunhão de bens, os bens do seu cônjuge também podem servir como pagamento.

- Código Civil - http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

Empresário Individual e EIRELI (Empresa Individual de Responsabilidade Limitada) são semelhantes; ou seja, são naturezas jurídicas que possuem apenas um titular. Entretanto, para se constituir EIRELI (Código Civil, artigo 980-A introduzido pela Lei 12.441/2011) é necessário que a empresa tenha no mínimo um capital social de 100 (cem) vezes o salário mínimo vigente. Portanto, as grandes diferenças são que a Eireli deverá subscrever um capital social mínimo para sua constituição e pode ser constituída por uma pessoa jurídica; enquanto que o empresário individual é, sempre, uma pessoa física. Ainda mais, o titular de uma EIRELI respondera limitadamente pelas obrigações da pessoa jurídica, ao passo que o empresário individual responde de forma ilimitada. Frisa-se, ainda, que a Lei 12.441/2011 admite a transformação do empresário individual em EIRELI, e vice-versa (artigos 980-A, §3º, 1.033, parágrafo único, e 1.113 a 1.115, todos do Código Civil).

Outro detalhe é a verificação das hipóteses existentes para o caso concreto de quais regimes tributários é possível enquadrar a empresa; ou seja, normalmente há mais de uma opção de enquadramento a critério do empresário e outras opções exigem certos requisitos além da manifestação do empresário.

Se a previsão de faturamento anual da empresa é menor que R$ 60.000,00 e o titular não faz parte de nenhuma outra empresa, provavelmente será um **MEI** (Microempreendedor Individual) e pode seguir um procedimento mais simples para se inscrever no CNPJ; o que garante outros benefícios como: isenção de taxas para registrar a empresa; direito à aposentadoria; facilitação com burocracias; contratação de funcionário com custo menor; redução da carga tributária; etc.

- http://www.portaldoempreendedor.gov.br/mei-microempreendedor-individual.

O MEI (Microempreendedor Individual), na condição de empresário individual, que é por força da LC (Lei Complementar) 128/2008, é pessoa física e não jurídica.

- Lei Complementar 128/08 - http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp128.htm.

O **Simples Nacional** ou Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte (http://www8.receita.fazenda.gov.br/SimplesNacional/), previsto na LC (Lei Complementar) nº 123/2006, é um regime compartilhado (União, Estados, Distrito Federal e Municípios) de arrecadação, cobrança e fiscalização de tributos (IRPJ, CSLL, PIS/Pasep, Cofins, IPI, ICMS, ISS e a Contribuição para a Seguridade Social – CPP) aplicável às Microempresas e Empresas de Pequeno Porte.

O **e-CNPJ** é a versão eletrônica do CNPJ, que garante a autenticidade e a integridade nas transações eletrônicas de pessoas jurídicas.

O interessado na obtenção de um certificado digital (e-CPF ou e-CNPJ) deverá contatar uma das Autoridades Certificadoras Habilitadas (confira supra sobre o e-CPF).

- http://www.iti.gov.br/index.php/certificacao-digital/como-obter;
- http://www.iti.gov.br/icp-brasil/estrutura;
- https://www.certisign.com.br/certificado-digital/para-empresa/ecnpj/documentos-necessarios-pj.

A pessoa jurídica estrangeira deverá indicar procurador residente no Brasil para figurar como responsável perante o CNPJ, bem como comunicar alterações referentes a dados cadastrais no prazo de 30 dias da alteração (IN SRF nº 1634/2016).

- http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=73658#1624555.

O investidor não residente pessoa jurídica obtém o CNPJ a partir do seu cadastramento no Sisbacen. Verificada a sua conformidade pelo Banco

Central, os dados são enviados à Receita Federal do Brasil, que atribui um número de CNPJ ao seu titular e o retorna ao Banco Central. Excetuam-se os casos de fundos de investimento constituídos no exterior e de pessoas jurídicas domiciliadas no exterior que possuam no Brasil, exclusivamente, aplicações no mercado financeiro e aplicações no mercado de capitais, que devem observar o disposto na regulamentação da Receita Federal do Brasil para obtenção do CNPJ.

- http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastro-nacional-de-pessoas-juridicas-cnpj/solicitacao-de-atos-perante-o-cnpj-por-meio-da-internet/orientacoes-para-pessoa-juridica-domiciliada-no-exterior;
- http://www.apexbrasil.com.br/como-estabelecer-uma-empresa-no-brasil;
- http://www.bernhoeft.com.br/empresa-estrangeira-no-brasil/.

Obtido o CNPJ, o próximo passo, no caso de empresa com atividade de prestação de serviços, é fazer a inscrição fiscal na Secretaria de Finanças do município. Normalmente, essa inscrição é solicitada em conjunto com o a emissão alvará de funcionamento.

O **alvará** é uma licença que permite o funcionamento de empresas comerciais, industriais, agrícolas e prestadoras de serviços; bem como de sociedade e associações de qualquer natureza. Este documento deve ser solicitado à prefeitura municipal ou à administração regional de cada município. Para a concessão do alvará é necessário que a atividade possa ser exercida no endereço da empresa, em conformidade com o código de posturas (Lei Orgânica ou alguma lei específica) do município. Conforme a natureza de cada atividade, a concessão do alvará de funcionamento pode exigir licenças do Corpo de Bombeiros, da Vigilância Sanitária, do Meio Ambiente e outros órgãos de segurança e fiscalização.

A **Inscrição Estadual** é obrigatória para empresas dos setores do comércio, indústria e serviços de transporte intermunicipal e interestadual, de comunicação e de energia, é necessária para obtenção da inscrição no ICMS (Imposto sobre Circulação de Mercadorias e Serviços). O cadastro no sistema tributário estadual deve ser feito junto à Secretaria Estadual da Fazenda. Atualmente alguns Estados possuem convênio com a Receita Federal que permite obter a Inscrição Estadual junto com o CNPJ por meio

de um único cadastro. Em alguns Estados, a inscrição estadual deve ser solicitada antes do alvará de funcionamento.

Toda empresa precisa estar cadastrada na **Previdência Social** e pagar os respectivos tributos, mesmo que não possua funcionários e tenha apenas os sócios. Para solicitar o cadastro, o representante deve dirigir-se à Agência da Previdência da jurisdição (área territorial) e solicitar o cadastramento da empresa e de seus responsáveis legais. O prazo para o cadastramento é de 30 dias após o início das atividades.

Por fim, resta solicitar a autorização para impressão de notas fiscais e autenticação de livros fiscais. Isto é feito na prefeitura municipal de cada cidade. Empresas com atividades na indústria e comércio deverão ir à Secretaria de Estado da Fazenda. Estados que têm nota fiscal eletrônica não precisam do aparato fiscal. Basta obter uma senha eletrônica (na própria Prefeitura) e a empresa já estará apta a emitir notas fiscais.

A legislação brasileira já é extensa, dispersa, burocrática, complexa, instável, problemática, emaranhada, confusa e, muitas vezes, incompreensível até mesmo para os próprios cidadãos nativos, quanto mais para os estrangeiros. Por essa razão, é altamente recomendável, praticamente indispensável, a contratação de profissionais, principalmente advogado e contador, para que não se cometa erros e sofre as consequências deles.

- http://www.paineldecontrolefinanceiro.com.br/;
- http://www.tributarioexpert.com.br/EbookDeSTDA
- http://tributarioexpert.com.br/manual-nfe;
- http://biblioteca.fbtedu.com.br/compliance;
- http://conteudo.myrp.com.br/ebook-impostos-para-micro-e-pequenas-empresas;
- http://www.valortributario.com.br/download.asp;
- http://www.administradores.com.br/noticias/carreira/20-livros-de-administracao-para-baixar-gratis/109547/.

FORMAS DE PAGAMENTOS ATUAIS

Atualmente, é muito frequente ou bastante popular o uso de meios de pagamento eletrônicos (cartão de crédito, cartão de débito automático, cartões “inteligentes”, telefone celular, etc.), favorecidos pela evolução tecnológica da computação e da telecomunicação. Essas novas formas de dinheiro eletrônico ganharam impulso com a criação da Internet, que permite a realização de compras via computador, debitando-se os respectivos custos em cartões de crédito ou diretamente na conta bancária do usuário.

Estamos vivenciando uma geração mais jovem se voltando rapidamente para a moeda eletrônica muito mais rápido do que as gerações mais velhas ainda possam pensar que fosse possível.

O dinheiro variou muito ao longo dos séculos. Já existiram muitos tipos de dinheiro. O mais familiar é a moeda; ou seja, um pedaço padronizado de metal gravado. No entanto, já existia dinheiro muito antes da invenção da cunhagem e as culturas prosperaram usando outras coisas como moeda. Desde a invenção do escambo até hoje desenvolveu-se um longo e progressivo processo de desmaterialização da moeda; ou seja, foi perdendo o seu conteúdo material. Assim após ter tido identidade, forma e valor próprios, posteriormente, passou a ser meros registos contabilísticos, efetuados pelos bancos, da circulação dos depósitos (moeda escritural).

A evolução das formas de moeda está vinculada ao aspecto intrínseco de que novas formas são adotadas por tornarem mais fáceis as transações entre os agentes econômicos. Desde seu surgimento até as modalidades atualmente existentes, as transformações da moeda estiveram vinculadas ao aspecto da redução dos custos de transação. Portanto, o incremento das trocas e o desenvolvimento da atividade econômica são responsáveis pelo progressivo recurso à moeda escritural, que torna o processo de transação fácil e mais rápido. Diante disso, atualmente enormes quantias circulam entre contas bancárias, no mesmo país ou entre países, através de meios eletrônicos (movimentação contabilística dos depósitos bancários por via informática); o que constituiu mais um passo no processo de desmaterialização da moeda.

Atualmente o uso do dinheiro em pecúnia (cédulas) é muito reduzido, tendo sido substituído pelo cheque, depois pelos cartões de débitos e créditos, pelo *home banking* (pagamentos e transferências pela Internet) e através de DOC (Documento de Ordem de Crédito) e TED (Transferência Eletrônica Disponível).

Os bancos comerciais literalmente criam continuamente moeda para empréstimos. Eles fazem isso simplesmente inserindo dígitos (créditos) nos saldos das contas bancárias de tomadores de empréstimos; os quais, então, gastam-nas como se fossem papel-moeda real. Hoje a grande maioria de todo o dinheiro existe apenas como meros números em contas bancárias. Assim, os bancos criam dinheiro a partir do nada ao simplesmente digitarem números como saldos ou créditos aos seus clientes. Explica-se. O banco não tem o correspondente dinheiro físico que emprestou. Quando o tomador do empréstimo gasta a quantia recebida como dígitos em sua conta, o banco priorizará o pagamento através de dígitos e, quando não poder fazê-lo assim, utilizará o dinheiro físico dos clientes. Em conclusão, se todos os cientes solicitarem do banco seus créditos/saldos em dinheiro físico, o banco somente conseguirá atender cerca de 10% deles; vez que os créditos que os bancos concedem a seus clientes não possuem lastro nenhum (não há nenhum equivalente ou reserva em dinheiro físico; muito menos em ouro). Como o dinheiro não precisa estar totalmente garantido nos cofres do banco, eles o emprestam a quem precisa, mas mantém nos registros. Isso é a moeda escritural, e é para evitar a criação descontrolada de dinheiro que o governo impõe o depósito compulsório.

Os **cartões de débitos e créditos** evoluíram para meras informações (nome do titular, número do cartão, data de validade e código de segurança) dispensando, na prática, a apresentação ou porte do cartão físico.

- https://www.paypal.com/br/home;
- http://bcash.com.br/;
- https://pagseguro.uol.com.br/;
- https://moip.com.br/;
- http://www.ipag.com.br/;

- http://payu.com.br/;
- http://www.authorize.net/
- https://stripe.com/;
- https://payments.amazon.com/home;
- https://moeda.digital/;
- http://www.stelo.com.br/;
- http://www.poprecarga.com.br/.

Com o desenvolvimento da tecnologia da informação e da computação, estamos entrando num novo estágio de uma nova evolução mundial de sistemas de pagamento e de recebimento.

A FICÇÃO SE TORNOU REALIDADE

O filme "De Volta Para o Futuro 2" ("Back to the Future - Part II"), lançado em 14/12/1989, colocou os protagonistas em uma viagem no tempo para 21/10/2015, em um cenário que buscou antecipar invenções que ocorreriam nas décadas seguintes. E aquele mundo utópico futurista está tomando forma e se tornado realidade. Boa parte do mundo de Marty McFly já faz parte do dia a dia de muita gente ou estará no mercado em breve.

Em um mundo onde o PC doméstico estava começando a engatinhar, o filme "De Volta para o Futuro 2" foi além. Em 1989 era praticamente impossível imaginar um computador leve, de finíssima espessura e que coubesse na palma da mão. O filme previu tudo isso, mas sem saber que eles se chamariam *tablets* ou iPads, ou que poderiam ter tamanho reduzido para caber na bolsa (como *notebooks* e *netbooks*). *Tablets* já existem há mais de 10 (dez) anos (http://www.blogdopaz.com.br/a-incrivel-historia-da-invencao-dos-tablets/), mas foi em 2010, com o lançamento do iPad, que a indústria cresceu e se tornou parte do desejo popular, trazendo à tona dezenas de fabricantes especializados nesse tipo de aparelho.

- *Smartphone* é um termo de origem inglesa que significa “telefone inteligente”. Trata-se de um aparelho de telefonia celular (telemóvel) com características de computador (possui agenda de contatos, sistema operacional multitarefa e multimídia, acesso à Internet, sincronismo de dados com o computador, vários aplicativos através do Google Play, Windows Store, App Store, etc.). As marcas mais conhecidas são o Iphone da Apple, BlackBerry e o Android da Google. Esclarece-se, assim, que um aparelho de celular comum, apesar de alguns modelos acessarem a Internet e possuírem recursos modernos (teclado Qwerty, *touch screen*, câmera, bluetooth, reprodução de MP3, rádio FM, etc.), ele não tem sistema operacional, possuindo interfaces simples, limitadas às funções básicas do aparelho; não lhe sendo possível instalar novos programas para aumentar as suas funcionalidades básicas.

- *Touch screen* significa “tela sensível ao toque”. Desse modo, a tecnologia *touch screen* reconhece a presença e a localização do toque feito na superfície de um display eletrônico e, consequentemente, transmite essa informação para que seja executada a tarefa pretendida.

- *Bluetooth* é uma tecnologia de comunicação sem fio, a partir de ondas de rádio, desenvolvida em 1994 pela empresa de telecomunicações Ericsson, que permite que equipamentos se conectem e troquem dados e arquivos entre si.

- *Tablet* é um tipo de computador portátil, de tamanho pequeno, fina espessura e com tela sensível ao toque (“touch screen”). É um dispositivo prático com uso semelhante a um computador portátil convencional.

- *Notebook* (ou *laptop*) é um computador portátil, leve, projetado para ser transportado e utilizado em diferentes lugares com facilidade.

- *Netbook* é uma versão menor de *notebook*, mais leve, barata e otimizada para o acesso à Internet.

Na década de 1980 a Geração Y presenciou os maiores avanços na tecnologia e diversas quebras de paradigma do mercado de trabalho. Entretanto, enquanto que a geração anterior (X) foi concebida na transição para o novo mundo tecnológico, a geração Y foi a primeira verdadeiramente nascida neste meio, mesmo que incipiente. A Geração X é formada pelos filhos da Geração "Baby Boomers" ("Explosão de Bebês" ou explosão populacional), formada logo após a Segunda Guerra Mundial (nascidos entre a década de 1950 e 1960) e pelos pais da Geração Y. Enquanto a Geração "Baby Boomer" se apresenta como contemporânea ao nascimento da tecnologia, a Geração X surgiu já fazendo uso dos recursos tecnológicos promovidos por sua geração precursora.

Durante os anos 1990, as tecnologias criadas na década de 1980 foram aperfeiçoadas e popularizadas, entre elas, o computador, a Internet e o

telefone celular. A geração que nasceu a partir de 1995 (data do nascimento da Internet no Brasil), conhecida por Y (ou "After Eighty", "Post-80" ou pós 80), não conheceu o mundo sem Internet, celular ou televisão e querem tudo para agora. São pessoas que já cresceram inseridas nesse contexto tecnológico e de Internet.

Os nascidos a partir do ano 2000, são conhecidos como nativos digitais (ou geração Z) por estarem conectados ("on line") o tempo todo. Foram influenciadas desde crianças pelo mundo complexo e veloz que a tecnologia engendrou. E, cada vez mais, a idade em que a criança ganha seu primeiro *tablet* e/ou *smartphone* é cada vez mais precoce. É a geração da interatividade, da conectividade, da portabilidade, da simplificação tecnológica, da mídia digital. Possuem acesso muito fácil à informação, o que os coloca um passo à frente dos mais velhos, concentrados em adaptar-se aos novos tempos.

O número de crianças que desde cedo já sabem usar um celular e computadores de última geração é cada vez maior, parece que elas já nascem sabendo administrar esses utensílios melhor do que as gerações passadas que fizeram o uso de cursos de informática para se adaptar a esta nova era que estava chegando e não ficar obsoleto.

Já estamos ultrapassando a geração Alpha ("Alpha generation"), que é formada pelos que nasceram depois do ano 2010. A grande diferença entre a nova geração e a Z (nascidos nos anos 90) é a interação com a tecnologia desde o nascimento. Quem nunca viu um bebê que mal ainda mexer com a maior naturalidade num *smartphone*?

Faz décadas que as crianças (que cresceram, entraram na puberdade, viraram adolescentes, ficaram adultas e tiveram filhos e até netos) estão habituadas com o manuseio diário e constante de videogames modernos, computadores, *notebooks*, *tablets*, *smartphones* e a Internet. A máquina de escrever, o mimeógrafo, a vitrola, o disco de vinil (LP – *Long Play*), o videocassete, a fita cassete, a fita VHS, o CD, o DVD, o aparelho despertador, o rádio relógio, a agenda eletrônica, o *walkman*, o *discman*, o pager/bip, Mini e Micro Systems, o fax, o uso de papel e, até mesmo, a letra manuscrita e o uso de carteira convencional são coisas do passado, de

saudosistas e de idosos. A ficção científica já virou realidade. O futuro já chegou. Atualmente é tudo cada vez mais eletrônico e *on line* ("em linha", ou seja, conectado a computadores em tempo real).

A tendência é dos cartões bancários, de débito e de crédito e, inclusive dos bancos e do próprio dinheiro, serem gradualmente substituídos por **meios eletrônicos *on line***.

Já não é de hoje, mas já faz bastante tempo, que os bancos e demais instituições financeiras adotaram a política de cada vez mais recomendarem, estimularem, incentivarem, promoverem, pressionarem e, até mesmo, coagirem os seus clientes e demais usuários de seus serviços a não utilizarem de intermediação humana (funcionários dos bancos e financeiras) para os atendimentos e realização de operações; mas, pelo contrário, passarem a usarem, com cada vez mais frequência, as opções de auto atendimento, tais como, por exemplos, caixas eletrônicos e *home banking*.

> ***Remote Banking*** são os serviços que os bancos oferecem além de sua estrutura física, ou seja, é todo e qualquer serviço prestado fora do ambiente da agência com intuito de facilitar a vida do cliente e diminuir o uso de filas, como, por exemplo, os caixas eletrônicos 24 horas.
>
> ***Home Banking*** são os serviços oferecidos pelos bancos e instituições financeiras através da internet e do telefone para as pessoas físicas. Já o *Office Banking* é a mesma coisa, só que destinado às pessoas jurídicas (empresas).
>
> ***Internet Banking*** ou *e-banking* é o banco online. Através dele se faz operações (consulta saldo e faz pagamentos, transferências, investimentos, etc.) sem ter de ir até uma agência bancária.
>
> Veja Banco Digital.

Enquanto que em 1996 apenas alguns pioneiros se arriscavam a oferecer serviços bancários através da Internet, hoje milhões de usuários no mundo todo transformaram o *Internet banking* numa das aplicações de maior sucesso no universo do comércio eletrônico.

O Bradesco foi o primeiro site “.com” do Brasil e o primeiro banco no Brasil a disponibilizar o saldo dos clientes pela Internet.

Das iniciais consultas a informações de saldo e extrato de contas bancárias, em pouco tempo o *Internet banking* evoluiu para oferecer uma gama de serviços crescente. Transferência de fundos e pagamento de contas foram seguidos por aplicações e resgates de investimentos, solicitações de crédito, desbloqueio de talões de cheques, solicitação de cartões e outros serviços, além de extratos por e-mail, renovação de crédito para telefones celulares, são serviços cada vez mais comuns no ambiente de *Internet banking*.

Em 2003, a parte mais significativa dos serviços nas agências bancárias já estava disponível nos sites dos bancos. O Brasil já se consolidou como um dos principais países na utilização do *Internet banking*, rivalizando e mesmo superando países com grande tradição de uso de tecnologia bancária. Todos os grandes bancos do país já possuem sites que, mais do que uma vasta diversidade de serviços, atendem a uma enorme parcela dos seus clientes pela Web.

Com a disponibilização da Internet para uso civil ocorreu o “boom” (enorme crescimento) das lojas virtuais, com o que surgiu a necessidade de pagamentos *on line* (em tempo real) para melhor atender esse tipo de negócio (vendas e compras *on line*). Por outras palavras, passou a existir a demanda (necessidade) no mercado e os bancos não podiam “nadar contra a maré” ou se manterem parados no tempo exigindo que os pagamentos fossem feitos através de boletos do modo convencional (numa agência bancária física ou num caixa eletrônico) ou, no máximo, por cartão de crédito. Desse modo, os pagamentos *on line* passaram a ser realidade há muito tempo.

Além do conhecido Paypal (https://www.paypal.com/br/home) e outros similares, há, ainda, o Amazon Payments (https://payments.amazon.com/) que efetua pagamentos internacionais através das informações do cliente que estão armazenadas na conta do Amazon.

Da demanda gerada pelo comércio eletrônico, surgiram serviços e empresas especializadas, tais como, por exemplos:

- F2b (https://www.f2b.com.br/);
- Mercado Livre (http://www.mercadolivre.com.br/);
- Mercado Pago (https://www.mercadopago.com.br/);
- PagSeguro (https://pagseguro.uol.com.br/);
- Pagamento Digital (https://blog.bcash.com.br/pagamento-online/);
- Bcash (http://bcash.com.br/);
- PayU (http://www.payu.com.br/);
- PayPal (https://www.paypal.com/br/webapps/mpp/home);
- pagar.me (https://pagar.me/);
- Moip (https://moip.com.br/);
- MundiPagg (http://www.mundipagg.com.br/);
- ClearSale (http://portal.clearsale.com.br/);
- Buscapé (http://www.buscape.com.br/);
- Adyen (https://www.adyen.com/pt_BR/);
- Rede (https://www.userede.com.br/);
- Stone (http://www.stone.com.br/);
- Stelo (http://www.stelo.com.br/);
- Cielo (https://www.cielo.com.br/solucoes-de-pagamentos/solucoes-para-e-commerce/index.html);
- Agência SI (http://www.agenciasi.com.br/);
- Vindi (https://www.vindi.com.br/);
- Adyen (https://www.adyen.com/pt_BR/).

Atualmente, além dos bancos e financeiras terem aumento a pressão para os seus clientes e usuários efetuarem as operações sozinhos pelo autoatendimento nos caixas eletrônicos, eles não querem nem mais que as pessoas se dirijam à uma agência bancária ou unidade física da instituição financeira.

Explica-se. Primeiramente os bancos queriam reduzir as despesas com funcionários e o tamanho das agências bancárias resultantes do atendimento pessoal. Assim passaram a “empurrar” as pessoas para os caixas eletrônicos. Agora, eles não querem nem ter as despesas com os caixas eletrônicos (os quais, aliás, estão sendo objeto de constantes furtos) e, muito menos, com a enorme quantidade de agências bancárias físicas. Por outras palavras, de forma semelhante ao que aconteceu com as lojas físicas que passaram a ser lojas virtuais para diminuírem as despesas (aluguel, IPTU, energia elétrica, água e esgoto, limpeza, segurança, seguro, funcionários, móveis, equipamentos, etc.) e prestarem um serviço melhor e mais barato

aos seus clientes, os bancos pretendem reduzir ao mínimo possível a quantidade de agências físicas.

Para os clientes, o uso do *Internet banking*, além da conveniência do acesso a qualquer hora e de qualquer lugar, oferece as vantagens de concentrar uma grande diversidade de serviços que podem ser realizados com relativa rapidez pelo próprio cliente, de acordo com as suas necessidades. Em alguns casos, a vantagem da redução de custos obtida pelos bancos é repassada para os clientes através da tarifa dos serviços mais barata pela Internet do que por outros canais.

Recordemos o exemplo da tradicional (desde 1936) revista (*magazine*) semanal americana Life (http://time.com/life/), que em 20/04/2007 teve sua última edição impressa (ou *off line*). Melhor ainda. Recordemos as extintas videolocadoras, os locais onde, antigamente, se comprava e aluga vídeos. No início os filmes eram em fitas VHS, depois passaram a ser em DVD e, pouco antes do fim, eram no formato Blu-ray. Um marco dessa extinção, foi a grande divulgação, recheada de drama, que a mídia/imprensa deu aos fechamentos gradativos das lojas da Starbucks. Atualmente, locação de filmes é praticamente somente on line ou via satélite.

Outro exemplo evolutivo é o Judiciário. Os processos judiciais que eram efetivados através de milhões de toneladas de papéis, passaram a ser de forma digital on line. A implantação do processo eletrônico começou no ano de 2006 e, em 2007, foi iniciada a tramitação eletrônica de processos judiciais no STF – Supremo Tribunal Federal (http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=156088&modo=cms).

A revista VEJA (http://veja.abril.com.br/), em processo de migração, faz anos que possui muito conteúdo online e, recentemente, lançou o *Mobile View*; um sistema de interação que soma o conteúdo impresso ao digital. Apontando a câmera de um celular ou tablet para as páginas da revista, o leitor terá acesso a conteúdos digitais exclusivos. São vídeos e galerias de fotos e áudios que complementarão as reportagens em todas as edições da revista.

- http://veja.abril.com.br/tecnologia/muito-alem-do-real/;
- http://veja.abril.com.br/tecnologia/mobile-view-um-novo-jeito-de-desfrutar-de-veja/;
- http://veja.abril.com.br/tecnologia/aprenda-a-utilizar-o-mobile-view-o-novo-recurso-de-veja/.

Outra recordação. Em 2010 foi a última vez em que o IRPF (Imposto de Renda da Pessoa Física) pode ser feito através de formulário de papel. Assim, desde 2011, todas as declarações de imposto de renda no Brasil passaram a serem recebidas pela Receita Federal apenas por meio eletrônico (via Internet). No mesmo caminho foram todas as outras declarações e documentos que devem ser entregues à Receita Federal. Na mesma trilha estão terminando de serem totalmente digitais as notas fiscais, os cupons fiscais, os conhecimentos de transportes, os títulos de créditos e até os processos judiciais.

No filme de 1968, "2001 - Uma Odisseia no Espaço" ("2001: A Space Odyssey") e vários outros posteriores semelhantes, já está passando de ficção para a realidade; ou seja, já podemos **conversar com as máquinas** como o super-herói, "homem de ferro", faz com seu assistente virtual, o Jarvis. Por outras palavras, já fazem alguns anos que a inteligência artificial é realidade.

- http://olhardigital.uol.com.br/noticia/veja-como-funciona-jarvis-a-inteligencia-artificial-criada-por-mark-zuckerberg/64802;
- http://www.techtudo.com.br/noticias/noticia/2016/12/mark-zuckerberg-apresenta-jarvis-inteligencia-artificial-para-casas.html;
- http://exame.abril.com.br/tecnologia/google-cria-assistente-virtual-com-inteligencia-artificial/;
- https://www.tecmundo.com.br/internet-das-coisas/94450-empresa-japonesa-cria-assistente-virtual-ia-forma-holograma.htm;
- http://smartmundo.com/siri-cortana-google-now-assistentes-virtuais/;
- http://targethd.net/samsung-galaxy-s8-tera-um-assistente-virtual-com-inteligencia-artificial/;
- http://escreveassim.com.br/2013/09/17/speaktoit-o-assistente-virtual-android/.

Bot*, abreviação de *robot, são *softwares* com função de simularem o comportamento humano a partir de uma inteligência cognitiva, por exemplo, servindo de usuários falsos em redes sociais para aumentar o número de seguidores, visualizações, curtidas, compartilhamentos e comentários. Os *bots* são sistemas de automação desenvolvidos também para atuarem em sites, programas e *apps* (aplicativos), interagindo com os visitantes e usuários. Exemplos comuns são os "mascotes" dos recursos de ajuda dos *softwares*; dos atendentes, vendedores ou assistentes virtuais nas lojas virtuais; e, dos moderadores robóticos e *chatbots* (exemplos, empresas Movile, Elo7 e Take.net) em redes sociais, salas de bate-papo e aplicativos de comunicação instantânea. Os *bots* poderão substituir as centrais telefônicas 0800 para oferecerem soluções mais rápidas a problemas que não podem esperar e que não requerem a ajuda de um humano. Não confundir com **"boot"** que é o processo de inicialização de um computador, o qual acontece no momento em que você pressiona o botão "Ligar" da máquina até o total carregamento do sistema operacional instalado.

- http://portalpublicitario.blog.br/conheca-o-seu-proximo-melhor-amigo-os-bots/;
- http://olhardigital.uol.com.br/noticia/conheca-o-murphy-o-novo-bot-da-microsoft/61079;
- http://www.buzzmonitor.com.br/blog/conheca-o-primeiro-bot-para-facebook-ads;
- http://www.tudocelular.com/tech/noticias/n75686/kip-novo-bot-messenger.html;
- http://www.b9.com.br/64090/tech/conheca-tay-o-bot-de-twitter-que-usa-inteligencia-artificial-da-microsoft-para-conversar/;
- https://palcodj.com/2016/06/19/dj-bot-esta-no-ar-conheca-o-primeiro-robo-do-messenger-especialista-em-djs-e-edm/;
- http://eusouandroid.com/dica-conhea-melhor-o-telegram-seus-bots-e-bots-em-lua/.

Melhor ainda que os *bots*, a Microsoft já fornece a Cortana (https://developer.microsoft.com/pt-br/cortana) e, a Apple, o Siri (http://www.apple.com/br/ios/siri/). E, faz muito tempo, que é possível realizar pesquisas na Internet, através de computadores, *smartphones* ou *tablets* através de comando de voz

(https://support.google.com/websearch/answer/2940021?hl=pt-BR&ref_topic=3378866).

O Google aposta numa nova forma de pagar as compras: simplesmente ordenando que o celular faça isso. O "Hands Free" - https://get.google.com/handsfree/ (que traduzido do Inglês para o Português significa "Mãos livres"), funcionará independentemente do Android Pay, o sistema de pagamento por aproximação via NFC - *Near Field Communication* (comunicação de campo próximo) para celulares. A diferença em relação ao Apple Pay, Android Pay e Samsung Pay é que o consumidor não precisará nem sequer tirar o smartphone do bolso e encostar na maquininha de cartão. O pagamento será a partir do comando de voz. No momento da compra, a pessoa só vai precisar dizer ao caixa "I'll pay with Google" ("Eu vou pagar com Google") para fazer o pagamento. Antes de finalizar, o funcionário confirmará a identidade do usuário, a partir da foto de perfil registrada no serviço e o nome.

O recurso de comando de voz já existe em vários equipamentos domésticos: Smart TV, *smartphones*, ar condicionado, som, luzes, fogão, geladeira, máquina de lavar roupas, etc.

Já é possível conversarmos como os automóveis pelo fato deles possuírem um sistema de chofer virtual.

Os automóveis ou veículos autômatos ou com piloto automático já são realidade. Empresas como Audi, BMW e Mercedes-Benz já fornecem carros com sistema de navegação automática. E, empresas de alta tecnologia da nova economia, como Google e Uber, já se movimentam para entrar no mercado.

- http://www.droidskill.com/2015/10/taxis-autonomos-comecam-circular-ja-no.html;

Desde 2009, o Google começou um projeto bem ambicioso chamado "The Self-driving-car Project" (SDC). No Brasil, desde 2010, existe o projeto Carina (Carro Robótico Inteligente para Navegação Autônoma), da USP de São Carlos.

A Toyota e a Audi divulgaram na "Consumer Eletronics Show 2013" seus modelos de carros autômatos.

Há décadas já existe o piloto automático nos aviões comerciais e, há anos, os tratores e demais maquinários agrícolas andam sozinhos com orientação por GPS.

O filme "De Volta para o Futuro 2" também previu a **interação da televisão**; ou seja, a TV além de comportar videoconferências, seria multitarefas.

"Smart TV" é uma expressão em inglês que se utiliza para designar as chamadas televisões inteligentes (ou televisões híbridas). É possível associar a Smart TV a um computador pelo fato de dispor de um sistema operativo, à semelhança de muitos outros dispositivos. Tal como aconteceu com os celulares, que se tornaram smartphones, algumas TVs de hoje têm processador, sistema operacional, loja de apps (mais de 400 aplicativos) e muita conectividade.

Uma Smart TV caracteriza-se por ter conexão à Internet e oferecer diversos serviços digitais; ou seja, como em um smartphone ou num tablet, ela permite a instalação de aplicativos. Isso significa que, pela TV, é possível acessar o YouTube, Instagram, FaceBook, Netflix, dentre outros sites e aplicativos. Assim, toda televisão que se conecta à Internet é chamada de "Smart TV". Com uma Smart TV, pode-se procurar conteúdo na Internet (filmes, séries, fotografias, etc.) e visualizá-los no ecrã/tela. Também pode-se gravar ao vivo programas num disco rígido ("hard disc" ou "hd") e interagir, de diversos modos, com os canais de televisão através de várias aplicações.

A televisão digital interativa diferentemente da tradicional televisão analógica, herda o conceito de comunicação bidirecional, criando a possibilidade de uma interação do usuário com a informação que está sendo exibida, permitindo-o ter melhor escolha e controle da experiência de assistir televisão.

Pensando numa forma de oferecer uma plataforma padronizada, com apps e serviços que funcionassem em todas as Smart TVs, surgiram os primeiros sistemas operacionais para este tipo de aparelho. O Google, a Samsung e a LG lideraram o caminho, apresentando em 2014 os sistemas Android TV, Tizen e WebOS, respectivamente.

No Brasil, o sistema (SBTVD - Sistema Brasileiro de TV Digital) idealizado para a DTVi (TV Digital Interativa) é o Ginga (http://www.ginga.org.br/ e http://www.gingancl.org.br/). É um *software* (*middleware*) instalado em aparelhos que serve para rodar aplicações transmitidas pelas emissoras. Trata-se de uma plataforma para aplicações hipermídia. Ele permite a interatividade em nosso sistema de TV Digital, o SBTVD (Sistema Brasileiro de Televisão Digital), o padrão de TV Digital desenvolvido no Brasil, tendo como base o padrão japonês.

O Gired (Grupo de Implantação do Processo de Redistribuição e Digitalização de Canais de TV e RTV) é o grupo criado pela Abert (http://www.abert.org.br/), pelas emissoras de TV aberta e por operadoras de telefonia que decide todo o processo de migração das TVs analógicas para os canais digitais no Brasil (também chamadas de “Ginga C”).

O sinal analógico de TV no Brasil, portanto, está com os dias contados. Muitos anos após deixar de ser transmitido nos Estados Unidos, seu encerramento já está começando no Brasil. A primeira cidade a deixar de ter sinal analógico de TV foi Rio Verde, em Goiás, que está servindo de cidade-piloto para o resto do país desde 15/02/2016. Em seguida, Brasília e uma série de cidades de Goiás terão o sinal desligado a partir de 26/10/2016. São Paulo continuará com sinal analógico até 29/03/2017, e Goiânia passará pelo desligamento em 31/05/2017. Uma tabela com o atual cronograma para o desligamento do sinal analógico no país pode ser em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=25/01/2016&jornal=1&pagina=67&totalArquivos=88.

O decodificador digital (também conhecido como *set-top-box* ou STB) D-Link DTB-332, com software TQTVD (http://www.tqtvd.com.br/), foi escolhido pela EAD - Entidade Administradora da Digitalização (responsável pelo processo de digitalização da TV no Brasil) para integrar o

Kit Conversor (http://vocenatvdigital.com.br/) dos programas Bolsa Família, Minha Casa Minha Vida, Tarifa Social de Energia Elétrica, etc. para levar a TV Digital interativa a beneficiários dos programas sociais. Um dos aplicativos de cunho social que já virá embarcado na plataforma é o Projeto Brasil 4D (http://www.ebc.com.br/brasil-4d), idealizado pela Empresa Brasil de Comunicação (EBC). Ele permite acessar, pelo controle remoto a conteúdos como vagas de emprego, informações sobre saúde e programas de apoio à mulher.

A finalidade, principal e histórica, de uma televisão é o seu conteúdo em vídeo, mas em uma televisão inteligente esse espectro se amplia muito mais; tal como a evolução do celular, ela se tornou multifunção ou multitarefa. Por meio de aplicativos e da conexão à Internet é possível ter acesso a canais online de todo o mundo, serviços de *streaming* como Netflix (https://www.netflix.com/br/), NetMovies (https://www.netmovies.com.br/), Vimeo (https://vimeo.com/), Crunchyroll (http://www.crunchyroll.com/), Google Play Filmes (https://play.google.com/store/movies?hl=pt_BR), Crackle (antigo Kalixta, http://www.crackle.com.br/), Globosat (http://globosatplay.globo.com/globosat/), SBT (https://play.google.com/store/apps/details?id=br.com.sbt.app), SSIPTV (http://ss-iptv.com/en/), Smart IPTV (http://iptvglobal.com.br/), TED (https://www.ted.com/), Google Play Música (https://play.google.com/store/music?hl=pt_BR), Deezer (http://www.deezer.com/), jogos ("games") on line e multiplayers (vários jogadores juntos), previsão do tempo (exemplo, Accuweather), apps específicos de alguns veículos de comunicação, redes sociais (como FaceBook e Twitter) e até fazer cursos e realizar ligações (videochamadas e videoconferências) pelo Skype (https://www.skype.com/pt-br/).

Dá até para consultar conta bancária (http://www.bradescocorretora.com.br/SiteBradescoPortal/Classic/Topo/Bradesco-Samsung-Smart-TV).

Pode-se dizer que pelos aplicativos disponíveis no modelo é que se define qual Smart TV comprar.

A possibilidade de acessar às redes sociais, desfrutar de transmissões digitais em "streaming" (transmissão de som e imagem através de uma rede sem a necessidade de efetuar downloads [baixar o arquivo], pois a retransmissão é instantânea ou em tempo real), descarregar jogos e realizar compras online ("T-commerce") também vinculam a Smart TV com um computador.

O T-commerce, venda de produtos on-line através da TV, não é nenhuma novidade, mas ainda está engatinhando no Brasil.

Em 2003 a Sky lançou o Sky Store (https://www.skystore.com/ e http://www.sky.com/shop/tv/sky-store/).

- http://www.dci.com.br/comercio/operadora-sky-lanca-no-brasil-o-comercio-pela-televisao-id12037.html.

Em 2012 a Vodafone lançou o serviço "Yubuy" de compras através da televisão (http://www.yubuy.tv/). Em 2013, a Zon também aderiu ao YuBuy.

- https://pplware.sapo.pt/informacao/vodafone-ja-e-possivel-comprar-atraves-da-tv/.

Ainda existem recursos adicionais como PiP e PAP ("Picture in Picture"), que permitem mostrar duas imagens de diferentes fontes ao mesmo tempo, divididas por uma janela de visualização ou criando uma janela menor dentro da imagem maior.

A Smart TV também permite o uso de serviços de vídeo sob pedido (VoD - "Video on Demand" ou PPV - "Pay-Per-View"). Isto faz com que os telespectadores possam alugar filmes on line ou escolher quando ver determinado filme ou programa. As marcas costumam ter sua própria loja de compra e aluguel de filmes; além do Netflix e do iTunes.

Com a Smart TV é possível jogar direto na TV sem a necessidade de um console (Xbox, PS - PlayStation, etc.), via *streaming*, como, por exemplo, o Gamefly (https://www.gamefly.com/#!/stream) ou, até mesmo, baixá-los (fazer download) dos jogos diretamente para a Smart TV.

Os modelos mais recentes de Smart TV possuem um dispositivo que reconhece voz e movimento, muito próximo do Kinect do Xbox (http://www.xbox.com/pt-BR/Kinect/Home-new). Isso permite que o usuário altere os comandos da TV ao mexer as mãos ou falar.

Elas também possuem um espaço de interação, como, por exemplo, o Social Hub da Samsung (http://www.samsung.com/galaxyace/socialhub.html), que serve para juntar todos os contatos da agenda, informações de redes sociais e comunicadores em um só lugar. Sempre que quiser acessar a Internet através do navegador embutido ou dos aplicativos de redes sociais já instalados, é só ingressar por essa página especial.

O Apple TV (http://www.apple.com/br/tv/) é um STB - "set-top box" (receptor com tecnologia digital que se conecta a um televisor e a uma fonte externa de sinal, substituindo a função receptora de sinal da tv); ou seja, ele "transforma" televisores comuns em Smart TVs. Ele consegue acessar o conteúdo do iPhone, iPad, iPod touch e Mac pelo AirPlay. Os dispositivos móveis podem inclusive virar controle remoto da televisão por meio do app Remote. Naturalmente, o iTunes vem instalado, permitindo comprar e alugar filmes e ver cenas de bastidores com o iTunes Extras. A Smart TV da Apple vem com serviços populares como Netflix e conta com recurso de compartilhamento familiar.

O Google Cast (https://www.google.com/cast/) também serve para "turbinar" uma tv e deixá-la semelhante à uma Smart TV.

- http://www.androidpit.com.br/melhores-aplicativos-chromecast-android;

Os consoles de *games* (jogos) também oferecem muita conectividade e interatividade para um televisor. Através de qualquer um deles é possível substituir e aposentar o aparelho leitor de CD e DVD. Também possuem uma infinidade de aplicativos que podem ser instalados e, inclusive, os serviços de compra, locação e assinatura de filmes e séries.

Os consoles PlayStation 4 e Xbox One disputam, dia após dia, o coração (ou as mãos) dos jogadores (*gamers*). Há, ainda, o console Nintendo Wii.

O Xbox permite jogar enquanto conversa no Skype, acompanha notícias, guia de *achievement*, sites, entre outros.

O Kinect, além de ler gestos e ouvir comandos para dispensar controles remotos e joysticks, também permite o reconhecimento facial para fins de substituição de senha, jogos pausados/salvos e personalização de configurações. No PS é a PS Câmera.

O ex-projeto Morpheus, atual PlayStation VR, é um visor de realidade virtual que promete levar a pessoa para dentro dos jogos; enquanto o HoloLens, da Microsoft, é uma espécie de visor de realidade aumentada, que promete trazer os games para fora da tela.

O Xbox (http://www.xbox.com/pt-BR/Live/Home-New) tem integração com o Twitter para fazer postagens.

O Upload Studio e o shareFactory permitem a edição e compartilhamento de vídeos gravados.

O aplicativo para celular e tablets Smart Glass permite digitar mensagens e controlar várias aplicações no Xbox One.

Crunchyroll é um dos maiores acervos de *animes* (desenhos animados) do mundo.

O Dropbox (serviço de salvamento de arquivos on line) da Microsoft funciona em conjunto com o Xbox One.

Geralmente a cada 15 ou 30 dias para quem é assinante da Xbox Live Gold, tem o direito de baixar um ou dois jogos gratuitos.

O PlayStation Now é um serviço de assinatura mensal que conta com uma grande biblioteca de jogos que podem ser usados via streaming.

Recentemente a Microsoft anunciou o "Projeto Scorpio" para rivalizar com o PlayStation 4.

Até mesmo **o antigo "toca fitas" ou rádio dos automóveis evoluiu e muito**. Central Multimídia (ou Kit Multimídia) para carros é um aparelho com tela *touch screen*, TV Digital, Rádio AM/FM, DVD, Bluetooth, entrada **USB** (*Universal Serial Bus* ou porta universal, um tipo de conexão *plug and use*; ou seja, "ligar e usar"), *slot* de cartão de memória SD, GPS (*Global Positioning System*), conecção com a Internet, microfone e alto-falante embutidos para fazer e receber ligações sem pegar o celular, entrada Áudio e Vídeo, controle remoto e sensor de estacionamento com câmera de ré. Recursos como o Apple CarPlay e Android Auto já fazem suas estreias no país em veículos como o Fox 2016 e em centrais multimídia de empresas como a Pioneer.

Diante desse cenário, os **bancos** estão pressionando para que as pessoas desacostumem, desapeguem, desprendam, "desmamem" ou "tenham o cordão umbilical cortado" da necessidade de um intermediário humano e de uma agência física para a realização de operações bancárias. Em resumo, para sermos claros, o banco não quer nem mais ter que disponibilizar caixas eletrônicos; muito menos agências físicas. **Tudo será feito sozinho pelo cliente ou usuário em seu próprio aparelho**.

Tal adequação inicia-se através da promoção do uso dos *smartphones* (celulares inteligentes) como agências bancárias *on line*. E, detalhe, várias pessoas que não possuem computador, *notebook*, *netbook* ou *tablet*, possuem *smartphone* pela praticidade do mesmo. Portanto, o *smartphone* é o objeto que a enorme maioria das pessoas portam (trazem consigo) a todo tempo, em todo lugar e em qualquer situação ou circunstância. Desse modo, se há um objeto que deve incorporar um sistema de recebimentos e pagamentos, o *smartphone* é o mais indicado por esse motivo.

Numa fase inicial, o cliente não precisa comparecer à agência bancária para depositar um cheque, bastando apenas bater uma foto dele e enviar pela Internet ao banco; mas permanece a exigência de comparecer para assinar documentos e realizar outras operações. Desse modo, através de simples captura da imagem do cheque pelo celular ou *tablet*, é possível realizar o depósito sem precisar ir até a agência bancária.

- http://economia.estadao.com.br/noticias/negocios,cheques-ja-podem-ser-depositados-pelo-celular,1566581;
- http://banco.bradesco/html/classic/produtos-servicos/outros/deposito-de-cheque-pelo-celular.shtm;
- http://banco.bradesco/next/deposito-cheque.shtml.

M-Banking Banrisul é o canal de atendimento do banco Banrisul que disponibiliza mobilidade para a realização de operações financeiras utilizando smartphones ou tablets por meio das plataformas Android, iOS e Windows Phone (http://www.banrisul.com.br/mbanking).

Outro passo evolutivo, que já existe, é combinação de um número ilimitado de cartões bancários num único cartão, controlado por um aplicativo de *smartphone*, como, por exemplo, o Curve (https://www.imaginecurve.com/). As assinaturas manuais já estão sendo substituídas por certificados digitais totalmente eletrônicos (sem token ou cartão com chip), tais como, por exemplos, o Certillion (https://play.google.com/store/apps/details?id=br.com.esec.icpm.android) e o Token Original do banco virtual Original (https://play.google.com/store/apps/details?id=br.com.bancooriginal.mobile.token). Depois com o aprimoramento e popularização dos serviços, não haverá nenhuma necessidade de ir até uma agência bancária física e, assim, os *smartphones* praticamente se tornam uma agência virtual da instituição financeira.

> "Quando uma rede de varejo decide vender também pela Internet e cria um canal para isso, isto não significa que ela se tornou uma empresa digital. Significa apenas que agora ela tem um canal digital. Tornar-se digital significa captar clientes pelo meio digital e relacionar-se com eles por meio do mundo digital, oferecendo uma experiência comparável a empresas digitais de outros segmentos. Da mesma forma, quando um banco cria uma agência digital não significa que se tornou digital. Mesmo porque sabemos que, em vários momentos, o cliente precisará ir na agência para assinar um documento ou passar num caixa automático para autorizar uma operação. Estes processos não contínuos não fazem parte do mundo digital." (Guilherme Horn *in*

http://link.estadao.com.br/blogs/seu-bolso-na-era-digital/o-que-nao-e-um-banco-digital/).

Portanto, atualmente já existe em prática no Brasil os serviços de pagamentos de boletos e de contas diversas, transferências de valores, depósitos de cheques, etc., não só através do computador, mas também pelo *smartphone* (celular) ou tablet.

- http://www.bb.com.br/pbb/pagina-inicial/atendimento/bb-no-celular#/;
- http://banco.bradesco/html/classic/produtos-servicos/outros/aplicativos/home/index.shtm;
- https://www.itau.com.br/conveniencia/celular/;
- http://www.caixa.gov.br/atendimento/aplicativos/caixa-celular/Paginas/default.aspx.

E, os aparelhos de celular, se transformaram em verdadeiras máquinas de leitura de código de barras, de QR Codes, de cartões e, inclusive, caixas eletrônicas e, até mesmo, agências bancárias *on line* personalizadas.

- http://blogs.ne10.uol.com.br/mundobit/2015/06/11/celular-respondeu-por-10-das-transacoes-bancarias-em-2014/.

No Quênia e Tanzânia grande parte da população faz compras e realiza transferências financeiras utilizando o M-pesa (https://www.mpesa.in), um sistema de movimentações financeiras via telefone celular que utiliza os créditos do celular como moeda de troca.

- http://g1.globo.com/Noticias/Economia_Negocios/0,,MUL1366395-9356,00-CELULAR+E+BIOMETRIA+DEVEM+SUBSTITUIR+CEDULAS+E+MOEDAS+DIZEM+ESPECIALISTAS.html.

O MB Way (https://www.mbway.pt/) é uma aplicação que permite efetuar compras e transferências imediatas através de um smartphone ou de um tablet. Esta aplicação associou-se à sétima edição do Rock in Rio, permitindo aos festivaleiros usufruírem do aplicativo.

Em Portugal, a SIBS, empresa que gere a rede Multibanco, disponibiliza uma aplicação (MB Way) para celulares que permitirá fazer pagamentos

eletrônicos e transferências de dinheiro entre as contas bancárias dos utilizadores.

- https://www.mbway.pt/.

Inclusive, a MasterCard e a Alibaba vão testar sistemas de pagamentos (respectivamente, "ID Check" e "Smile to pay") que detecta e reconhece o rosto do cliente.

- http://www.mobiletime.com.br/30/09/2015/mastercard-testa-sistema-de-pagamentos-com-reconhecimento-facial-na-europa-e-estados-unidos/420929/news.aspx;
- http://oglobo.globo.com/economia/alibaba-planeja-sistema-de-pagamentos-com-reconhecimento-facial-15655390;
- http://www.selfieblog.net/noticias/sistema-de-pagamento-via-selfie/.

O reconhecimento facial automático existe no Facebook desde o ano 2010 e já foi implantado nas câmeras de lojas e de demais estabelecimentos para realizar a indetificação e o *check-in* de formas automáticas.

- http://www.mobiletime.com.br/07/07/2016/start-up-oferecera-para-lojistas-reconhecimento-facial-de-consumidores/444943/news.aspx;
- http://link.estadao.com.br/noticias/inovacao,quando-o-rosto-e-sua-mais-nova-identidade,10000029132;
- http://www.ipc.digital/japao-consumidor-pode-usar-o-rosto-como-forma-de-pagamento/;
- http://www.gazetadopovo.com.br/economia/inteligencia-artificial/cuidado-seu-rosto-pode-revelar-mais-sobre-sua-vida-do-que-voce-pensa-0nrqszo8tg8sd9v74gbqm56qg;
- https://canaltech.com.br/noticia/facebook/Facedeals-faca-check-in-com-seu-proprio-rosto/;
- https://spyratus.wordpress.com/2012/08/15/servico-de-loja-reconhece-o-rosto-dos-consumidores-no-facebook/.

O **Google Wallet** (https://www.google.com/wallet/) foi lançado em 2011 para facilitar as operações de crédito e débito (virtuais ou não). É uma carteira virtual para o sistema Android, que permite fazer recebimento e envios de dinheiro até mesmo usando apenas o e-mail ou o SMS. Também utiliza o NFC. Ao adquirir créditos no serviço é possível usar ele como um

cartão de débito. Atualmente está disponível para mais de 100 países, incluindo o Brasil. Ele está sendo atualizado, substituído ou operado em conjunto com os Google Play (https://play.google.com/store), Android Pay (https://www.android.com/pay/) e Google Store (https://store.google.com/).

O "Google Market" foi atualizado ("upgrade") para "Google Play (Store)". Em informática, "E-store" ou simplesmente "store" (“loja”), é uma loja virtual de programas. "Google Play Store", "Play Store" ou "Google Play" (https://www.google.com.br/mobile/play/ e https://play.google.com/store) é uma loja virtual da Google. Portanto, trata-se de uma "one-stop-shop" (um balcão único, uma loja de parada ou uma fonte de parada; em síntese, uma loja onde se pode adquirir tudo que precisa: “compra em uma única parada”). Antes de março de 2012, o "Android Market" era só sobre aplicativos enquanto que o "Google Music" e o "Google Books" versavam, respectivamente, livros e músicas. No "Google Play" (como também na iTunes da Apple [https://itunes.apple.com/br/app/apple-store/id375380948?mt=8] e na Windows Phone [https://www.microsoft.com/pt-br/store/apps/windows-phone]) pode-se comprar, ou adquirir gratuitamente músicas, filmes, livros e, é claro, aplicativos (Apps). Para ter acesso à loja é necessário ter uma Conta Google gratuita; caso não tenha, você pode criar no próprio celular, tablet ou computador (https://accounts.google.com/SignUp?hl=pt-BR).

Do mesmo modo existe a "Amazon App store" (https://www.amazon.com.br/gp/mas/get/android e https://itunes.apple.com/br/app/aplicativo-da-amazon-compre/id297606951?mt=8).

A "Google Store" (https://store.google.com/) é uma loja online onde pode descobrir e comprar celulares e tablets Android, relógios Android Wear, Chromebooks, dispositivos de transmissão de multimídia e acessórios relacionados. Anteriormente, estes produtos encontravam-se disponíveis no Google Play. Agora, o Google Play (https://play.google.com/store?hl=pt_BR) vende apenas aplicações do Google Play e conteúdo de música, de filmes, de TV, de livros, etc.

Basicamente, o "Android Pay" é o mesmo recurso "tap-to-pay" ("toque para pagar") do "Google Wallet"; exceto que é menos complicado. Com o "Google Wallet", era preciso abrir um aplicativo e, em seguida, digitar um número pin (senha) para que o Google pudesse desbloquear os cartões de crédito armazenados no celular. O velho "Google Wallet" será atualizado para o "Android Pay" assim que este último finalmente estiver pronto e disponível ao público. O novo "Android Pay" (existia uma versão anterior dele) assumirá o pagamento por itens que os usuários comprarão, tanto em lojas físicas quanto online.

As formas de pagamento aceitas no Google Payments (http://payments.google.com/) ou Google Wallet (https://wallet.google.com/) são: cartões de débito e de crédito: American Express, MasterCard, Visa, Discover (somente EUA), JCB (somente Japão e EUA), Visa Electron (somente fora dos EUA) e Elo (somente no Brasil); conta bancária (nos Estados Unidos e no Reino Unido é possível vincular uma conta bancária à conta do Google); e, PayPal na Alemanha, Austrália, Áustria, Bélgica, Canadá, Cingapura, Espanha, Estados Unidos, Finlândia, França, Grécia, Holanda, Irlanda, Itália, México, Nova Zelândia, Portugal, Reino Unido, Rússia, Suécia e Suíça. Não é possível utilizar as seguintes formas de pagamento na Conta do Google: transferências eletrônicas, transferências bancárias, Western Union, MoneyGram, cartões de crédito virtuais (VCC), contas de poupança de saúde (HSA), cartões de transporte público e qualquer tipo de garantia de pagamento.

Basta pesquisar na lista de aplicativos para smartphone na plataforma Windows phone (https://www.microsoft.com/pt-br/store/apps/windows-phone) e no sistema Android (https://play.google.com/store/apps) para constatar a variedade de aplicativos para *smartphones* e tablets com a função de **substituir os cartões bancários**, de débito e de crédito; bem como da necessidade de carteira convencional e de portar dinheiro em espécie (físico).

Outra forma cogitável por muitos de substituir o uso de cédulas, cheques e cartões, seria os microchips ou certificados digitais deixarem de serem usados em cartões de plástico e serem instalados em outros dispositivos que as pessoas já costumam carregar consigo (relógios [*smartwatch*], pulseiras,

anéis, celulares [*smartphones*], chaves de casa ou do carro, etc.) ou serem implantados sob a pele da pessoa. Mas isso é muito inconveniente e envolve transtornos, trabalho e despesas aos usuários; bem como implica em risco de o chip ser danificado ou ser perdido.

O Bradesco e a Visa projetaram uma **pulseira** de pagamentos para substituir os cartões bancários. Referida pulseira realiza a transferência monetária via **NFC - *Near Field Communication*** (comunicação de campo próximo); uma tecnologia de comunicação por proximidade que troca dados criptografados com a maquininha de débito. A comunicação entre os dispositivos é realizada mediante radiofrequência, na faixa dos 13,56 MHz, os dispositivos devem estar a uma distância de no máximo 10 cm para que a comunicação pode ser iniciada. As maquininhas de cartão mais modernas (e nem precisam ser tão modernas assim) já possuem o NFC; ou seja, estão automaticamente habilitados para se comunicar com o aplicativo/smartphone e realizar um pagamento, com direito a duas vias da notinha e tudo, igualzinho ao que vemos quando pagamos com cartões.

O aplicativo Ourocard do Banco do Brasil também possibilita a realização de pagamentos via NFC (https://play.google.com/store/apps/details?id=br.com.bb.oewallet&hl=pt_BR).

Apesar do recente alarde sensacionalista das marcas de renome, Paypal, Bcash (http://bcash.com.br/), PagSeguro (https://pagseguro.uol.com.br/), Oi Carteira (http://oi.com.br/oi/oi-pra-voce/oi-para-comprar/oi-carteira), Meu Dinheiro Claro (http://br.mobiletransaction.org/meu-dinheiro-claro-bradesco/), TIM Mobile Payment, TIM Mobile Money, Tim Multibank (http://www.tim.com.br/sp/para-voce/servicos-tim/servicos-financeiros/multibank/multibank ou https://lojaonline.tim.com.br/landingpage/timmultibank), Zuum (http://www.zuum.com.br/), Picpay (https://www.picpay.com/br/) e eWally (http://www.japaga.com.br/pages/index.php), dentre várias outras opções, há tempos, também permitem realizar e receber pagamentos utilizando o aparelho celular. Inclusive a tecnologia NFC já estava em uso antes das divulgações na Mídia. Referida tecnologia é um padrão definido pelo NFC

Fórum (http://nfc-forum.org/), um consórcio global criado em 2004 (http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-nfc.html).

Em poucas palavras, o NFC (http://nfc-forum.org/ e http://nearfieldcommunication.org/) é uma especificação que permite a comunicação sem fio (wireless) entre dois dispositivos mediante uma simples aproximação entre eles, sem que o usuário tenha que digitar senhas, clicar em botões ou realizar alguma ação semelhante ao estabelecer a conexão. Daí o nome: *Near Field Communication* (Comunicação de Campo Próximo ou Comunicação em Área Próxima). Isso significa que, tão logo os dispositivos envolvidos estejam suficientemente próximos, a comunicação é estabelecida automaticamente e dispara a ação correspondente. Esses dispositivos podem ser telefones celulares, tablets, crachás, cartões de bilhetes eletrônicos e qualquer outro item capaz de suportar a instalação de um chip NFC.

A NFC é baseada no RFID ("Radio-Frequency Identification"), tecnologia mais consolidada que permite, tal como o nome indica, aplicações de identificação por radiofrequência.

Bradesco e Visa já testam o sistema de pagamentos por aproximação desde 2008, quando lançaram um modelo e cartão compatível com a tecnologia NFC. A tecnologia hoje está disponível em cartões emitidos pelo banco e também pelo Original.

O consumidor tem um número de ID e cartão vinculados à sua conta na pulseira, mas não é preciso ter conta no banco Bradesco para usar o acessório. A pulseira funciona como um cartão de débito pré-pago, que pode ser recarregada por boleto ou por meio de um aplicativo dos sistemas Android e iOS (da Apple).

Recentemente também, a Bradesco Seguros iniciou os testes de sua Carteira Digital, para facilitar o acesso aos benefícios dos planos assinados, o que muitas vezes é dificultado pelo esquecimento dos cartões físicos por parte dos clientes.

O Bradesco é um dos bancos parceiros da **Samsung no Pay** (http://www.samsung.com.br/samsungpay/), o que vai permitir que seus correntistas usem seus cartões no sistema. É inevitável a comparação com o Apple Pay (http://www.apple.com/apple-pay/), o serviço de pagamentos via NFC dos aparelhos iPhones da Apple. Enquanto o sistema de pagamentos da empresa da maçã (Apple) só funciona com máquinas que possuam o padrão de conectividade NFC, o Samsung Pay poderá ser usado em qualquer terminal de cartão de crédito. Encontrado facilmente no comércio, é preciso apenas do leitor de tarja magnética para usá-lo. Isso só é possível graças à tecnologia LoopPay (https://www.looppay.com/). Dessa forma, os novos aparelhos da companhia virão com uma pequena bobina de metal, implantada internamente, que criará uma corrente magnética reconhecida pelo famoso leitor de cartão de crédito. Já o padrão NFC necessita de um leitor específico.

Os bancos estão constantemente aperfeiçoando os seus caixas eletrônicos e uma das novidades é a **inclusão de leitor de NFC**, para viabilizar operações programadas previamente no *smartphone* ou mesmo no *smartwatch* do correntista. Preparando-se para essa demanda, a provedora de soluções de automação bancária Oki Brasil (antiga Itautec) desenvolveu um caixa eletrônico com NFC ("Near Field Communication"), o Adattis Mobicash.

> ***Smart watch*** é a junção de duas palavras distintas: "smart", que significa “inteligente” e watch, que quer dizer “relógio”. Desse modo, trata-se de um relógio inteligente; ou seja, um aparelho que mistura a aparência de um relógio de pulso tradicional com as funcionalidades de um smartphone.

A fabricantes suíça de **relógios Swatch** lançou um novo modelo capaz de efetuar pagamentos. Os primeiros mercados a receber o relógio serão Estados Unidos, Suíça e Brasil. Em parceria com a VISA, a empresa lançou o modelo *Swatch Bellamy*, o primeiro relógio "pay-by-the-wrist" (pago pelo pulso), trazendo um adesivo NFC que permitirá comunicação com as maquininhas de cartão. Este adesivo já é usado por alguns bancos nos Estados Unidos para serem colocados em chaveiros e pulseiras (https://www.swatch.com/pt_br/pages/bellamy-watch).

O Google (https://www.android.com/wear/) possui 19 dispositivos diferentes de *smartwatch* (http://www.wareable.com/smartwatches/best-android-watch) e a Apple também possui seu *Smartwatch* (http://www.apple.com/br/watch/ e http://www.apple.com/br/watchos-preview/).

O Apple Watch mede batimentos cardíacos, atende ligações, realiza pagamentos e possui a Siri (assistente virtual com base em inteligência artificial).

O Apple Watch funciona conectado, via Bluetooth, a um iPhone 5 ou mais recente. Como o iPhone 6 e o iPhone 6 Plus, o Apple Watch tem conexão NFC e poderá ser usado como carteira digital para pagamentos. Para pagar, bastará aproximar o dispositivo de um terminal.

O Nubank (https://www.nubank.com.br/), primeiro cartão de crédito totalmente online (sem agência física) do Brasil, assim como no smartphone, possui aplicativo para o Apple Watch, fornecendo informações sobre a conta e efetuando pagamentos com o relógio.

O smartphone faz quase tudo que o Apple Watch faz. Para usar o relógio, basta ter um iPhone 5 ou mais recente por perto.

Os relógios inteligentes que rodam o Android Wear (https://www.android.com/intl/pt-BR_br/wear/), versão do sistema operacional do Google para aparelhos vestíveis, também funciona com iPhones.

A empresa chinesa Mobvoi desenvolveu o relógio inteligente Ticwatch 2 (http://ticwear.com/ticwatch2/), que traz o sistema operacional Ticwear 4.0, um Android Wear otimizado.

O relógio inteligente (“smart watch”) funciona de forma muito limitada sem o *smartphone*. Então, por que não usar só o *smartphone*?

Os ***smartphones* são como canivetes suíços digitais**, pois num aparelho tão portátil estão disponibilizados milhões de recursos e funções. Desse modo, esse pequeno, leve e prático aparelho substitui o aparelho telefônico fixo, orelhão (telefone público), disk hora certa, disk previsão do tempo, secretária eletrônica, videoconferência, identificador de chamadas, pager, fax, relógio, lanterna, agenda de contatos e telefones, lista telefônica, catálogo de empresas e profissionais, catálogo da programação da tv, manuais impressos dos usuários, manual de primeiros socorros, calendários, tabelas (de conversões, periódica, tabuada, etc.), planilhas, agenda de compromissos, diário, jornais e revistas, livros, dicionários, enciclopédias, livro de receitas, biblioteca, formulários impressos, cartões de visitas, currículo impresso, orçamentos impressos, panfletos, classificados impressos, bússola, GPS, navegador, rastreador, velocímetro, pedômetro, mapas, guias de cidades e de ruas, câmera fotográfica, editor de fotos, álbum de fotos, filmadora, videocassete, DVD player, espelho, lupa, régua, nível, binóculo, microscópio, caneta e bloco de notas, prancheta, lembretes, lista de compras, carta, gravador de voz, calculadoras, despertador, rádio relógio, temporizador, cronômetro, termômetro, medidor de luz, game boy, videogame portátil, jogos de tabuleiro, tv, monitor de câmeras, rádio, micro system, *walkie talkie*, videolocadora, *walkman*, *discman*, mp3 player, CD, DVD, pendrive, afinador de instrumentos, equalizador, vibrômetro, decibelímetro, altímetro, apitos, repelentes de insetos e animais, polígrafo, metrônomo, controle remoto, roteador, simuladores, cabos de informática, órgão (piano) eletrônico, máquina reprográfica (copiadora), scanner, leitor de digitais, leitor de código de barras, medidor de batimentos cardíacos, babá eletrônica, talão de cheques, carteira, cartão bancário, leitor de cartões bancários, caixa eletrônico, ponto de táxi, lojas e escritórios e consultórios físicos, etc.

Usar o relógio inteligente (“smart watch”) como uma extensão do *smartphone* não passa de preguiça de ter que pegar o celular (do bolso, do cinto, da bolsa ou da pasta) e ter que segurá-lo (com a mão).

O relógio inteligente, além de caracterizar pura vaidade, ostentação, exibicionismo e impulso consumista, também serve, de fato, para facilitar o manuseio do celular quando há risco de perder ou estragar o celular ou se está com as mãos ocupadas ou impossibilitadas de manuseá-lo, tais como,

por exemplo, quando se está dirigindo, pilotando, navegando, esquiando, surfando, escalando, saltando de paraquedas, mergulhando, pendurado pelas mãos, etc. Entretanto, recorda-se que já existe há muito tempo, fones de ouvido e *headset* ou *headphone* com *Bluetooth* para que se possa atender o celular sem usar as mãos; bem como conectar o *smartphone* ao sistema operacional do automóvel e a vários dispositivos de mídia.

Os usuários com smartphones Windows 10 mobile contam com uma ferramenta para concorrer com o Android Pay e o Apple Pay. O aplicativo Wallet (http://www.windowscentral.com/tag/wallet) foi adicionado no programa *Windows Insider*. O Wallet age de maneira similar ao Android e ao Apple Pay; utiliza a tecnologia NFC para pagamentos e gerencia cupons, cartões de fidelidade e passes.

O **Samsung Pay** possui compatibilidade com praticamente qualquer maquininha de cartão. Tanto usa o NFC como o MST ("Magnetic Secure Transmission"); uma tecnologia mais antiga das maquininhas de cartões (aquelas que não possuem o NFC).

O Brasil é o sétimo país do mundo e o primeiro da América Latina a receber a tecnologia Samsung Pay.

Inicialmente, Visa e Mastercard, as duas principais bandeiras de cartão de crédito do mercado, poderão ser integradas ao Samsung Pay. A Samsung já conta com vários parceiros para a empreitada no Brasil: Banco do Brasil, Bradesco, Brasil Pré-Pagos, Caixa Econômica Federal, Itaú, Nubank, Porto Seguro, Santander, Banrisul, Bradesco, Itaú, Nubank (https://www.nubank.com.br/) e Brasil Pré-Pagos (https://www.brasilprepagos.com.br/).

O Samsung Pay funciona totalmente *off-line* (não usa o sinal da sua operadora de celular ou da sua rede de dados móveis), pois assim que aproxima o smartphone Samsung compatível com a maquininha para realizar o pagamento, é a operadora da própria maquininha que realiza o procedimento.

Samsung Pay só funciona com determinados smartphones da linha Galaxy da Samsung.

O Apple Pay autentica a transação NFC através do seu sensor biométrico (“Touch ID”). Com o Apple Pay é possível acrescentar cartões de crédito ao celular através do Apple Passbook, simplesmente tirando uma foto do cartão e autorizando o processo no banco. O TouchID consta dos smartphones iPhone 5S, 6 e 6 Plus, bem como nos Air iPad 2 e iPad Mini 3.

Antes da tecnologia NFC, ou seja, em aparelhos celulares mais simples, a tecnologia de SMS ("Short Message Service" ou, serviço de mensagens curtas, o popular "torpedo") pode efetivar uma transação, com uma simples mensagem de texto que confirma a compra. E, ainda, existe a tecnologia USSD ("Unstructured Supplementary Service Data" ou Dados de Serviços Suplementares Não Estruturados), que associa uma conta bancária virtual ao número de celular do cliente. Com ela também é possível realizar pagamentos e transferências de dinheiro. O USSD é uma tecnologia presente em praticamente todo e qualquer celular, e que é bastante parecida com a utilizada para transmissão de mensagens de texto SMS. Os bancos e as operadoras de cartões de crédito já utilizam, há anos, esses recursos para confirmarem e autorizarem transações.

Em celulares que não possuem o NFC, este recurso pode ser substituído através do *Bluetooth*. Exemplos disso são as leitoras de cartões e os respectivos aplicativos da iZettle (https://www.izettle.com/br), da Payleven (https://payleven.com.br/), da PagSeguro (https://pagseguro.uol.com.br/), etc.

Existem aplicativos de *smartphones* que checam se o aparelho possui NFC, tais como, por exemplos, o NFC Check by Tapkey e o NFC Enabled?. Existe, também, o Conexão Fácil NFC, que permite que o smartphone se conecte, via *Bluetooth*, aos dispositivos compatíveis com NFC da Sony.

A título de comparação de avanço tecnológico, através da Portaria 105/2016 da CVM (Comissão de Valores Mobiliários), foi regulamentado no Brasil a ***FinTech*** ("financial" + "technology"); ou seja, sistema eletrônico de controle das *startups* (empresas em fase embrionária ou iniciando) no

mercado de ações. Os operadores dessas *startups*, denominados *players* (jogadores), se utilizam da tecnologia de ponta para realizar as operações com títulos e ações de grandes companhias, trabalho este, até então, desenvolvido em grandes estruturas físicas com número elevado de corretores. Em apenas um click, o investidor compra e negocia títulos, em forma não presencial, por senhas, login e reconhecimento biométrico.

- http://www.cvm.gov.br/export/sites/cvm/decisoes/anexos/2016/20160607/PORTARIA-105.pdf;

Também é perfeitamente possível e viável a utilização de outros meios de pagamentos e recebimentos **sem qualquer forma física envolvida**, mas mantendo algum método de identificação do titular (impressões digitais, traços faciais, retina, voz, DNA, etc.).

Alguns bancos foram ainda mais longe ao dispensar o cartão de plástico. Desde 2012, Bradesco e Itaú permitem fazer saque e consultar saldo usando apenas a biometria (não precisa de *smartphone*). Basta ir ao caixa eletrônico, digitar sua agência e conta e colocar o dedo (ou o pulso) no leitor biométrico e sair com o dinheiro.

O Bradesco já possibilita, nos seus caixas eletrônicos, os clientes a sacarem dinheiro sem a necessidade de cartão e sequer de senha, mediante o uso da biometria da empresa Fugitsu (http://banco.bradesco/next/biometria.shtml). O procedimento de identificação ou autenticação do cliente consiste na leitura da palma da mão, ou melhor, dos vasos sanguíneos existentes na mão. De forma semelhante, os bancos Itaú e Banco do Brasil estão aderindo à sistemas biométricos para identificar seus clientes e facilitar as transações nos caixas automáticos.

Em 2013 o Banco do Brasil projetou um caixa eletrônico com reconhecimento biométrico conjunto do rosto, da íris e da voz.

- http://economia.estadao.com.br/noticias/geral,banco-do-brasil-lanca-caixa-eletronico-futurista,167890e;

Ainda no filme "De Volta Para o Futuro 2", o personagem Biff **pressiona o polegar num pequeno aparelho para pagar** uma corrida de táxi (ou será de Uber, Cabify, WiiGo, Televo, EasyGo, Fleety, 99Taxis, T81 ou Lyft?). Seria um leitor de cartão de crédito para celular? Essa ideia Jack Dorsey, um dos fundadores do Twitter, teve ao transformar o aparelho móvel em uma prática máquina de cartão de crédito, isso através de um aplicativo chamado Square (https://squareup.com/global/en/pos). O pagamento por celular já existe, por exemplos, através do Apple Pay, Android Pay e Samsung Pay.

A convergência de computadores e telecomunicações permitiu conectar computadores e outros dispositivos, criando a oportunidade para a implantação de toda uma variedade de novos serviços bancários. Já faz parte da atividade bancária atualmente estar disponível 24 horas por dia, sete dias por semana, com a possibilidade de o cliente acessar o seu banco através de computadores, caixas eletrônicos, *smartphones*, etc.

Desde 2014 o Banco do Brasil já projetou o uso do *smartphone* no lugar do cartão.

- http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=36971&sid=5;

Desde 2014, o Banco do Brasil oferece o "saque móvel", que permite realizar saques sem cartão usando o app para smartphone.

- http://www.bb.com.br/pbb/pagina-inicial/voce/produtos-e-servicos/contas/todos-os-servicos/saque-movel#/;

Pouco tempo atrás, o JPMorgan Chase, maior banco dos EUA, divulgou que vai instalar caixas eletrônicos que usarão o *smartphone* no lugar do cartão.

Enquanto que o Amazon Wallet (https://www.amazon.com/wallet) iniciou apenas oferecendo a capacidade de armazenar e organizar cartões de presente e cartões fidelidade de lojas virtuais; o Alipay e a empresa Huawei, se juntam em projeto de inovação para viabilizar o pagamento através de **digitais no celular**.

Com MasterPass da MasterCard (https://www.mastercard.com/br/masterpass/) é possível armazenar os dados de pagamento e entrega; ou seja, adicionar os cartões de crédito, débito e pré-pago, de qualquer banco e diversas bandeiras. Portanto, trata-se de uma carteira digital, quase ao estilo Google Wallet (https://www.google.com/wallet/).

Atualmente **sensores biométricos** (leitores de impressões digitais, retina, íris, rosto, etc.) são populares, principalmente em fechaduras eletrônicas, cartões de ponto e *smartphones*. Recurso bastante popularizado pela Apple com o lançamento do iPhone 5S e que já existe em outras marcas, como a Samsung, a partir dos modelos Nexus 5X e Nexus 6P.

Os *smartphones* Galaxys S5, Note 5, A5 e A7 também possuem leitor de impressões digitais (para desbloquear o aparelho e autorizar transações via Samsung Pay), semelhante ao que já fazia a Apple, com o *Touch ID* (identificação por toque para autorizar as compras no iTunes e na Apple Store ou em outras ocasiões em que seja necessário uma senha), desde o iPhone 5s em 2013. Entretanto, enquanto que no iPhone 5s basta repousar o dedo sobre o botão, no Galaxy S5 é necessário deslizar o dedo. O HP Elite x3 e o Android M também possuem leitor de digitais. O Samsung Pay realiza pagamentos sem usar NFC através da tecnologia MST (transmissão segura magnética), que emula a tarja magnética do cartão de crédito ou débito.

Atualmente a principal rival da Apple é a Samsung, que já deixou a Apple para trás com o leitor de íris (a parte mais visível e colorida do olho que circunda a pupila). Os *smartphones* Fujitsu Arrows NX F-04G, TCL 3S M3G, ZTE Blade S6, Microsoft Lumia 950 e 950 XL, HP Elite x3, Samsung Galaxy Note 7, HomTom HT10 e Alcatel Idol 3 fazem leitura da íris; já os Galaxy S7 e LG G5 possuem leitores de íris e retina.

- http://www.samsung.com/global/galaxy/galaxy-note7/;

A **retina** humana é a camada de tecido nervoso que recobre internamente a parte posterior do olho. Trata-se de um tecido fino composto por células neurais. A retina capta a imagem e cria impulsos que são enviados ao cérebro através do nervo óptico. Devido à estrutura complexa dos capilares

que abastecem a retina com o sangue, a retina de cada pessoa é única. A rede de vasos sanguíneos na retina é tão complexa que até mesmo os gêmeos idênticos não compartilham um padrão (tal como as digitais). Embora padrões de retina podem ser alterados em casos de diabetes, glaucoma ou doenças degenerativas da retina, a retina tipicamente permanece inalterada desde o nascimento até à morte. Um identificador biométrico conhecido como um *scan* de retina é usado para mapear os padrões únicos de retina de uma pessoa. Os vasos sanguíneos dentro da retina absorvem a luz mais prontamente do que o tecido circundante e são facilmente identificados com iluminação apropriada.

Já a **íris** é o anel colorido ao redor da pupila. Trata-se de uma estrutura fina, circular no olho que é responsável por controlar o diâmetro e tamanho da pupila e, portanto, a quantidade de luz que atinge a retina. Centenas de milhões de pessoas ao redor do mundo têm sido matriculados em sistemas de reconhecimento de íris para fins de conveniência e segurança de postos de fronteira automatizado sem passaporte para funções de identidade nacionais.

Enquanto que a retina pode ser afetada por doença, a textura da íris permanece notavelmente estável. Assim, uma das principais vantagens do reconhecimento da íris, além de sua velocidade de correspondência e sua extrema resistência a falsos resultados, é a estabilidade da íris como um órgão interno, protegido, ainda visível externamente do olho, com o que permite a captura e análise à distância. Para o reconhecimento da íris utiliza-se uma câmera, semelhante a qualquer câmera digital, mediante uma fotografia normal à certa distância (como, por exemplo, através de câmeras de segurança em aeroportos), que identifica pontos e anéis na faixa colorida do globo ocular; já para a digitalização da retina, exige muito mais proximidade com o aparelho que emite um feixe de luz profunda no interior do olho para proceder à digitalização dos vasos sanguíneos. Além disso, exige-se que o indivíduo deve fique imóvel, com o olhar fixo, levemente arregalado, para a câmera da máquina de biometria.

Um exemplo relevante do avanço tecnológico dos sistemas bancário e financeiro, bem como da tendência irreversível para a migração virtual ou o fim do serviço bancário convencional, é a greve (paralisação) dos bancários em 2016, que durou 31 (trinta e um) dias (ocorreu de 06/09 a 06/10/2016), e

foi a greve de maior duração desde 2004. Ignorando a questão de ter tido, ou não, motivação puramente política (ser retaliação ou desobediência civil em represália contra o *impeachment* da Dilma Rousseff), essa greve, apesar de sua duração, praticamente ninguém sentiu falta dos bancários; ou seja, para a grande maioria das pessoas foi como se não estivesse tendo greve. Para a minoria que percebeu a greve, esta só lhes estimulou, incentivou e convenceu de que não precisam de um banco físico e de atendimento bancário feito por pessoas presencialmente; vez que através da Internet podem acessar e usufruírem de todos os serviços bancários. Por outras palavras, essa greve foi o maior "tiro no próprio pé" dos bancários; pois os usuários cada vez mais aprendem a utilizar o *home banking* e as agências virtuais, culminando em mais fechamento de agências físicas e em mais bancários perdendo o emprego. Mesmo quem não sabe usar ou não tem acesso aos serviços pela Internet e nem mesmo aos caixas eletrônicos (terminais de autoatendimento), as agências dos Correios, as casas lotéricas e, até mesmo, certos estabelecimentos comerciais, realizam serviços bancários. Explica-se. Alguns bancos têm convênios com casas lotéricas, supermercados, lojas de departamento e drogarias para o pagamento dessas contas. Já a CEF (Caixa Econômica Federal) tem convênio com as casas lotéricas, o Banco do Brasil com os Correios e, o Bradesco, com os supermercados Extra, Compre Bem, Pão de Açúcar e Barateiro.

O Bradesco está para lançar sua versão de banco digital totalmente independente da sua estrutura tradicional. "A plataforma tradicional dificilmente terá o mesmo *sex appeal*. Vamos desenvolver algo equivalente ao FaceBook, ao Waze ou ao WhatsApp e, para isso, temos de repensar o banco do ponto de vista do cliente por meio de uma outra plataforma" (Maurício Minas, vice-presidente executivo do Bradesco *in* http://fusoesaquisicoes.blogspot.com.br/2016/06/bradesco-prepara-seu-banco-digital.html).

Desde 2011, o Banco Central do Brasil permite que as instituições financeiras disponibilizem contas bancárias gratuitas para movimentação via Internet, telefone ou caixas eletrônicos. Isso quer dizer que com as contas digitais os clientes não pagam nada para fazer transferências, saques e pagamentos sem custos.

- Resolução Bacen 3.919, de 25/11/2010 - http://www.bcb.gov.br/htms/normativ/RESOLUCAO3919.pdf.

Ainda mais, em reforço, recentemente, o CMN - Conselho Monetário Nacional (http://www.bcb.gov.br/Pre/CMN/Entenda%20o%20CMN.asp) aprovou a Resolução 4.480/2016, que permite que as instituições financeiras abram e encerrem contas de depósitos para pessoas físicas pela Internet (sem a necessidade de irem pessoalmente a uma agência bancária).

- http://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50185/Res_4480_v1_O.pdf.

A conta digital funciona exatamente do mesmo modo que uma conta corrente. A diferença é que nessa modalidade de pacote bancário o cliente fica isento de cobranças ao utilizar o banco somente por meios eletrônicos (caixa eletrônico, *internet banking*, aplicativo para celular ou atendimento por telefone). Em resumo, se não houver necessidade de interação com um atendente físico, os serviços não são cobrados, o que torna a conta digital bem interessante.

> "O "Banco Digital" (ou "Digital Banking") é uma nova tendência no mercado financeiro que está surgindo rapidamente no mercado como uma evolução do Internet Banking e do Mobile Banking, com o objetivo de manter todo o relacionamento bancário no celular, aproveitando a hiperconectividade da nossa sociedade. Nós já estamos chegando no momento em que todo o processo de relacionamento entre os bancos e seus clientes pode ser feito online, dispensando a presença física e a papelada burocrática. E é aí que entra o conceito de "Banco Digital": ele é uma nova forma de relacionamento fim-a-fim, enquanto o Internet Banking e o Mobile Banking surgiram apenas para ser mais um canal de interação com o banco - assim como as agências, *call center* e caixas eletrônicos. Ou seja, o Internet e o Mobile Banking são apenas mais um canal transacional, enquanto o Banco Digital foca em todo o relacionamento com o cliente (não apenas as transações)." (Anchises *in* http://anchisesbr.blogspot.com.br/2016/06/cyber-cultura-surge-o-banco-digital.html).

O Intermedium é um banco 100% digital e sem tarifas (https://www.intermedium.com.br/index.jsf).

Diferentemente da Digiconta do Bradesco (http://banco.bradesco/html/classic/produtos-servicos/conta-corrente/digiconta.shtm), no Intermedium não há a necessidade de comparecer até uma agência para abrir conta, pois todo o processo é feito online.

O aplicativo Itaú abreconta promete abrir uma conta corrente online, sem precisar ir até uma agência (https://play.google.com/store/apps/details?id=com.itau.aco&hl=pt_BR).

A Conta Digital Intermedium conta com um aplicativo para smartphones com sistemas operacional IOS (iPhone) e Android, com ele é possível consultar a conta e realizar transações pelo celular. Uma das funções do aplicativo é permitir o depósito de cheques, basta tirar uma foto frente e verso do cheque para que o valor seja creditado em sua conta corrente.

- https://www.intermedium.com.br/conta-corrente.jsf.

De igual modo, também há o Banco Original (https://www.original.com.br/) e, similarmente, a Conta Super (http://www.contasuper.com.br/index.html).

Já a http://conta.mobi/ permite a realização de cobranças por boleto bancário, pagar contas sem filas, efetuar transferências bancárias (DOC e TED), organizar recebimentos e pagamentos, guardar dinheiro, utilizar cartão de débito Visa para efetuar saques e compras em estabelecimentos credenciados, fazer compras também fora do país com o cartão conta.MOBI Internacional.

Outros exemplos de bancos ou contas digitais:

- Moven (https://www.moven.com/);
- Fidor (https://www.fidor.de/);
- mBank (https://www.mbank.pl/);

- iGaranti (http://www.igaranti.com.tr/ig/);
- CTT (https://www.bancoctt.pt/);
- Banamex (https://www.banamex.com/);
- Nubank (https://www.nubank.com.br/);
- Atom (https://www.atombank.co.uk/);
- Celcoin (https://www.celcoin.com.br/);
- Neon (http://www.banconeon.com.br/);
- Maré (http://www.bancomare.com.br/);
- Sofisa direto (http://www.sofisadireto.com.br/);
- e-Dinheiro (https://edinheiro.net.br/).

Com o desenvolvimento dos meios de comunicação e da transferência eletrônica de dados, há ainda campo aberto para a criatividade humana encontrar novas formas de intermediar as trocas de aquisição de bens e serviços.

> "Vivemos numa sociedade em que os bens físicos perdem muito da primazia que tiveram nos séculos passados. Há uma clara desmaterialização dos bens." (http://www.domtotal.com/artigo.php?artId=4589).

> "A desmaterialização é um acontecimento oriundo da volatilidade das relações comerciais. Da origem dos títulos – quando da necessidade dos comerciantes em carregar consigo não moedas, para efetuar a compra, mas o título papel, que lhes trazia segurança no transporte – à informatização da comunicação. Um passo importante e civilizacional para os títulos de crédito fora a desmaterialização. Com alcance relativo, mas obtido através da evolução informática, realizou-se para melhor satisfação das necessidades contemporâneas." (https://jus.com.br/artigos/19882/da-documentacao-dos-direitos-em-papel-aos-titulos-de-credito-eletronicos).

Espera-se, assim, que sejam utilizados cada vez mais meios eletrônicos de pagamento que substituam o papel-moeda e as moedas metálicas convencionais.

- "O dinheiro, como o conhecemos, apareceu na Suécia por volta de 1660. Coincidentemente, o primeiro país do mundo no qual as cédulas devem ser extintas. É claro que houve outras moedas em civilizações mais antigas, como a China, romanos, gregos e fenícios. Mas, formalmente, o papel-moeda tornou-se aceito a partir da Suécia. Portanto, as cédulas com a qual os mais de 200 países do mundo fazem transações têm, pelo menos, 350 anos. Com a digitalização dos meios de pagamento, no entanto, é uma questão de tempo para que cédulas, moedas e o sistema financeiro tradicional passem por um processo de "uberização", ou seja, tal e qual tem acontecido com a ruptura do modelo tradicional de táxis no mundo, surja um (alguns) Uber para romper também com o setor." (10/05/2016; http://www.proxxima.com.br/home/proxxima/2016/05/10/o-uber-dos-bancos-tradicionais-esta-proximo.html).

- O Futuro do Dinheiro - Flavio Pripas | TEDxMauá 2015 - https://www.youtube.com/watch?v=Qs6WmELwNvg.

OUTROS MEIOS DE PAGAMENTO ELETRÔNICO OU DIGITAL

Senão vejamos alguns exemplos.

As **milhas aéreas** (Smiles, Multiplus, etc.) praticamente viraram uma moeda porque deixaram de ser simplesmente uma forma de adquirir passagens grátis e passaram a, também, serem aceitas como dinheiro para adquirir produtos de grandes redes varejistas. No mesmo caminho, outros programas de troca de pontos por prêmios também têm evoluído.

- http://oglobo.globo.com/economia/milhas-aereas-viram-moeda-criam-um-mercado-de-2-bilhoes-por-ano-6536567;
- https://www.dotz.com.br/Selecione-Sua-Regiao.aspx;
- https://www.petrobraspremmia.com.br/home/.

Segundo o site http://bastidoresdoturismo.blogspot.com.br/2007/12/quanto-vale-1-milha.html, o valor padrão ou médio de 1 (uma) milha aérea no mercado seria de US$ 0,02 (dois centavos de dólar). Entretanto, "Os valores variam todos os dias, por isso não colocamos nesta publicação o quanto valem suas milhas e na composição do mesmo são inseridas várias variáveis como: concorrência, valor médio do dólar (que implica em valor dos combustíveis e leasing das aeronaves dentre vários outros), disponibilidade dos assentos, e distância a ser percorrida pela aeronave do ponto de partida até o ponto de chegada, etc., etc." (https://flexmilhas.com.br/vender-milhas-preco/). Desse modo há muitas variáveis, fatores, elementos ou condicionantes a serem levados em consideração para poder avaliar o valor de cada milha aérea, tais como, por exemplos, a situação atual do mercado aéreo, de qual instituição são os pontos (Multiplus, Smiles, Vermelho, Plus e Black, Voeazul ou Tudo Azul, Aadvantage, Platinum, Black - Black Sig., Gold - Latam, Amigo, etc.), de qual companhia aérea são os pontos ou em que eles serão utilizados (Latam, Gol, Azul, Avianca, American Airlines, etc.), em que voo específico se pretender utilizar as milhas, etc.

Existem vários sites que negociam (compram e intermediam vendas) milhas aéreas e, obviamente, pagam valor inferior:

- http://www.vendasuasmilhas.com.br/;
- http://www.jbmilhas.com.br/;
- http://www.centralmilhas.com.br/;
- http://www.milhasaereas.net/;
- https://flexmilhas.com.br/;
- https://comprosuasmilhas.com.br/;
- http://www.elomilhas.com.br/;
- https://www.hotmilhas.com.br/como-vender-milhas/;
- http://www.lidermilhas.com/vender-milhas/;
- http://www.globalmilhas.com.br/default/default.asp;
- http://www.evsmilhasaereas.com.br/vender.html;
- http://figueiramilhasaereas.com.br/cotacao.php;
- https://clubmilhas.com.br/;
- http://www.milhasmais.com/;
- http://milhasbrasil.com.br/;
- https://www.webmilhas.com.br/.

Além das milhas aéreas várias outras empresas e estabelecimentos possuem **programas de fidelidade onde atribuem pontos de créditos** aos seus clientes, que podem ser convertidos em benefícios, descontos e aquisições de produtos e serviços. Assim, por exemplo, nas compras no site Ponto Frio (http://www.pontofrio.com.br/), adquire-se pontos no Multiplus (https://www.pontosmultiplus.com.br/home/), uma rede de fidelidade, com mais de 400 parceiros, onde se acumula os pontos de diversas origens, empresas e programas e pode trocá-los por passagens aéreas, hospedagem, ingressos para espetáculos, equipamentos eletrônicos, eletrodomésticos, acessórios esportivos e milhares de outros produtos e serviços.

Também, faz muito tempo, que existem os sites que dão **cupons de descontos**, informam ofertas ou realizam **compras coletivas**:

- https://www.groupon.com.br/cupons;
- http://www.peixeurbano.com.br/;
- http://www.tatubaratto.com/;
- https://uvarosa.com.br/;
- http://www.ofertaja.com.br/;
- http://www.posthaus.com.br/;
- http://sejasocio.samsclub.com.br/;
- http://www.umbarato.com/;
- http://www.bolsadeofertas.com.br/top-50-ranking-maiores-sites-compra-coletiva-2/;
- http://www.bolsadeofertas.com.br/brasil-ja-tem-mais-de-1000-sites-de-compras-coletivas/;
- http://www.valejunto.com.br/;
- https://www.cuponomia.com.br/;
- https://www.ciadosdescontos.com/;
- http://www.cupomgratis.net/;
- http://www.cupomvalido.com.br/;
- https://www.pegadesconto.com.br/;
- https://www.picodi.com/br/;
- http://www.saveme.com.br/;
- https://www.loucospordesconto.com.br/;
- http://www.descontosja.com/;
- http://www.hotcupom.com/;
- http://www.1001cupomdedescontos.com.br/;
- https://www.maiscupon.com.br/;
- https://www.meucupom.com/;
- https://www.cuponomia.com.br/;
- http://www.cuponeria.com.br/;
- http://www.couponita.net/;
- http://www.cupomoff.com.br/;
- http://cuponomize.com/;
- https://www.ofertalandia.com.br/;
- http://www.cantinhodasestrelas.com/;
- http://www.codigospromocionais.com/;

- http://www.cupomofertadesconto.com/;
- http://www.cupomdesconto.com.br/;
- https://cupom.com/;
- https://www.cupom.org/;
- http://www.valecupomdesconto.com.br/;
- http://www.encontredesconto.com.br/;
- http://blog.thiagorodrigo.com.br/.

De modo semelhante, o **Cielo Fidelidade** (https://cielofidelidade.com.br/) é um programa de relacionamento que transforma as vendas realizadas na máquina da Cielo em vantagens (descontos, prêmios e promoções).

Pelos sites http://www.goodfinancialcents.com/best-cash-back-credit-cards/ e http://www.mybanktracker.com/credit-cards é possível **comparar os cartões americanos** e, em http://www.comparecards.com/reward os programas de recompensas de cartões americanos. Já em https://www.comparaonline.com.br/cartao-de-credito e https://comparabem.com.br/cartoes-credito compara-se os **cartões de créditos brasileiros**. Também é possível comparar os bancos em https://wallethub.com/banks/ e http://banks.credio.com/; em http://www.findabetterbank.com/ é possível localizar mais bancos. Já no Brasil, é possível comparar as tarifas bancárias em http://www.febraban-star.org.br/ e http://www.febraban-star.org.br/CompararTarifaPasso1.asp. Sobre bancos europeus, há uma relação em https://pt.wikipedia.org/wiki/Lista_de_bancos_da_Europa.

Já a **Beblüe** (http://www.beblue.com.br/), similarmente à Nota Fiscal Paulista (http://www.nfp.fazenda.sp.gov.br/default.asp), **devolve em dinheiro parte do valor gasto em compras ("cashback")** com cartões de crédito ou de débito (Mastercard ou Visa), nos estabelecimentos da rede credenciada. Com exceção da Nota Fiscal Paulista, nos outros dois, é necessário baixar um aplicativo para o *smartphone*.

Portanto, já é possível ganhar dinheiro com compras através de programas ou plataformas de fidelidade denominadas **"cashback" ou "reward"**. "Cashback" significa "dinheiro de volta" e "reward" é recompensa. Desse modo, trata-se de uma espécie de reembolso de parte do

valor pago na aquisição de um produto online ou através do cartão. Semelhantes aos antigos programas de fidelidade onde se dava descontos, pontos ou milhas aéreas aos clientes, nesses programas dá-se dinheiro; mas de forma muito melhor do que os programas Nota Fiscal Paulista (http://www.nfp.fazenda.sp.gov.br/), Nota Fiscal Paulistana (http://nfpaulistana.prefeitura.sp.gov.br/) ou Nota Paraná (http://www.notaparana.pr.gov.br/).

- https://www.meliuz.com.br/;
- https://www.compraevolta.com.br/;
- http://www.cambyo.com.br/;
- https://www.poup.com.br/;
- http://br.beruby.com/;
- https://www.cashola.com.br/;
- http://bumeranggue.com.br/;
- http://www.maxximofidelidade.com.br/;
- http://www.retorna.com.br/;
- http://www.mooba.com.br/;
- https://www.ganhedevolta.com.br/;
- http://www.curtivendi.com.br/;
- http://www.bondsclub.com.br/;
- http://www.i9dinheirodevolta.com/;
- https://www.lyoness.com/br;
- http://www.h2h.com.br/;
- https://www.cartaoacredito.com/como-funciona-o-cashback-dos-cartoes-de-credito/;
- https://www.santander.com.br/br/pessoa-fisica/santander/cartoes/escolha-seu-cartao/todos-os-cartoes/santander-reward;
- http://www.cartaobrb.com.br/Portal/Home/Beneficios/CashBack;
- https://www.citibank.com.br/cartoes/cartoes_de_credito/cashback.html;
- https://www.citibank.com.br/welcomekit/cartoes-credito/cashback/platinum.html;

- https://www.credicard.com.br/beneficios/programa-pontos/cash-back;
- https://www.credicard.com.br/escolha/credicard-cash-back-international-mastercard;
- https://www.credicard.com.br/escolha/credicard-cash-back-international-visa;
- https://www.credicard.com.br/escolha/credicard-cash-back-gold-visa;
- https://www.nerdwallet.com/cash-rewards-credit-cards;
- https://www.ally.com/bank/cash-back-credit-card/;
- https://creditcards.chase.com/credit-cards/cash-back;
- https://www.discover.com/credit-cards/cashback-bonus/;
- http://www.comparaja.pt/cartao-de-credito/cashback;
- https://www.americanexpress.com/us/content/credit-cards/cash-back-cards/;
- http://www.wisebread.com/5-best-cash-back-credit-cards;
- http://www.comparaja.pt/blog/os-5-melhores-cartoes-de-credito-cashback-em-2015;
- http://www.moneycrashers.com/best-cash-back-credit-cards/;
- https://www.microsoft.com/emea/mos/.

Quem trouxe o *Cashback* para o Brasil foi a Compra3, em 2007, mas como na época, o e-commerce não tinha tanta força no país, a startup acabou fechando.

Hoje existem no Brasil, pelo menos, 107 **moedas sociais** (http://www.bcb.gov.br/pre/microfinancas/arquivos/horario_arquivos/apres_116.pdf). Elas foram criadas por bancos comunitários com o objetivo de que o dinheiro dos moradores circulasse dentro das próprias comunidades, ou seja, que o consumo local fosse estimulado e, assim, gerasse emprego e renda nessas regiões. O lastro delas é em real: uma Palma, por exemplo, tem de equivaler a um real. Além disso, a circulação é restrita a uma região e, diferente da moeda oficial, só aceita quem quiser.

O Instituto **Banco Palmas** (http://www.institutobancopalmas.org/) criou, com seus parceiros, uma plataforma eletrônica chamada "e-dinheiro", que em breve vai se espalhar por todo o Brasil através da Rede Brasileira de Bancos Comunitários: dos ribeirinhos da Amazônia às periferias de São Paulo, das quebradeiras de coco no Piauí aos quilombolas de Alcântara (MA), dos índios Tremembés no Ceará aos morros do Rio de Janeiro. Onde tiver Banco Comunitário lá estará o "e-dinheiro", independe de acesso à internet. Com o aplicativo "e-dinheiro" pode ser feito depósitos, transferências, pagamentos, recebimentos, sem precisar da intermediação de um banco tradicional. O custo para os usuários e comerciantes é bem menor que qualquer alternativa. Como a gestão é do Banco Comunitário, a plataforma permite a criação de circuitos econômicos locais ao se organizar uma rede de grandes e pequenos comércios na região/município por onde circulará o dinheiro eletrônico. Além dos ativos circularem na própria região gerando trabalho localmente, os rendimentos destas operações ficam para o Banco Comunitário reinvestir na comunidade.

- http://www.cdlfor.com.br/portal/index.php/pg/18965/dn-banco-palmas-desenvolve-1-moeda-social-eletronica;
- http://economia.estadao.com.br/noticias/geral,moeda-social-palmas-ganha-versao-eletronica,1701248.

O Banco Comunitário Muçubank, na comunidade de Muçumagro, em João Pessoa, lançou a moeda social "Muçu Real".

- http://www.fundacaomargaridaalves.org.br/2015/06/15/moeda-social-e-lancada-na-comunidade-de-mucumagro-joao-pessoa/.

Estes meios eletrônicos provavelmente farão parte da grande convergência tecnológica que se anuncia atualmente entre microcomputadores, telefones celulares, aparelhos de televisão e a biometria (leitura de impressões digitais, palma da mão, íris, etc.). Esta convergência geraria um só aparelho que exerceria todas estas funções, inclusive a função de pagamento e movimentação da conta bancária.

No final de 2011, o Google lançou o **Google Wallet** (https://www.google.com/wallet/) em parceria com o Citibank e MasterCard. Baseado na tecnologia NFC (*Near Field Communication*), o

Google Wallet permite aos usuários armazenar as informações de pagamento na nuvem e pagar por mercadorias pressionando o seu telefone no momento da compra. Esta forma de moeda eletrônica permite aos usuários pagar pela internet e, também, enviar e receber dinheiro. O Google já está emergindo como um banco, pois já possui licença bancária em vários países e o sistema operacional Android do Google funciona em muitos smartphones pelo mundo; sendo que quanto mais jovem a geração, maior a quota de mercado que o Google já tem pronta. O Plaso está sendo testado pelo Google e logo irá integrar o Google Wallet.

- http://www.techtudo.com.br/tudo-sobre/google-wallet.html.

Várias pessoas já efetuaram compras no https://play.google.com/store; seja de aplicativos, de livros, de jogos, de filmes, de músicas, etc.

Agora em substituição, há o **Android Pay** (https://www.android.com/pay/), que é essencialmente uma interface entre seus cartões de crédito e débito existentes, o seu telefone e leitores de cartão NFC em lojas.

O iPhone (da Apple) já é equipado com sensor de impressão digital para poder se tornar o cartão de crédito mais seguro. E a Apple está usando essa tecnologia em sua plataforma de música (iTunes), que é utilizada em maior proporção conforme descer na faixa etária.

A Apple já usa o **Apple Pay**, que é um sistema fechado de pagamentos baseado na tecnologia NFC (*Near Field Communications*), que se utiliza de radiofrequência para a transmissão de dados para consumar as compras. Foi concebido para se tornar um padrão de pagamentos, mas não tem sido usado realmente. Inclusive, algumas empresas americanas começaram a desativar pagamentos via Apple Pay, dando ênfase ao CurrentC (https://www.currentc.com/), um sistema alternativo ao qual estão afiliados. Entretanto, apesar de ter apoio econômico, o CurrentC não parece ter as qualidades necessárias para ser um sucesso: não usa NFC, mas sim códigos QR. Assim, o comprador tem que tirar o celular do bolso, abrir um aplicativo (de leitura de códigos QR), tirar uma foto do código em questão e

efetuar o pagamento. Trata-se de um processo muito mais complexo do que simplesmente "aproximar o iPhone com o dedo no *TouchID*.

- http://www.tecmundo.com.br/apple-pay/63027-funciona-apple-pay-o-novo-sistema-pagamentos-iphone.htm;
- http://www.tecinnfo.com.br/2015/04/currentc-rival-de-apple-pay-chega-nos.html;
- http://techapple.com.br/2014/12/como-usar-o-apple-pay-no-brasil/;
- http://exame.abril.com.br/tecnologia/noticias/americanos-rejeitam-sistema-de-pagamentos-moveis-da-apple;
- http://www.tudocelular.com/windows/noticias/n44782/CurrentC-o-rival-do-Apple-Pay-nao-pretende-suportar-aparelhos-Windows-Phone.html;
- http://pplware.sapo.pt/informacao/currentc-um-sistema-de-pagamentos-moveis-mais-seguro/.

O Apple Pay tem o apoio das principais operadoras de cartão de crédito dos Estados Unidos, como Mastercard, American Express e Visa, e de bancos como Chase, Citi, Capital One, Bank of America e Wells Fargo, mas perdeu espaço com algumas redes de varejo. CVS, Rite Aid, Wal-Mart e Target se juntaram para desenvolver uma solução própria e deixaram de aceitar o meio de pagamento da Apple.

A Samsung comprou a *startup* norte-americana de serviços de carteira eletrônica Loop Pay (https://www.looppay.com/), mostrando a intenção de lançar um serviço de pagamentos por smartphone para competir com a rival Apple, que colocou no mercado, em 2014, o Apple Pay. Enquanto o Apple Pay funciona exclusivamente via NFC, o **Samsung Pay** tem suporte também à leitura magnética (*Magnetic Secure Transmission*), que é a tecnologia presente nas máquinas da maioria das lojas do mundo. Detalhe, será possível fazer compras pela televisão.

- http://olhardigital.uol.com.br/noticia/samsung-cria-pagamento-facilitado-para-apps-de-smart-tvs/50279.

A LG está trabalhando no seu próprio sistema de pagamentos, o "**LG Pay**". Mas, na contramão da tendência de desmaterialização, projetou um

cartão físico, em branco programável, com um chip de CI (Circuito Integrado).

Para não ficar para trás, a Microsoft fez uma plataforma de pagamentos que vem sendo chamada de ***Microsoft Payments***.

- http://www.techtudo.com.br/noticias/noticia/2015/04/microsoft-payments-apple-pay-e-google-wallet-podem-ganhar-novo-rival.html;
- https://www.windowsteam.com.br/microsoft-parece-ter-planos-para-criar-o-seu-proprio-sistema-de-pagamentos-via-nfc-e-mais/.

O **FaceBook** (https://www.facebook.com/) recebeu aprovação de licença bancária nos Estados Unidos e na Irlanda (onde está sua sede fiscal europeia) para oferecer serviços bancários usando sua vasta rede on-line em toda a Europa; com o que seus usuários poderão armazenar dinheiro eletrônico na rede social e usá-lo para fazer compras online ou trocar com outras pessoas.

- http://derisio.com.br/2015/07/o-banco-do-facebook/;
- http://blogs.estadao.com.br/link/como-o-facebook-ganha-dinheiro/;
- http://oglobo.globo.com/economia/facebook-mira-servicos-financeiros-quer-emitir-dinheiro-eletronico-12185635;
- http://www.ihu.unisinos.br/noticias/40314-facebook-impoe-sua-propria-moeda-virtual-na-internet;
- http://meiobit.com/312385/facebook-messenger-sistema-pagamentos/;
- http://br.wwwhatsnew.com/2015/05/como-funciona-o-sistema-de-pagamentos-no-facebook-messenger/;
- https://mikasia.wordpress.com/2016/03/01/facebook-to-czy-bank/.

Os clientes do banco mBank (https://www.mbank.pl), já podem fazer pagamentos via FaceBook.

- https://www.mbank.pl/pobierz/zasady-realizacji-przelewow-na-profil-facebookowy.pdf.

“FaceBook Credits” ou "FaceBook Game Cards" é a moeda usada nos jogos e aplicativos que funcionam no FaceBook (https://www.facebook.com/gamecards).

- https://www.facebook.com/FacebookApps/?fref=ts.

Desse modo, o Google e o FaceBook podem emergir a qualquer momento como contas eletrônicas para uma base de clientes que cada vez mais se afastam de bancos físicos, tornando-os obsoletos exatamente como a Amazon (livraria virtual que vende livros eletrônicos) eliminou um monte de livrarias.

> "De acordo com uma pesquisa realizada pela Fujitsu - que se tem uma divisão de finanças - 20 por cento dos entrevistados disseram que usam o FaceBook, Google ou Amazon para comprar os serviços bancários ou de seguros, se disponível." (http://thenextweb.com/facebook/2016/05/05/banks-google-facebook-amazon/#gref).

> "No Reino Unido, que é considerado o centro financeiro mundial por excelência, mais de 2 milhões de pessoas não têm contas bancárias. Por outro lado, cerca de 90% dessas pessoas têm smartphones, pelos quais é possível fazer qualquer transação financeira sem bancos que intermedeiem o processo. E são vários os setores envolvidos – os consumidores, o varejo, os fornecedores de celulares, os criadores de apps, os desenvolvedores de softwares, os próprios bancos tradicionais e os fornecedores de tecnologia. Quando se fecha o círculo com esses fornecedores numa cadeia que inclui o e-commerce e o pagamento sem transações bancárias, definitivamente, é o fim do dinheiro." (10/05/2016; http://www.proxxima.com.br/home/proxxima/2016/05/10/o-uber-dos-bancos-tradicionais-esta-proximo.html).

> - https://medium.com/enrique-dans/welcome-to-googlebank-facebook-bank-amazon-bank-and-apple-bank-c9c3955006d4#.yzh4fa3vq.

A **Advanced Cash** (http://advcash.com/en/), um sistema de pagamento online versátil e de fácil utilização, anunciou que começou a trabalhar com a

BitPay (https://bitpay.com/), líder mundial em processamento de pagamentos com bitcoins, para dar andamento à sua funcionalidade de bitcoin. A Advanced Cash oferece uma plataforma de *e-currency* (moeda eletrônica) que inclui carteiras eletrônicas, cartões de débito plásticos ou virtuais, transferências internacionais de valores, pagamentos em lote para empresas, além de muitos outros recursos.

O Citibank está trabalhando na criação da sua própria moeda digital chamada de **Citicoin**.

- http://www.tudocelular.com/mercado/noticias/n57358/Citigroup-cria-a-sua-propria-moeda-digital.html.

O grupo JP Morgan também está tentando patentear sua própria moeda digital.

Outro campo que promete mudanças no futuro é o das moedas únicas continentais. O sucesso do Euro como moeda única europeia despertou o interesse de outras organizações continentais pelo tema, que tem como principal atrativo o incremento do comércio intracontinental. Ásia, América do Sul e África são continentes que estudam a possibilidade de implementar as suas moedas únicas em um futuro próximo.

MOEDA DIGITAL OU ELETRÔNICA

A **moeda digital ou eletrônica** (*eletronic money*, *eletronic cash* ou *digital cash*), pelo fato de estar em constantes desenvolvimento e evolução, inclusive por não ser regulamentada e nem padronizada, ainda não possui uma definição precisa ou unânime; mas refere-se às transações efetuadas através de aparelhos ou sistemas eletrônicos inteligentes (caixas/terminais eletrônicos, computadores, *notebooks*, *tablets*, *smartphones*, smart TVs, consoles de games, chips, cartões smarts ou inteligentes de débito e/ou crédito, etc.) visando à transferência de créditos de uma pessoa para outra. Pelo fato de sua definição ser genérica, ampla e imprecisa até os cartões de recargas (de telefone, de TV por assinatura, de jogos online, etc.) poderiam estar incluídos.

A criptomoeda ("cryptocurrency") ou moeda de criptográfica ("crypto currency") é um meio de troca ("medium of exchange") usando criptografia ("cryptography") para proteger as transações (*transactions*) e para controlar a criação de unidades adicionais de moeda ("coin" ou "currency"). Portanto, bitcoin é uma das criptomoedas ("cryptocurrencies") existentes. Já a palavra "altcoins", a princípio, é uma abreviação da expressão "coin alternative" (moeda alternativa); mas, na verdade, é muito mais do que isso, se trata de uma sigla de trocadilho abreviado da expressão "bitcoin alternative" (alternativa ao Bitcoin). Portanto se refere às outras moedas criptográficas com exceção da bitcoin.

A primeira discussão sobre criptografia em meios eletrônicos de pagamento surgiu em 1982 com um artigo de David Chaum a respeito de assinaturas cegas para pagamentos eletrônicos não rastreáveis (David Chaum. *Blind signatures for untraceable payments. In Advances in cryptology*, pages 199–203. Springer, 1983). Nele, o autor propôs um sistema onde chaves criptográficas validam notas assinadas por uma entidade certificadora, no caso, um banco, possibilitando transferir valores através de redes de computadores. Este conceito deu origem a uma empresa chamada DigiCash em 1990, que até 1998 competiu no mercado de pagamentos online, quando pediu falência, devido à preferência dos usuários pelo uso do cartão de crédito (Julie Pitta. *Requiem for a Bright Idea*. Forbes http://www.forbes.com/forbes/1999/1101/6411390a.html, Janeiro 1999).

Ressalta-se que **não se pode confundir o pagamento com a moeda**. O pagamento é amplo e genérico se referindo a qualquer tipo ou espécie de moeda, de dinheiro, crédito ou meio de troca. Já a moeda eletrônica ou digital, por definição, exclui as moedas convencionais (físicas ou materiais); ao invés disso, um valor monetário é eletronicamente creditado ou debitado. A moeda é apenas umas das espécies, modalidades, tipos, instrumentos ou formas com que se efetua um pagamento.

Quando se usa a expressão "dinheiro eletrônico" está se referindo a uma forma de pagamento eletrônica (um valor monetário é eletronicamente creditado ou debitado); mas não necessariamente a uma moeda digital.

O dinheiro eletrônico ou digital é um sistema composto de unidades ou símbolos de valor monetário, devidamente codificado (criptografado), representando montantes de dinheiro, que podem ser convertidos em dinheiro físico.

A moeda na forma digital (mecanismos de pagamento por via eletrônica) implica redução significativa nos custos de transação. E, seu surgimento e desenvolvimento, também estimulam novas oportunidades de negócios.

A moeda digital (e-moeda, *e-currency*, e-metal, *e-money*, *digital gold currency*, moeda criptográfica, *cryptocurrency*, etc.) é a moeda não física (não impressa, cunhada e nem palpável) e nem emitida (atualmente também não garantida) por qualquer país (descentralizada). Algumas são de emissão de empresas ou instituições financeiras e outras são de criação coletiva.

As moedas virtuais não são emitidas nem garantidas por uma autoridade monetária. Algumas são emitidas e intermediadas por entidades não financeiras e outras não têm sequer uma entidade responsável por sua emissão. Em ambos os casos, as entidades e pessoas que emitem ou fazem a intermediação desses ativos virtuais não são reguladas e nem supervisionadas por autoridades monetárias de qualquer país.

Elas não têm garantia de conversão para a moeda oficial; tampouco são garantidos por ativo real de qualquer espécie. O valor de conversão de um

ativo conhecido como moeda virtual para moedas emitidas por autoridades monetárias depende da credibilidade e da confiança que os agentes de mercado possuam na aceitação da chamada moeda virtual como meio de troca e das expectativas de sua valorização. Não há, portanto, nenhum mecanismo governamental que garanta o valor em moeda oficial dos instrumentos conhecidos como moedas virtuais, ficando todo o risco de sua aceitação nas mãos dos usuários.

Em síntese, não se pode confundir moeda eletrônica com moeda virtual. A primeira não é uma moeda, mas sim um meio de pagamento, tal como um cartão de crédito ou transferências eletrônicas de uma conta bancária convencional. Já a moeda virtual é gerada (já nasce) em ambiente virtual através de algoritmos e não estão vinculadas a outra moeda.

O Banco Central do Brasil (Comunicado n.º 25.306/2014) esclareceu que **as chamadas moedas virtuais não se confundem com a "moeda eletrônica" de que tratam a Lei n.º 12.865/2013** e sua regulamentação infralegal. Moedas eletrônicas, conforme disciplinadas por esses atos normativos, são recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento denominada em moeda nacional. Por sua vez, as chamadas moedas virtuais possuem forma própria de denominação; ou seja, são denominadas em unidade de conta distinta das moedas emitidas por governos soberanos, e não se caracterizam dispositivo ou sistema eletrônico para armazenamento em Reais.

- Comunicado 25.306/2014 - https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277;

- Lei 12.865/2013 - http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm.

Coin, é uma palavra inglesa que significa "moeda" e o termo "bit" é usado comumente para indicar algo relativo a computadores.

Bitcoin não é mais uma das formas disponíveis de pagamento virtual. Sequer é uma simples forma de pagamento. Bitcoin é uma moeda.

Apesar de que a bitcoin não foi a primeira moeda digital, seu protocolo criou conceitos que são usados por várias outras moedas digitais.

Alguns exemplos bem-sucedidos de moedas virtuais anteriores a bitcoin são os “Linden dollars” do *Second Life* (http://secondlife.com/?lang=pt-BR) e os e-Rewards (http://www.e-rewards.com.br/home.do?lc=pt_BR) do Upromise.

"Nem sempre a primeira versão vinga. Antes do Google se afirmar como primeiríssimo motor de pesquisa houve os pioneiros ”Lycos” e “Altavista”. Nas moedas digitais pode acontecer que o Bitcoin não seja mais do que o lançamento de uma nova ideia para o mundo das finanças, uma prova de conceito para o aparecimento de novas formas de valorização de ativos subjetivos mais do que de valor intrínseco!" (Francisco Lavrador Pires *in* http://elearningclub.blogspot.com.br/2013/11/moedas-alternativas-em-xcoins-moedas.html).

Obviamente o uso de qualquer moeda digital implica em algum tipo de identificação segura do titular dos créditos; seja através de senhas, códigos, chaves, assinatura digital, reconhecimento facial, leitor de impressão digital, reconhecimento de voz, escâner de retina, certificado digital, etc.

SEGURANÇA DIGITAL

Outra característica dos pagamentos eletrônicos (*electronic payments*) e das moedas digitais (*digital coins*) é que costumam ter as informações criptografadas para fins de segurança e sigilo. **Encriptação** (*encryption*) é a transformação de dados em alguma forma ilegível, com o propósito de garantir privacidade da mensagem. A **decriptação** (*decryption*) é o inverso: é a transformação de dados ilegíveis (incompreensíveis) numa mensagem inteligível (compreensível). A encriptação e a decriptação utilizam uma chave secreta (*secret key*). Alguns algoritmos (*algorithms*) utilizam a mesma chave para encriptar e decriptar, enquanto outros utilizam chaves diferentes para estas operações. À criptografia que utiliza as mesmas chaves para encriptação e decriptação é a simétrica; já a assimétrica é quando chaves diferentes são utilizadas: uma privada (conhecida apenas por seu possuidor) para encriptar e/ou assinar e outra pública (conhecida por todos) para decriptação e verificação de assinatura.

A palavra **criptografia** tem origem grega nas palavras "kryptós" e "gráphein" e significa a arte de escrever em códigos de forma a esconder a informação na forma de um texto incompreensível. A criptografia, portanto, possui a finalidade de codificar uma informação de forma que somente o emissor e o receptor (*receiver*) possam acessá-la, evitando que um estranho consiga compreendê-la. A informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de cifragem (*encryption*) e o processo inverso, ou seja, obter a informação original a partir do texto cifrado, chama-se decifragem (*decipher*).

- http://cartilha.cert.br/criptografia/.

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave (*key*) que é utilizado para definir como o programa irá se comportar. Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta,

basta cifrar a informação e manter em sigilo (segredo) a chave; daí o nome chave privada (*private key*) ou chave secreta (*secret key*).

Uma **chave criptográfica** (*cryptographic key*) é um conjunto de bits utilizado com um algoritmo capaz de codificar e de decodificar informações. Sem a chave correta é impossível acessar a informação.

As chaves criptográficas podem ser simétricas (mesma chave para encriptar e decriptar) ou assimétricas (chaves diferentes para encriptar e decriptar). Por outras palavras, atualmente, existem dois tipos de criptografia: a simétrica e a de chave pública (*public key*).

Chave simétrica (*symmetric key*) é um tipo de chave criptográfica mais simples, onde o emissor e o receptor fazem uso da mesma chave compartilhada previamente entre eles (remetente e destinatário); isto é, uma única chave é usada na codificação e na decodificação da informação.

Explica-se. O emissor de uma mensagem utiliza um algoritmo de criptografia (*encryption algorithm*) e uma chave secreta para transformar a mensagem original em um texto cifrado. O destinatário da referida informação criptografada, por sua vez, utiliza o algoritmo de descriptografia (*decryption algorithm*) correspondente para decifrá-la (ou descriptografá-la) e a mesma chave para transformar o texto criptografado na mensagem original. Um terceiro (estranho ou intruso), por não possuir a chave secreta (privada), mesmo que conheça e possua o algoritmo (de desencriptação), não conseguirá decifrar a mensagem. Desse modo, a segurança do sistema baseia-se na chave específica que deve utilizada na mensagem específica e não no algoritmo empregado em qualquer mensagem ou com qualquer pessoa. Em razão disso, o remetente e o destinatário da mensagem devem manter a chave em segredo.

A criptografia simétrica, portanto, realiza a cifragem e a decifragem de uma informação através de algoritmos que utilizam a mesma chave para garantir o sigilo na transmissão e armazenamento de dados. Como a mesma chave deve ser utilizada na cifragem e na decifragem, a chave deve ser compartilhada entre quem cifra e quem decifra os dados. O processo de compartilhar uma chave é conhecido como troca de chaves. A troca de

chaves deve ser feita de forma segura; vez que todos que conhecem a chave podem decifrar a informação cifrada ou mesmo reproduzir uma informação cifrada.

Desse modo, como cada par (emissor e o receptor) necessita de uma chave para se comunicar de forma segura, exige-se uma infinidade de quantidade de chaves e a necessidade de saber onde cada uma dessas inúmeras chaves deve ser usada. Outro problema da criptografia simétrica é que ela não garante a identidade de quem enviou ou recebeu a mensagem (autenticidade e não-repudiação).

Existem vários **algoritmos que usam chaves simétricas**, como, por exemplos, DES, IDEA, RC, 3DES, Twofish, Blowfish, etc.

- DES (*Data Encryption Standard*), criado pela IBM em 1977, faz uso de chaves de 56 bits, permite 72 quatrilhões de combinações e opera em blocos de 64 bits. É usado na Internet em conexões Web segura, pois o SSL utiliza do DES.

- IDEA (*International Data Encryption Algorithm*), criado em 1991, é um algoritmo semelhante ao DES que faz uso de chaves de 128 bits.

- RC (*Ron's Code ou Rivest Cipher*), é um algoritmo muito utilizado em e-mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões (RC2, RC4, RC5 e RC6), que se diferenciam pelo tamanho das chaves. O RC2 é 2 vezes mais rápido que o DES; já o RC4 é 10 vezes mais rápido.

- AES (*Advanced Encryption Standard* ou Padrão de Criptografia Avançada) é baseado no DES. Também conhecido por Rijndael, é uma cifra de bloco adotada como padrão de criptografia pelo governo dos Estados Unidos.

- 3DES (ou Triple DES) é uma variação do DES, de 112 ou 168 bits, que utiliza três ciframentos sucessivos, podendo empregar

versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.

- Blowfish, algoritmo de 32 a 448 bits, que permite escolher entre maior segurança ou melhor desempenho através de chaves de tamanho variável. Sua versão aperfeiçoada é o Twofish, que concorre com o AES.

Em agosto de 1999, NIST - *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos) selecionou cinco algoritmos de análise mais extensa:

- MARS, apresentado por uma grande equipe de IBM Research;
- RC6, apresentado pela RSA Segurança;
- Rijndael (ou AES), apresentado por dois criptógrafos belgas, Joan Daemen e Vincent Rijmen;
- Serpente, apresentado por Ross Andersen, Eli Biham e Lars Knudsen;
- Twofish, apresentado por uma grande equipe de pesquisadores, incluindo criptógrafo respeitada da Counterpane, Bruce Schneier.

As implementações de todos esses itens supra foram testadas extensivamente nas linguagens de programações ANSI, C e Java, atentando-se quanto à rapidez e segurança na criptografia e descriptografia, chave de tempo, configuração do algoritmo e resistência a vários ataques, tanto em sistemas de hardware e *software-centric*. Os membros da comunidade criptográfica global conduziram análises detalhadas (incluindo algumas equipes que tentaram quebrar suas próprias apresentações). Depois de muitos *feedbacks* (comentários de retorno), debates e análises, a cifra Rijndael (uma mistura de sobrenomes dos criadores Daemen e Rijmen) foi selecionada como o algoritmo proposto para a AES em outubro de 2000.

Assim, a AES tornou-se eficaz como um padrão do governo federal americano em 2002.

A **criptografia assimétrica** (*asymmetric cryptography*) não utiliza somente uma chave (secreta), mas duas: uma privada e outra pública. Portanto, a chave assimétrica está baseada no conceito de par de chaves. O emissor deve criar uma chave de codificação e enviá-la ao receptor, é a chave pública. Já a outra chave (privada ou secreta) deve ser criada para a decodificação. Qualquer pessoa pode enviar uma mensagem ao destinatário se possuir a chave pública do destinatário (a qual é amplamente divulgada); mas as mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente.

Desse modo, os algoritmos de chave pública operam com duas chaves distintas: **chave privada (*private key*) e chave pública (*public key*)**. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja revertida pela outra. Na verdade, qualquer uma das chaves é utilizada para cifrar uma mensagem e a outra (restante) para decifrá-la (vide explicação abaixo). A chave privada (ou secreta) deve ser mantida em sigilo (segredo) e protegida por quem gerou as chaves. A chave pública, por sua vez, é disponibilizada e tornada acessível a qualquer indivíduo que deseje se relacionar com o proprietário da chave privada correspondente.

O emissor ou emitente (*issuer*) que deseja enviar uma informação sigilosa deve utilizar a chave pública do destinatário para cifrar a informação. Para isto é importante que o destinatário disponibilize sua chave pública, utilizando, por exemplo, diretórios públicos acessíveis pela Internet.

O sigilo é garantido, já que somente o destinatário (*recipient*) que possui a chave privada conseguirá desfazer a operação de cifragem; ou seja, decifrar e recuperar as informações originais. Por exemplo, para o remetente (*sender*) poder compartilhar uma informação de forma secreta com o destinatário, o remetente deve cifrar (ou encriptar) a informação (*information*) ou mensagem (*message*) usando a chave pública do destinatário. Somente o destinatário pode decifrar a informação, pois somente ele possui a chave privada correspondente àquela chave públlica.

No processo de autenticação (*authentication*), as chaves são aplicadas no sentido inverso ao da confidencialidade (*confidentiality*).

O autor de um documento utiliza sua chave privada para cifrá-lo de modo a garantir a autoria em um documento ou a identificação em uma transação. Esse resultado só é obtido porque a chave privada é conhecida exclusivamente por seu proprietário.

O algoritmo assimétrico (*asymmetric algorithm*) mais utilizado é o RSA (*Rivest, Shamir and Adleman*). A premissa adotada no RSA é a de que é fácil multiplicar dois números primos para se obter um terceiro número, mas extremamente difícil recuperar os dois números primos a partir do terceiro número deles derivado. Assim, o processo de geração da chave pública envolve a multiplicação de dois números primos grandes. Já a derivação da chave privada (a partir da chave pública) envolve fatorar um número grande. E se o número for grande o suficiente, ninguém pode fazer isto em uma quantidade de tempo razoável.

Números primos são os números naturais que têm apenas dois divisores diferentes: o 1 e ele mesmo. Na verdade, se considerarmos os sinais (positivos e negativos), os números primos são os números inteiros que admitem exatamente 4 divisores. Assim, por exemplo, os únicos divisores de 3 são: -3, -1, 1 e 3. Essa divisão não pode resultar em número incompleto (possuir somente zero à esquerda da vírgula), mas pode possuir resto ou centavos. O quociente (resultado) também não pode ser um número exato. Diante essas explicações, o número 1 não é primo, pois possui apenas um número divisor que é ele mesmo. Já o número 0 não pode ser primo porque é uma indeterminação. Para verificar se um número é primo, ou não, deve-se dividir o número investigado começando pelo menor número primo, que é o número 2, e posteriormente com os demais números naturais primos, até que seu quociente (resultado) seja menor, igual ou o próprio número que está sendo dividido. Assim, por exemplo, na divisão de 127 por 11, o resultado (11,54545454545455) é 11 com 6 de resto. Logo, o número 127 é primo. Todos os números pares são divisíveis por 2, por isso, se o número investigado for par (terminado em 0, 2, 4, 6 ou 8), automaticamente é um

número composto (possui mais de dois divisores) e, como tal, não é um número primo. O número 2 é o único número primo que é par.

O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de *hash*, é chamada de assinatura digital.

Como a utilização da criptografia assimétrica na assinatura digital é inviável por causa da lentidão do seu algoritmo, utiliza-se a função *hashing*; que gera um valor de tamanho fixo derivado da mensagem a ser assinada.

Se a chave privada for usada para criptografar uma mensagem, o uso das chaves passa a ser invertido (a chave privada encripta e a chave pública decifra) e, assim, todos os que possuem a chave pública conseguirão decifrar a mensagem. Entretanto, somente quem tem a chave privada conseguirá escrevê-la. Através desse procedimento, a mensagem deixa de ser secreta, mas se torna uma mensagem com garantia de autenticidade, já que somente a pessoa que possui a chave privada poderá criptografá-la. Este é o processo da assinatura digital (*digital signature*).

O resumo criptográfico (*cryptographic summary*) é o resultado retornado por uma função de *hash*. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente. Esse mesmo procedimento é utilizado nos certificados digitais (*digital certificates*).

> "A assinatura digital consiste então no uso da função de hash junto ao documento a ser transmitido e na aplicação do esquema de chaves. No processo de conferência, deve-se calcular o hash e efetuar a decifragem com a chave pública do emissor. Se houver alterações na informação, por menores que sejam, essas mudanças farão o hash ser diferente. Daí as partes envolvidas saberão que o documento pode, por exemplo, ter sido adulterado." (http://www.infowester.com/assincertdigital.php).

A criptografia também prevê mecanismos para a autenticação (*authentication*). Uma assinatura digital relaciona um documento ao

possuidor de uma determinada chave privada e um *timestamp* (carimbo de data e hora) digital relaciona um documento a sua criação num determinado tempo. Estes mecanismos podem ser utilizados para controlar acessos a um disco compartilhado, uma instalação de alta segurança etc.

HASH

O **"Hash Code"** (resumo criptográfico, assinatura do arquivo ou sumário da mensagem) é um número que representa de forma única e exclusiva um arquivo ou dado específico como forma de identificá-lo e garantir sua integridade, autenticidade e validade.

> "Uma função hash é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função hash são chamados valores hash, códigos hash, somas hash (hash sums), checksums ou simplesmente hashes." (https://camarj.zendesk.com/hc/pt-br/articles/215138758-O-que-%C3%A9-HASH-).

> "A função Hash (Resumo) é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções Hash são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos. Dessa forma, as funções Hash são largamente utilizadas para buscar elementos em bases de dados, verificar a integridade de arquivos baixados ou armazenar e transmitir senhas de usuários." (http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html).

Um **algoritmo** é caracterizado por qualquer forma de resolver um problema de forma procedural a partir de padrões e regras. Assim, em informática trata-se de um programa (*software*) que realiza, passo a passo, procedimentos para solucionar um problema.

> "Um algoritmo nada mais é do que uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa. Ele não responde a pergunta “o que fazer?”, mas sim “como fazer”. Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa." (http://www.tecmundo.com.br/programacao/2082-o-que-e-algoritmo-.htm).

Uma cadeia (*chain*) de caracteres ("**string**") é uma sequência de caracteres, geralmente utilizada para representar palavras, frases ou textos de um programa.

> "Um hash (ou escrutínio) é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando 1/2 byte cada. O conceito teórico diz que “hash é a transformação de uma grande quantidade de informações em uma pequena quantidade de informações”. Essa sequência busca identificar um arquivo ou informação unicamente. Por exemplo, uma mensagem de correio eletrônico, uma senha, uma chave criptográfica ou mesmo um arquivo. É um método para transformar dados de tal forma que o resultado seja (quase) exclusivo. Além disso, funções usadas em criptografia garantem que não é possível a partir de um valor de hash retornar à informação original." (http://www.forum-invaders.com.br/vb/showthread.php/39628-O-que-%C3%A9-hash-e-quais-as-suas-principais-ferramentas).

> "Um hash, também chamado de "digesto", é uma espécie de "assinatura" ou "impressão digital" que representa o conteúdo de um fluxo de dados. Com certa frequência os hashes são chamados de checksum, o que provoca alguma confusão com os verdadeiros checksums, os quais têm aplicações e cálculos totalmente diferentes. Um hash pode ser comparado com um selo de embalagem que indica clara e inequivocamente se a embalagem já foi aberta ou violada. [..]. Os hashes produzem "selos de segurança" de comprimento fixo, não importa o comprimento do fluxo de dados ou do arquivo que representem. Qualquer alteração efetuada no arquivo, por mínima que seja, altera substancialmente o resultado hash. Isto ocorre porque, mesmo se apenas um dos bits do arquivo for alterado, muitos bits do resultado serão afetados. Este comportamento é conhecido como efeito avalanche." (http://www.numaboa.com.br/criptografia/hashes/340-o-que-e-hash).

O ***hash***, em síntese, é uma função ou fórmula matemática aplicada sobre um conjunto de dados gerando outro número. É praticamente como um digito verificador (*verifying digit*) ou algarismo de controle usado em documentos de identificação (RG, CPF, CNPJ, PIS, etc.), códigos de pagamentos (boletos bancários, código de barras, etc.), códigos identificadores (agência, conta corrente, etc.); o qual se trata de um ou mais algarismos (números ou dígitos) acrescentados a um valor original (tornando-se parte deste) e calculados a partir deste através de um determinado algoritmo. Em linguagem simples, o usuário deve saber informar com precisão qual é o único número, que aplicado à fórmula matemática complexa e desconhecida pelo usuário, resulta num valor específico esperado pelo destinatário. Didaticamente, é como se estivesse esperando a única resposta correta de uma pergunta não informada, mas existem infinitas dessas perguntas diferentes tendo cada qual a sua resposta exclusiva.

Também se assemelha à demonstração de resultado ou prova de uma operação matemática. Assim, por exemplo, dentre as várias provas em matemática, na prova real (ou operação inversa), é possível conferir se o resultado está correto realizando o procedimento invertido, inverso ou de trás para frente. É como um procedimento de *checksum* (ou soma de verificação). Desse modo, se o usuário conhece a fórmula matemática aplicada na verificação (*verification*), se torna possível descobrir qual deve ser o valor correto a ser informado. Esse é o raciocínio de programas geradores de números ou chaves seriais (*serial key generator* ou *keygen*) falsas, mas funcionais de programas de computadores pagos. De igual forma, existem os programas geradores de números de CPF (falsos, mas funcionais) para fins exclusivos de testes de softwares, sistemas e sites. Tais números falsos (de serial e de CPF) não sofrem a mensagem de erro “número

inválido” (*invalid number*) ou “número incorreto” (*incorrect number*), mas não estão imunes às de “número inexistente” (*non existent number*), “chave já utilizada” (*already used key*) ou “número incompatível ou divergente com os demais dados”.

Dificuldade (*difficulty*), dificuldade do Bitcoin (*Bitcoins difficulty*), dificuldade de mineração (*mining difficulty*) ou dificuldade de hash (*hash difficulty*) é uma medida de quão difícil é encontrar um *hash* (novo bloco) abaixo de um determinado alvo (*target*). A dificuldade, em si (na prática), é um número de 256 bits que coloca um limite máximo para o valor do *hash*; a grosso modo, a dificuldade é quantos zeros existem antes de chegar aos números validadores (*validator numbers*). Portanto, o grau de dificuldade para descobrir o valor de *hash* está na quantidade de zeros no início do cabeçalho do bloco (*block header*). A dificuldade Bitcoin começou em 1 e nunca pode ir abaixo disso. A dificuldade estabelece a quantidade de trabalho, em média, que deve ser feita para conseguir resolver um bloco (criar uma nova unidade de Bitcoin) na rede Bitcoin. Os blocos, portanto, são extraídos através da resolução de *hashes* abaixo de um determinado limiar (meta, objetivo ou alvo), através do poder de computação (processamento) computacional; tal como, por exemplo, uma fórmula matemática onde se exige que o resultado da operação seja menor ou igual a determinado número e quem conseguir aproximar mais o resultado do número alvo é o vencedor (um dos critérios de definição de qual é a corrente principal). É similar ao jogo de baralho 21. Desse modo, o cabeçalho do bloco não pode exceder ao valor do alvo. Com outras palavras, o objetivo da mineração (procedimento de tentativa e erro através do *nonce*) é encontrar um valor para o *nonce* (número aleatório) que resulte em um *hash* (valor) de cabeçalho de bloco menor do que o valor da dificuldade alvo (*target*). Diante disso, a mudança do grau de dificuldade de *hash* de um bloco (*block*) possui um enorme impacto (influência ou repercussão) sobre a quantidade de poder computacional necessário para resolver (criar) o próximo bloco. O algoritmo (*hashcash*) de prova de trabalho (PoW - *proof-of-work*) é que define o grau de dificuldade (*difficulty*) de mineração da criptomoeda. A dificuldade do processo de mineração do Bitcoin é atualizada a cada 2.016 blocos e cresce (aumenta) à medida que mais poder computacional é disponibilizado em mineração e/ou mais caçadores de recompensa participam da disputa ("corrida do ouro"). Explica-se. A cada

2.016 blocos, a média de *hashrate* durante esse período é medida e a dificuldade é reajustada com base nesse poder de processamento. Quanto maior a dificuldade, mais difícil será a mineração. E quanto maior a dificuldade de mineração, maior poder de processamento será exigido. O principal objetivo da dificuldade no Bitcoin é manter o prazo de 10 (dez) minutos para as confirmações (*confirmations*) das transações (*transactions*) na rede.

Confira a *mining difficulty* (dificuldade de mineração) na rede Bitcoin em https://tradeblock.com/bitcoin/historical/1d-f-diff_avg-01071-blksize_per_avg-01071.

O **RSA** é um algoritmo assimétrico que utiliza números primos e é o mais amplamente utilizado em chaves públicas, por ser uma das mais poderosas formas de criptografia de chave pública conhecidas. Seu nome é a sigla do sobrenome de seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT (*Massachusetts Institute of Technology* - Instituto de Tecnologia de Massachusetts), nos Estados Unidos. A premissa do RSA é que apesar de ser fácil multiplicar dois números primos para obter um terceiro número, é muito difícil recuperar os dois primos a partir desse terceiro número. Esse procedimento matemático se chama fatoração (decomposição de um número em fatores primos). Desse modo, gerar uma chave pública envolve multiplicar dois números primos grandes e qualquer um pode fazer isso. Entretanto, derivar a chave privada a partir da chave pública envolve fatorar um número enorme. Assim, se o número for grande o suficiente e bem escolhido, em tese, ninguém poderá fazer isso durante uma quantidade de tempo razoável. Por exemplo, no filme "O Jogo da Imitação" (*The Imitation Game*) conta-se a história (e não estória) do matemático Alan Turing, que precisou criar uma supermáquina para poder decifrar a criptografia nazista durante a segunda guerra mundial; vez que era, humana e fisicamente, impossível decifrar o código da máquina enigma dos nazistas pelo fato dos aliados terem uma amostra da mensagem nazista codificada às 06h00 e a máquina enigma mudava a sua combinação às 00h00. Desse modo, a segurança do RSA baseia-se na dificuldade de fatoração de números grandes pelo fato de exigir muito trabalho e tempo para “quebrar” o algoritmo. Entretanto, em 1999, após cerca de 7 (sete) meses de trabalho, uma chave RSA de 512 bits (utilizada por 95% dos sites de comércio

eletrônico) foi quebrada pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 (seis) países e 300 (trezentas) estações de trabalho.

O ElGamal é outro algoritmo comutativo de chave pública utilizado tanto para assinatura digital quanto para gerenciamento de chaves, mas com procedimento matemático diferente do RSA e que envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém do logaritmo discreto (dificuldade de se calcular logaritmos discretos em um corpo finito).

Já o Diffie-Hellman, também usa o algoritmo discreto e apesar do conceito de chave pública ter sido inventado em 1976 pelos seus criadores, esse criptosistema não permite ciframento e nem assinatura digital, mas tão somente possibilita duas pessoas entrarem em um acordo ao compartilharem um segredo em público.

O DSA (*Digital Signature Algorithm*), por sua vez, uma variação dos algoritmos de assinatura ElGamal e Schnorr, inventado pela NSA (*National Security Agency* ou Agência de Segurança Nacional - https://www.nsa.gov/) e patenteado pelo governo norteamericano, é destinado exclusivamente às assinaturas digitais. Foi proposto, em agosto de 1991, pelo NIST (*National Institute of Standards and Technology* ou Instituto Nacional de Padrões e Tecnologia - https://www.nist.gov/) para utilização no seu padrão DSS (*Digital Signature Standard* ou Algoritmo de Assinatura Digital) e foi adotado, em dezembro de 1994, como padrão final.

Portanto, a **função *hashing*** (*message digest*, *one-way hash function*, função de condensação ou função de espalhamento unidirecional) é como uma impressão digital de uma mensagem, que a partir de uma entrada de tamanho variável, gera um valor fixo pequeno: o *digest* ou valor *hash*.

Exemplificando, para garantir a integridade dos dados compartilhados, os *softwares* clientes de *torrent* calculam uma sequência ("algorithm" ou algoritmo) de caracteres (letras e/ou números) única ("hash" ou "hashsum") e a atribui aos arquivos ou pastas originais que começarão a ser compartilhados. É como se fosse um número serial de algum aparelho ou

produto, que o identifica e o individualiza; tal como o CPF para as pessoas físicas, o CNPJ para as pessoas jurídicas ou, melhor ainda, como a impressão digital dos humanos. Essa catalogação é semelhante a inserção de chips identificadores e rastreadores em animais; ou seja, serve para garantir a integridade dos dados compartilhados, evitando-se corrompimento, manipulações, adulterações, acréscimos, inserções de *malwares* ou *trojans*, etc. Desse modo, quando algum usuário do *torrent* clica em determinado arquivo para efetuar o *download*, antes que o mesmo efetivamente comece, o programa utilizado para isso (cliente) pede ("checksum") a mesma sequência de letras e números (“hash info” ou "message digest", a identidade do arquivo selecionado) para o computador que está servindo o arquivo em questão (disponibilizando ou efetuando *upload*). Se a numeração estiver diferente ("not match"), significa que o arquivo foi alterado (adulterado ou corrompido) e que não deve ser baixado. Caso esteja correta, a transferência é então iniciada. Por esse mesmo método, pode ser feita a conferência de uma senha ("password" ou “login”). Se a senha informada estiver de acordo com o "hash" da senha cadastrada, ela será confirmada; portanto, o sistema não vê a senha propriamente dita, mas apenas sua indexação. Já um sistema simples armazena as próprias senhas literalmente e a validação é mera comparação de "strings". Neste caso, basta dar uma mera espiada no arquivo da base de dados para saber a senha. **Nos Certificados Digitais a função de "hash" (resumo criptográfico) é chamada de assinatura digital** (http://cartilha.cert.br/criptografia/).

> "Torrent é a extensão de arquivos utilizados por um protocolo de transferência do tipo P2P (*Peer to Peer*). Essa transferência acontece da seguinte maneira: os arquivos transferidos são divididos em partes e cada pessoa que tem tal arquivo ajuda a fazer o upload a outros usuários. Isso reduz significantemente o consumo de banda do distribuidor original do arquivo, não sendo necessário que o mesmo fique armazenado em um servidor. Para compartilhar esses arquivos, é necessário usar um programa específico, conhecido como cliente. Ele obtém as informações contidas nos arquivos e se encarrega de toda a comunicação entre os usuários." (http://www.tecmundo.com.br/torrent/166-o-que-e-torrent-.htm).

> "P2P (do inglês peer-to-peer, que significa par-a-par) é um formato de rede de computadores em que a principal característica é descentralização das funções convencionais de rede, onde o computador de cada usuário conectado acaba por realizar funções de servidor e de cliente ao mesmo tempo." (http://www.tecmundo.com.br/torrent/192-o-que-e-p2p-.htm).

Um algoritmo de dispersão, portanto, é um método utilizado pela criptografia para codificar dados e garantir a segurança e integridade. Desse

modo, somente possuindo essa sequência específica de caracteres é que se tem acesso aos dados ou arquivos relacionados.

Alguns tipos de **algoritmos de hash**:

- "O MD5 (*Message-Digest algorithm* 5) é uma função de dispersão criptográfica (ou função hash criptográfica) de 128 bits unidirecional desenvolvido pela RSA Data Security, Inc., descrito na RFC 1321, e muito utilizado por softwares com protocolo ponto-a-ponto (P2P, ou *Peer-to-Peer*, em inglês) na verificação de integridade de arquivos e logins." (https://pt.wikipedia.org/wiki/MD5).

- SHA-1 (*Secure Hash Algorithm*): de 160 bits foi desenvolvido pelo NIST e NSA e publicados como um padrão do governo Norte-Americano. É considerado o sucessor do MD5.

- "SHA-2 é um conjunto de funções hash criptográficas projetadas pela NSA (Agência de Segurança Nacional dos EUA). [1] SHA significa *secure hash algorithm* (algoritmo de hash seguro)." (https://pt.wikipedia.org/wiki/SHA-2).

- O SHA-512 é a versão melhorada do SHA-265, que por sua vez é uma versão muito melhor do SHA-1.

- O Whirlpool é um pouco mais lento que o SHA-512 e, consequentemente, mais “entrópico”, ou seja: mais seguro.

O termo **função de *hash*** é também utilizado para mapear elementos em uma estrutura de dados chamada "hash table". Uma **tabela de "hashing"** ("hashtable" ou tabela de dispersão) é uma estrutura de dados que faz associação de valores a chaves. Em ciência da computação, uma tabela de dispersão (ou de espalhamento) é uma estrutura de dados especial, que associa chaves de pesquisa a valores. Seu objetivo é, a partir de uma chave simples, fazer uma busca rápida e obter o valor desejado. É algumas vezes traduzida como tabela de escrutínio. "Hash function" é função de espalhamento. Uma tabela de dispersão (*hash table*) é uma maneira muito

popular de organizar uma tabela de símbolos. A função de *hashing* responde à pergunta: Em que posição da tabela de *hash* devo colocar esta chave? A função de *hashing* espalha as chaves pela tabela de *hash*. A função de *hashing* produz uma colisão quando duas chaves diferentes têm o mesmo valor *hash* e, portanto, são levadas na mesma posição da tabela de *hash*.

O sinal # é comumente chamado de "símbolo de hash".

Não confundir com **"hashtag"**; que é popularmente usado no Brasil para descrever palavra ou frase precedida pelo símbolo # e que resume o tema principal de uma postagem nas redes sociais, em especial no Twitter. A "hashtag", assim, é usada com frequência para fazermos busca sobre determinado assunto.

As populares *hashtags*, originalmente *Trending Topics* do Twitter (http://trends24.in/brazil/), são utilizadas pelos usuários das redes sociais (Twitter, Instagram, FaceBook, Google +, Pinterest, YouTube, etc.) para indexar postagens (como se fosse um bibliotecário catalogando o acervo), agrupando conteúdo do mesmo tema, para servir de posterior ferramenta de busca ao se transformar em um hiperlink. Dessa forma, ao adicionar o símbolo # antes do verbete indexador ou palavra-chave no padrão CamelCase; ou seja, tudo junto e sem espaços, como, por exemplo, #Bitconiscool!, os demais usuários encontram facilmente publicações sobre o mesmo assunto.

O símbolo #, no inglês britânico, é "hash" e como uma das traduções possíveis para o substantivo "tag" (do inglês americano) é “etiqueta”; logo "hashtag" seria uma espécie de etiqueta que serve para rotular uma publicação na rede social para mais fácil identificação. Entretanto, o termo correto para isso é "number sign" ou "pound sign".

O nome do símbolo # é *octothorpe* (cerquilha, antífen, cardinal, jogo da velha, porteirinha, cauabanga, caprino, tralha, malha, grade, quadrado, jogo-do-galo, mosca, jogo-do-gato, *gato*, lasanha, moiteiro, cruzadinha, chiqueirinho, cerquinha, Sharp, cadeia, número de chave, símbolo de número, *number sign*, *pound sign*, *almohadilla*, "hash" e, equivocadamente de sustenido). Foi criado na década de 1960 por Don Macpherson, um

supervisor da Bell Labs, para acesso a serviços de dados. A necessidade deste símbolo surgiu quando foi inventado o sistema DTMF (sigla em inglês para “tom duplo de multifrequência”). Quando o botão # entra em ação, a conversa é entre telefone e computador; por isso que até hoje, essa tecla nos telefones só funciona no sistema de tom e não no de pulsos. A junção da palavra *Octo* (referente aos oito espaços em branco que cercam o quadrado central da figura, ou ainda, às extremidades das retas que se cruzam) com o nome de Jim Thorpe (campeão de decatlo de 1912) resultaram no nome oficial (*Octothorpe*).

A expressão "pound sign" ou "sinal de libra", na Grã-Bretanha representa a moeda libra esterlina (£), mas nos Estados Unidos se trata do # ou referência à unidade de peso. Antes da introdução do IBM PC (primeiros computadores domésticos ou de uso pessoal), não havia nenhum padrão único aceito para o sinal £ na indústria de computadores no Reino Unido. Desse modo, utilizava-se o #.

O sustenido (♯) possui o símbolo ligeiramente diferente do octothorpe (#) e não são a mesma coisa. O sustenido é um termo de partitura (música) e se trata de um acidente que, tendo seu sinal de notação (♯) colocado à esquerda da nota (musical), indica que a altura desta nota deve ser elevada em um semitom. A palavra é usada como adjetivo para indicar entonação acima da altura constante da notação.

Para entender melhor, ou se profundar, sobre o que são as bitcoins e como elas são feitas, confira os capítulos: "CERTIFICADOS DIGITAIS", "*PEER-TO-PEER* (P2P)", "BITCOIN", "COMO A BITCOIN É FEITA?", "*BLOCKCHAIN*" e "COMO MINERAR BITCOINS E ALTCOINS".

ALGORITMO DE *HASH*

O algoritmo de *hash* (*hashing algorithm*) ou algoritmo de criptografia (*encryption algorithm*) mais popular no meio das criptomoedas (*crypto-coins*) é o SHA-256, que originalmente estreou como algoritmo de *hash* do Bitcoin. Com a introdução do Litecoin, o algoritmo Scrypt entrou em cena. Desde então, muitos outros algoritmos tomaram cena no palco das criptomoedas: Scrypt, Scrypt-N, Scrypt-N-R, Scrypt-ChaCha, X11, X12, X13, X14, X15, X17, Keccak, Quark, Groestl, e-256, NeoScrypt, Lyra2REv2, CryptoNight, EtHash, Equihash, Groestl, Keccak, NIST5, C11 Algorithm, Cuckoo Cycle, Jackpot, Momentum, Ocean, Prime Constellations, Primechain, Wild Keccack, etc. (https://minkiz.co/coin/algo).

- https://getpimp.org/what-are-all-these-x11-x13-x15-algorithms-made-of/.

Os três mais conhecidos são o SHA-256 (utilizado no Bitcoin, Namecoin, Devcoin, etc.) o Scrypt (usado no Litecoin, Dogecoin, Worldcoin, Fastcoin, etc.) e o X11 (aplicado no Darkcoin, Anonymouscoin, etc.).

O SHA-256 e o Scrypt são os dois sistemas de algoritmos de *hash* mais comumente utilizados pelos mineiros (*miners*) das criptomoedas (*crypto-currency*) para autenticação dos blocos de dados de transação.

Um **bloco** (*block*) da rede (ou protocolo) Bitcoin é onde ficam registradas as transações bitcoins. Quando alguém efetua uma transação Bitcoin (*Bitcoin transaction*), ela é rapidamente propagada por toda a rede (P2P) Bitcoin e fica à espera de ser incluída em um bloco por um minerador, junto com as demais transações pendentes (*pending transactions*). Por outras palavras, todas as transações Bitcoins ocorridas num certo período de tempo são aglomeradas para serem verificadas e validadas conjuntamente num mesmo bloco. Portanto, o bloco é um conjunto de informações que legitima e valida as transações por toda a rede Bitcoin. Pode-se fazer uma analogia do bloco como uma página do livro razão de contabilidade (*accounting ledger book*). Por outras palavras, o bloco é um arquivo em que os dados relativos à rede Bitcoin são permanentemente gravados na *Blockchain* (cadeia de blocos, livro razão ou contabilidade pública descentralizada). Quando a transação é incluída em um bloco válido (*valid block*), a transação passa a ser

considerada confirmada (*confirmed*) e fica registrada eternamente na *Blockchain*. Na prática, um bloco consiste num pequeno cabeçalho (*header*) contendo (dentre outras coisas) o *hash* (o resultado dos cálculos de *nonce* que é aceito pela rede Bitcoin) do bloco anterior (esse é o enigma a ser descoberto para validar o bloco) e a *Merkle root* (raíz de Merkle) das transações, que permite recuperá-las. O *hash* consiste num número que é gerado a partir de uma fórmula preestabelecida e representa uma informação. Cada *hash* é utilizado para produzir o *hash* do bloco seguinte (cada bloco bitcoin faz referência ao bloco anterior) e o processo continua em cadeia (sequência). Em termos didáticos, é preciso conseguir acertar o encaixe (combinação) do novo bloco com o bloco imediatamente anterior, tal como, de forma similar, num jogo de dominó. A cada bloco corretamente calculado, alguns novos Bitcoins são gerados, e são inicialmente atribuídos ao minerador do bloco. Com outras palavras, a cada *hash* resolvido é liberado um novo bloco, que se torna novas unidades da moeda digital além de registrar as transações realizadas.

Como o parágrafo supra evidencia, a palavra "bloco" é a mais utilizada neste e-book; vez que é a base de todo o sistema Bitcoin tal como as peças de montar do brinquedo Lego. Saiba mais sobre os blocos, principalmente, nos capítulos: "COMO A BITCOIN É FEITA?", "*FORK*", "*BLOCKCHAIN*", "COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?", "O QUE É MINERAÇÃO DE BITCOIN?" e "COMO MINERAR BITCOINS E ALTCOINS".

O **Scrypt** é uma função de derivação de chaves (KDF - *Key Derivation Function*), que usa senhas para proteger os dados, com a segurança baseada principalmente em torno de exigir grandes quantidades de memória para concluir as operações. Para um usuário legítimo, a operação é rápida e completa em pouco menos de um segundo. Já se um usuário está tentando violar ou invadir o sistema através do método de força bruta, a operação teria de ser concluída bilhões de vezes, o que torna quase impossível de obter êxito em uma quantidade razoável de tempo. Isso decorre do recurso *time-memory trade off* (troca de tempo de memória), que força o *hacker* a ter que usar muito mais memória para tentar concluir a operação mais rápido, ou usar menos memória e completar a operação muito mais lentamente. O Scrypt é utilizado na verificação de *PoW - Proof of Work*

(prova de obra ou de trabalho) em troca de criptomoeda, como a Litecoin. Ironicamente, o Scrypt foi implementado como uma solução para a mineração bitcoin via GPU o que foi visto como demasiado pelos desenvolvedores Litecoins, com o que implementaram uma correção para evitar do Litecoin (https://litecoin.org/pt/) ser extraído usando GPU.

Algumas altcoins que usam o **algoritmo (*algorithm*) Scrypt**:

- 10-5 - TenFive Coin (https://bitcointalk.org/index.php?topic=500971.0);
- AIR - AIRcoin (https://bitcointalk.org/index.php?topic=476383.0);
- ANC – Anoncoin (https://anoncoin.net/);
- BTCs/BTC2 – Bitcoin Scrypt (http://bitcoinscrypt.co/);
- BTM – Bitmark (https://github.com/project-bitmark/bitmark);
- CATc - Cataloniacoin (https://bitcointalk.org/index.php?topic=518418.0);
- CGB – Cryptogenic Bullion (https://github.com/MercStills/CryptogenicBullion);
- DGC – DigitalCoin (http://digitalcoin.org/);
- ELC – Elacoin (https://github.com/elacoin/elacoin);
- FTC – FeatherCoin (https://www.feathercoin.com/);
- GIARCOC - Giarcoin (https://bitcointalk.org/index.php?topic=545529.0);
- GLD – GoldCoin (http://www.gldcoin.com/);
- GNS - Genesiscoin (https://bitcointalk.org/index.php?topic=518258.0);
- H2O - H2O Coin (https://bitcointalk.org/index.php?topic=494229.0);
- IFC – Infinitecoin (http://infinitecoin.org/);
- KRN – Ekrona (https://github.com/ekrona/ekrona);
- LAT – Latium (https://github.com/LatiumCoin/Latium);
- LTC – Litecoin (https://litecoin.org/);
- MΣC – Megacoin (http://www.megacoin.eu/);
- MID – MidasCoin (https://github.com/MidasPaymentLTD/midascoin);

- MMC – Memorycoin 2.0 (https://github.com/memorycoin/memorycoin);
- NVC – Novacoin (https://novaco.in/);
- ONC - Onecoin (https://github.com/onecoin/onecoin);
- PND/PAND – PandaCoins (https://github.com/pandacoin-official/pandacoin);
- RT2 - Rotocoin (https://bitcointalk.org/index.php?topic=516138.0);
- TAG – Tagcoin (http://tagcoin.org/);
- WDC – WorldCoin (https://worldcoin.global/);
- YAC - YaCoin (https://www.yacoin.org/);
- XSV - SiliconValleyCoin (https://bitcointalk.org/index.php?topic=520249.0).

O SHA-256 é mais complexo que o Scrypt e é usado pelo Bitcoin e a maioria das moedas com base em seu código. O processamento de blocos de dados com SHA-256 tende a ser mais demorado que pelo Scrypt, mas é mais completo e deixa menos margem para erros. A mineração bem-sucedida de moedas usa SHA-256, o qual requer, muitas vezes, taxas de *hash* na potência de gigahashes por segundo (GH/s) ou superior; o que dificulta o trabalho de mineiros individuais. O Scrypt é mais rápido e mais simples do que o SHA-256. Entretanto, as novas moedas digitais que surgiram preferiram o SHA-256. Alguns argumentam que esse sistema mais simples é mais suscetível a problemas de segurança, vez que os tempos de rotação rápida pode significar que o sistema não está olhando direito ou vendo completamente os dados. Seus defensores, no entanto, afirmam que isso não passa de teoria, pois ainda não se soube de nenhum caso concreto.

O Scrypt, também, é muito mais fácil de executar em uma CPU já existente (computador doméstico) e tende a usar menos energia do que usando SHA-256; desse modo, é preferido pela maioria dos mineiros individuais. Em comparação com SHA-256, as taxas de hash do Scrypt para a mineração variam em kilohashes por segundo (KH/S) ou megahashes por segundo (MH/s) nas áreas de dificuldade; potência esta que pode ser alcançada com computadores regulares, sem a necessidade de ASICs ou outro *hardware* especial. Ao longo do tempo, presume-se que irá ser elevada a dificuldade de *hash* para as moedas mais populares que usam o SHA-256,

com o que ocorrerá uma restrição ainda maior na mineração dessas moedas; ou seja, exigirá hardwares muito mais potentes dos que já existem. Como resultado, espera-se que as moedas digitais que utilizam Scrypt tenham um aumento substancial em popularidade, com base na facilidade de mineração solo (sozinho). Mas tal condição não se manterá por muito tempo, pois está iniciando-se uma corrida armamentista em Litecoin e demais criptomoedas Scrypt, em razão de empresas como a Alpha Technologies (https://alpha-t.net/) estarem na iminência de fornecerem mineradoras ASIC para o algoritmo Scrypt. **ASICs** são peças (*hardwares*) personalizadas de computador que são projetadas exclusivamente para executar uma função específica. Uma desvantagem da *PoW - Proof of Work* (prova de obra ou de trabalho) é que ela é demorada e requer muito poder de computação e, portanto, desperdiça muita energia elétrica. Desse modo, o Scrypt possui rendimento muito maior ainda em outro tipo de método ou mecanismo de consenso.

O **algoritmo (*algorithm*) SHA-256** é utilizado pelas seguintes criptomoedas:

- 21 - 21Coin (https://bitcointalk.org/index.php?topic=426853.0);
- ACOIN - Acoin (https://cryptocointalk.com/topic/14814-acoin-acoin-information/);
- AMK - AmKoin (http://www.amkon.net/ e https://github.com/bryceweiner/amkoin);
- ARK - Arkhash (https://github.com/Arkhash/arkhash);
- ARS - Arkenstone (https://bitcointalk.org/index.php?topic=608482.0);
- ASC - AsicCoin (https://bitcointalk.org/index.php?topic=292501.0);
- BCX - Battlecoin (https://bitcointalk.org/index.php?topic=354612.0);
- BEN - Benjamins (https://bitcointalk.org/index.php?topic=444543.0);
- BET - Betacoin (https://bitcointalk.org/index.php?topic=321266.0);
- BLC – Blakecoin (https://blakecoin.org/);

- BNS - Bonuscoin (https://bitcointalk.org/index.php?topic=524212.0);
- BTC - Bitcoin (https://bitcoin.org/pt_BR/);
- BTE - Bytecoin (https://github.com/ahmedbodi/bytecoin/);
- BTN - Bitinium (https://github.com/Bitinum/Bitinum);
- BTP - BitPeso (https://cryptocointalk.com/topic/7398-bitpeso-btp-information-added-to-1st-exchange/);
- CC - ColbertCoin (https://bitcointalk.org/index.php?topic=567491.0);
- CREA - Cryptoeagle (https://github.com/cryptoeagle/cryptoeagle);
- CTM - Continuumcoin (https://cryptocointalk.com/topic/3795-continuumcoin-ctm-information/);
- CURE - Curecoin (https://www.curecoin.net/);
- DEM - Deutsche eMark (http://www.deutsche-emark.org/ e https://bitcointalk.org/index.php?topic=310939.0);
- DGC - Digitalcoin (http://digitalcoin.org/);
- DIEM - CarpeDiem (https://bitcointalk.org/index.php?topic=513599.0);
- DVC - Devcoin (https://bitcointalk.org/index.php?topic=34586.0);
- FER - Ferengicoin (https://bitcointalk.org/index.php?topic=484841.0);
- FFC - FireFlyCoin (https://github.com/FireFlyCoin/FireFlyCoin);
- FRC - Freicoin (http://freico.in/ e http://www.freicoin.org/);
- FSS - FastoinSHA (https://github.com/raziel420/fastcoinsha);
- GLB - Globe (https://bitcointalk.org/index.php?topic=360255.0);
- HAM - HAMRadioCoin (https://bitcointalk.org/index.php?topic=675564.0);
- HKC - HongKongCoin (https://bitcointalk.org/index.php?topic=518669.0);
- I0C – I0coin (https://izerocoin.org/);
- IMP - ImperialCoin (https://github.com/ImperialCoin/ImperialCoin);
- IXC - iXcoin (https://bitcointalk.org/index.php?topic=36218.0);

- LOOT - CryptoLOOT (https://github.com/CryptoLOOT/loot-master);
- MYR - Myriadcoin (http://myriadcoin.org/pt/home);
- MZC - Mazacoin (http://www.mazacoin.org/ e https://github.com/MazaCoin/MazaCoin);
- NEOS - NeosCoin (http://www.neoscoin.com/);
- NMC - Namecoin (http://namecoin.info/);
- ORO - Orobit (https://github.com/orobit/orobit);
- OSC - Ocoin (https://github.com/OCoin/OSC);
- P$ - Petrodólares (https://bitcointalk.org/index.php?topic=472238.0);
- PI (https://github.com/picoinnewdev/pi);
- PMC - PremineCoin (https://bitcointalk.org/index.php?topic=427519.0);
- PPC - Peercoin (https://www.peercoin.net/);
- PT - Platinum (https://bitcointalk.org/index.php?topic=452121.0);
- PWNY - Pwnycoin (https://github.com/pwnycoin/pwnycoin);
- RKC – Reikicoin (http://altcoins.com/rkc-reikicoin.html);
- SCOT - Scotcoin (http://scotcoinproject.com/ e https://github.com/scotcoin/scotcoin);
- SHA - SHACoin (https://bitcointalk.org/index.php?topic=512808.0);
- SNC - Snowcoin (https://bitcointalk.org/index.php?topic=359948.0);
- SPC - SpeedCoin (http://speedcoin.net/);
- STL - STLcoin (https://github.com/stlcoin/stlcoin);
- TAK - Takcoin (https://bitcointalk.org/index.php?topic=452902.0);
- TEA - Teacoin (https://github.com/teacoind/teacoin);
- TEK - Tekcoin (http://tekcoin.org/ e https://bitcointalk.org/index.php?topic=289490.0);
- TGC - Tigercoin (https://tigercoin.wordpress.com/);
- TIT - Titcoin (http://www.titcoins.biz/ e http://www.prurient.com/);
- TRC - Terracoin (http://terracoin.sourceforge.net/);
- UNB - UnbreakableCoin (http://www.unbreakablecoin.com/);

- UNIC - Unicoin (https://bitcointalk.org/index.php?topic=392204.0);
- UNIT - UniversalCurrency (https://www.u-currency.com/);
- UNO - Unobtanium (http://unobtanium.uno/);
- V - Version (https://github.com/staycrypto/version);
- WAS - WeAreSatoshi (https://bitcointalk.org/index.php?topic=506912.0);
- XJO Joulecoin (https://bitcointalk.org/index.php?topic=299308.0);
- XXC - CREDS (https://cryptocointalk.com/topic/8084-creds-xxc-information/);
- ZET - Zetacoin (http://www.zetac.org/ e https://github.com/zetacoin/zetacoin);
- ZS - Zimstake (https://bitcointalk.org/index.php?topic=583591.0);
- Etc.

O melhor equipamento para mineração em SHA-256 são os processadores ASIC's.

Keccak (http://keccak.noekeon.org/) é um padrão de **SHA-3** - *Secure Hash Algorithm version 3* (https://asecuritysite.com/encryption/sha3). É utilizado pelas seguintes moedas:

- 365 - 365Coin (https://bitcointalk.org/index.php?topic=492311.0);
- CLR - Copperlark, CTD - Catedoge (https://bitcointalk.org/index.php?topic=528453.0);
- GLN - Galleon (https://bitcointalk.org/index.php?topic=519538.0);
- HXC - Helixcoin (https://bitcointalk.org/index.php?topic=489172.0);
- MAX - MaxCoin (https://bitcointalk.org/index.php?topic=438150.0);
- METH - CryptoMETH (https://bitcointalk.org/index.php?topic=500175.0);

- SLOTH - Slothcoin (https://bitcointalk.org/index.php?topic=512903.0);
- WEC - Wecoin (https://bitcointalk.org/index.php?topic=502337.0);
- Etc.

O **X11** também é um algoritmo de verificação de *PoW - Proof of Work* (prova de obra ou de trabalho), mas atrelado a 11 (onze) algoritmos diferentes e encadeados sobre os *hashes* para garantir as criptomoedas e suas transações. São eles: blake, bmw, groestl, jh, keccak, meada, luffa, cubehash, shavite, SIMD e eco. O X11 tem a vantagem de um sistema multimistura, o que significa que, para que o algoritmo falhe, todos os onze dos seus *hashes* teriam de falhar ao mesmo tempo. Levando-se em conta a probabilidade muito baixa de um único *hash* ser quebrado, a chance de falha do sistema X11 é praticamente zero. Se o SHA-256 e o Scrypt fracassarem, qualquer criptomoeda pode migrar para o X11 como um apoio mais seguro. No momento, Dashcoin é a moeda mais popular que usa o X11. O X11 é de longe o mais popular da série "X" de algoritmos de *hash* (X11, X12, X13, X14, X15 e x17). O X11 é uma ótima escolha para os mineiros que usam GPU (*Graphical Processing Unity*), pois o desempenho do X11 é melhor na GPU. As moedas que usam X11 são Dash (https://www.dash.org/), Startcoin (https://startcoin.org/), XCurrency (http://xcurrency.com/), Digitalcoin (http://digitalcoin.org/), Urocoin (https://chainz.cryptoid.info/uro/), Karmacoin (http://www.givekarma.net/), etc.

Algumas altcoins que suportam **X11**:

- ADZ - Adzcoin (http://www.adzcoin.com/);
- XBTS - Beatcoin (https://bitcointalk.org/index.php?topic=1625301.220);
- Bitz (https://bitcointalk.org/index.php?topic=954125.0);
- Dash (https://www.dash.org/);
- CANN - CannabisCoin (http://cannabiscoin.net/);
- CPC - Capricoin (http://capricoin.org/);
- CRBIT - Creditbit (https://bitcointalk.org/index.php?topic=1237511.0);

- ConspiracyCoin (https://github.com/C-Y-Coin/cyc-master/releases);
- CREVA - Crevacoin (https://bitcointalk.org/index.php?topic=1066542.0);
- CRYPT - CryptCoin (https://bitcointalk.org/index.php?topic=618377.0);
- Europecoin (http://www.europecoin.eu.org/);
- FC2 - FuelCoin (https://bitcointalk.org/index.php?topic=589879.0);
- GRN - GraniteCoin (http://www.granitecoin.com/);
- GiveCoin (http://2givecoin.info/);
- GB - GoldBlocks (http://goldblocks.eu/);
- HashCoin (https://www.hashcoin.io/);
- HTC - Hitcoin (http://hitcoininfo.com/);
- INFX - Influxcoin (https://influxcoin.xyz/);
- LXC - Librexcoin (https://bitcointalk.org/index.php?topic=703042.0);
- Logicoin (https://github.com/Logicoin/logicoin);
- MTR - MasterTraderCoin (http://www.mastertradercoin.com/);
- MOJO - Mojocoin (https://mojocoin.org/);
- Muniti (https://github.com/muniti/muniti);
- Nyancoin (https://github.com/nyancoin-release/nyancoin);
- PC - Pinkcoin (https://bitcointalk.org/index.php?topic=591666.0);
- PIGGY - Piggycoin (https://www.piggy-coin.com/);
- PUTIN - PutinCoin (https://bitcointalk.org/index.php?topic=1526495.0);
- SCRT - Secretcoin (https://bitcointalk.org/index.php?topic=1161754.0);
- SUPER - SuperCoin (http://www.supercoin.the-node.net/);
- SmartCoin (http://smartcoin.cc/);
- SPR - SpreadCoin (http://www.spreadcoin.info/);
- StartCoin (https://startcoin.org/);
- TRUMP - Trumpcoin (http://www.trumpcoin.com/);
- TRUST - TrustPlus (http://trustplus.com/);

- U - Ucoin (https://ucoin.co/);
- UNC - Unioncoin (https://bitcointalk.org/index.php?topic=365399.0);
- Uro - (https://bitcointalk.org/index.php?topic=600639.0);
- WMC - WMCoin (https://bitcointalk.org/index.php?topic=1432330.0);
- XCurrency (https://github.com/atcsecure/XCurrency)
- Etc.

No site http://com-http.us/ é possível conferir várias outras moedas que utilizam o X11.

Inicialmente lançado como Xcoin, então conhecido como DarkCoin, Dash (https://www.dash.org/) é uma criptomoeda que visa trazer a privacidade de volta para as transações. Dash mudou seu nome para se desvincular da DarkWeb. Dash usa X11. Quando consultamos eram 367 moedas usando X11 segundo o site http://com-http.us/.

Através dos sites http://www.coinwarz.com/cryptocurrency e https://whattomine.com/ é possível fazer uma simulação de mineração através de diferentes algoritmos de hash.

A moeda Prime (https://bitcointalk.org/index.php?topic=1149892.0, http://www.primechain.in/ e https://github.com/DigiCubeCrypto/PrimeChain) estabeleceu uma prova-de-obra baseada na procura de números primos. Três tipos de cadeias principais, conhecidos como Cunningham cadeia de primeiro tipo, Cunningham cadeia de segundo tipo e uma corrente bi-twin são qualificados como prova-de-obra. Também utilizam a **Primechain** (cadeias de número primo): DTC - Datacoin (http://datacoin.info/ e https://github.com/foo1inge/datacoin), RIC - Riecoin (http://riecoin.org/) e XPM - Primecoin (https://github.com/primecoin/primecoin).

O algoritmo de *hash* do **Quark** (http://www.quarkcoins.com/) realiza 9 (nove) rodadas de *hash* a partir de 6 (seis) funções de *hashing* únicos (blake, groestl, blue midnight wish, jh, SHA-3 e skein).

Além da própria Quark, também usa esse algoritmo de *hash*, as moedas:

- MonetaryUnit: https://bitcointalk.org/index.php?topic=778322.0;
- AmsterdamCoin: http://amsterdamcoin.com/;
- Dimecoin: https://bitcointalk.org/index.php?topic=382164.0;
- Molecule: https://bitcointalk.org/index.php?topic=377252.0;
- Atom: https://bitcointalk.org/index.php?topic=380546.0;
- SecondsCoin: https://bitcointalk.org/index.php?topic=381587.0;
- Union Coin: https://bitcointalk.org/index.php?topic=365399.0;
- SecureCoin: https://bitcointalk.org/index.php?topic=270852.0 e http://securecoin.org/;
- Frozen: https://bitcointalk.org/index.php?topic=366762.0;
- RVDCoin: https://bitcointalk.org/index.php?topic=357196.0;
- Cthulhu: https://bitcointalk.org/index.php?topic=294383.0;
- Particle: https://bitcointalk.org/index.php?topic=392804.0;
- ZurCoin: https://bitcointalk.org/index.php?topic=391806.0;
- Darkcoin: https://bitcointalk.org/index.php?topic=384582.0;
- C-Notes: https://bitcointalk.org/index.php?topic=397916.0;
- Photon: https://bitcointalk.org/index.php?topic=404623.0;
- Bull Coin: https://bitcointalk.org/index.php?topic=409903.0;
- FairQuark: https://bitcointalk.org/index.php?topic=417700.0;
- MiniCoin: https://bitcointalk.org/index.php?topic=429105.0;

- PlatinumCoin: https://bitcointalk.org/index.php?topic=434184.0;
- RandomQuark: https://bitcointalk.org/index.php?topic=500123.0;
- BitQuark: https://bitcointalk.org/index.php?topic=468018.0;
- QuarkBar: https://bitcointalk.org/index.php?topic=488455.0;
- Probe: https://bitcointalk.org/index.php?topic=508908.0;
- AnimeCoin: https://bitcointalk.org/index.php?topic=423339.0;
- Etc.

No algoritmo da moeda SKN - Skeincoin (https://bitcointalk.org/index.php?topic=322828.0), a primeira rodada de *hashing* é feito usando **Skein** e, a segunda, usando SHA256 (Skein-SHA2). A moeda XDC - Xedoscoin (http://xedoscoin.com/), também usa o algoritmo Skein.

Salvo engano, o algoritmo **Scrypt-Jane** é uma biblioteca (gcc, icc, clang, MIX, SALSA/SALSA64, SHA256/512, BLAKE256/512, Skein512 e Keccak256/512) da Floodyberry (https://libraries.io/github/floodyberry), baseada na atualização do Bitcoin Core versão 0.9.1 (https://bitcoin.org/en/release/v0.9.1). Scrypt-Jane contém muitos misturadores e hashers incluindo aqueles (CHACHA, SHA256, SHA512, BLAKE256, BLAKE512, SKEIN512, KECCAK256 e KECCAK512) usados pela Yacoin (https://www.yacoin.org/); daí uma confusão de Scrypt-Jane com o Scrypt-Chacha da Yacoin. Melhor seria chamar de Scrypt-YAC. As seguintes moedas utilizam o Scrypt-Jane:

- BDC - BlackDragonCoin (https://bitcointalk.org/index.php?topic=597006.0);
- BTL - Bitleu (http://www.bitleu.org/);
- GRP - Graphene (https://bitcointalk.org/index.php?topic=527890.0);
- MRC - microCoin (http://microcoin.alcurex.info/).

Já o algoritmo de *hash* (*hashing algorithm*) Scrypt-Chacha, além da Yacoin, é utilizado pela UTC - Ultracoin (http://ultracoin.net/).

Os **algoritmos de *hash* indicados para mineração GPU** (*Graphical Processing Unity*) são Ethash, Groestl, Chacha (Nf14), CryptoNight, Equihash, Lyra2Rev2, NeoScrypt, LBRY, Blake (2b), Blake (14r) e Blake (XVC). Já para ASIC são: SHA-256, Scrypt, X11, Quark e Qubit.

Pelos sites https://www.coingecko.com/ e http://www.coinwarz.com/cryptocurrency, é possível pesquisar qual é o algoritmo de *hash* utilizado pela criptomoeda.

Saiba mais no capítulo “LISTA DE ALTCOINS: CONSENSO E *HASH*”.

CERTIFICADOS DIGITAIS

O padrão PKI (*Public Key Infrastructure* ou infraestrutura de chave pública) é que regula o gerenciamento de chaves públicas. Ele define o local de armazenamento dos certificados digitais, a forma como são armazenados, a revogação de certificados, etc.

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais.

O **ITI - Instituto Nacional de Tecnologia da Informação** (http://www.iti.gov.br/) é uma autarquia federal que tem por missão manter e executar as políticas da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Ao ITI compete ainda ser a primeira autoridade da cadeia de certificação digital (AC Raiz) e é o responsável pela execução de políticas da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Na qualidade de Autoridade Certificadora Raiz (AC-Raiz), controla outras políticas e regulamentações relacionadas à tecnologia no Brasil. São atribuições da instituição:

- Executar as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

- Garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais ICP-Brasil, bem como a realização de transações eletrônicas seguras;

- Atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança;

- Estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital, como a popularização da certificação digital e a inclusão digital, atuando sobre questões como sistemas criptográficos, software livre,

hardwares compatíveis com padrões abertos e universais, convergência digital de mídias, entre outras.

Em resumo, o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Já o **Comitê Gestor da ICP-Brasil** (http://www.iti.gov.br/index.php/icp-brasil/comite-gestor), é um órgão vinculado à Casa Civil da Presidência da República. É a autoridade gestora das políticas relacionadas ao tema Tecnologia da Informação. Suas competências são:

• Adotar as medidas necessárias e coordenar o funcionamento da ICP-Brasil;

• Estabelecer a política, os critérios e as normas técnicas para o credenciamento das ACs, das ARs e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

• Estabelecer a política de certificação e as regras operacionais da AC-Raiz;

• Homologar, auditar e fiscalizar a AC-Raiz e os seus prestadores de serviço;

• Estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das ACs (Autoridades Certificadoras) e das ARs e definir níveis da cadeia de certificação;

• Aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das ACs e das ARs, bem como autorizar a AC-Raiz a emitir o correspondente certificado;

• Identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, regras de interoperabilidade e outras

formas de cooperação internacional; certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

• Delegar atribuições à AC-Raiz, primeira autoridade da cadeia de certificação.

A **AC-Raiz** é o ponto máximo de confiança da infraestrutura. Ela é responsável pela emissão dos certificados de todas as ACs (Autoridades Certificadoras) a ela diretamente subordinadas, as chamadas ACs Intermediárias de primeiro nível ou normativas. Uma AC pode emitir certificados para pessoas, empresas, equipamentos ou outras ACs, criando assim uma verdadeira infraestrutura de confiança. Desse modo, as ACs de primeiro nível emitem certificados para ACs de segundo nível ou ACs Finais.

- http://www.iti.gov.br/index.php/icp-brasil/como-funciona;
- http://www.iti.gov.br/index.php/icp-brasil/estrutura;
- http://www.iti.gov.br/images/icp-brasil/estrutura/2016/09_setembro/atualizacao_35/estrutura_detalhada.pdf;
- http://www.iti.gov.br/images/icp-brasil/estrutura/2016/09_setembro/atualizacao_35/estrutura_completa.pdf.

Exemplificando, a AC-JUS, como a AC-RAIZ e a AC-SRF, não emite certificados para usuários finais. Apenas credencia ACs (Autoridades Certificadoras), chamadas subsequentes, para que, seguindo as regras específicas da AC-JUS faça a emissão dos certificados aos usuários finais.

Os certificados emitidos na cadeia de certificação da AC-JUS recebem a marca Cert-JUS. Os certificados Cert-JUS são de uso exclusivo de servidores públicos, e ao utilizá-los o titular estará se identificando como servidor de determinada instituição pública. O Cert-JUS Institucional é de uso exclusivo de servidores do poder judiciário, O Cert-JUS Poder Público

é para utilização dos servidores de órgãos externos ao poder judiciário. O Cert-JUS Equipamento Servidor destina-se a aplicações e equipamentos servidores de órgãos públicos, e o Cert-JUS Código Seguro destina-se a assinatura de código fonte de programas.

- http://www.iti.gov.br/images/noticias/indice-noticias/2016/08_agosto/Curso_de_Direito_da_Certificação_Digital.pdf.

Em resumo, **Autoridade Certificadora** (ou de certificação) é a entidade responsável pela emissão dos certificados digitais. Quem deseja ou precisa de um certificado digital, só pode adquiri-lo através de uma Autoridade Certificadora. Já Autoridade de Registro (AR) é entidade responsável pela identificação (validação) presencial do solicitante de um Certificado Digital. Explica-se. Para fins auxiliar no processo de validação da identidade física dos titulares, antes de emitir um certificado digital, as ACs delegam o trabalho de verificar a documentação física de pessoas e organizações às Autoridades de Registro.

O **certificado digital** é um documento eletrônico assinado digitalmente por uma terceira parte confiável, que associa uma entidade (pessoa, processo, servidor, etc.) à uma chave pública. Um certificado digital contém os dados de seu titular, tais como nome, e-mail, CPF, chave pública, nome e assinatura da Autoridade Certificadora que o emitiu. Na prática, o certificado digital funciona como uma carteira de identidade virtual que permite a identificação segura de uma mensagem ou transação em rede de computadores. O processo de certificação digital utiliza procedimentos lógicos e matemáticos para assegurar confidencialidade, integridade das informações e confirmação de autoria.

Em síntese. O Certificado Digital é um documento eletrônico, intransferível e único, que serve como uma carteira de identidade para transações feitas através da Internet. Contém informações que identificam uma empresa, pessoa física, servidor ou site na Web, provendo autenticidade, garantia jurídica e a confidencialidade aos documentos e dados das transações.

- http://www.infowester.com/assincertdigital.php;

- https://serasa.certificadodigital.com.br/o-que-e/;
- http://www.bbseguranca.com.br/solucao-de-seguranca/4-Certificado-Digital;
- https://www.acbr.com.br/;
- https://www.acdigital.com.br/;
- http://www.certisign.com.br/;
- http://www.serpro.gov.br/linhas-negocio/certificacao-digital;
- http://www.caixa.gov.br/empresa/identidade-digital/Paginas/default.aspx;
- http://www.esocial.gov.br/CertificadoDigital.aspx;
- https://www.digitalsigncertificadora.com.br/pt/certificados-digitais;
- http://www.certificadoboavista.com.br/.

O certificado digital é composto por um par de chaves (pública e privativa), que são criptografadas, a fim de manter segurança e possui caráter inviolável das informações. Além disso, são geradas por Autoridades Certificadoras, que são responsáveis por emitir, suspender, renovar ou revogar os certificados.

> "Na prática, o certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora." (http://www.iti.gov.br/index.php/certificacao-digital/o-que-e).

Um certificado digital é, assim, um documento eletrônico assinado por agente confiável, cujo propósito é transferir confiança na autenticidade por ele verificada de um dado ali contido. Normalmente é armazenado num cartão com chip ou num *token* (formato semelhante a um pen drive). Portanto, o Certificado Digital é uma assinatura com validade jurídica que

garante proteção às transações eletrônicas e outros serviços via Internet, permitindo que pessoas e empresas se identifiquem e assinem digitalmente de qualquer lugar do mundo com mais segurança e agilidade.

Os certificados digitais contêm os dados de seu titular, como nome, número do registro civil, assinatura da Autoridade Certificadora que o emitiu, entre outros, conforme especificado na Política de Segurança de cada Autoridade Certificadora.

O Certificado Digital pode ser usado para a declaração do imposto de renda, em leilões à distância, contratos, transações junto às instituições financeiras, comunicação com os poderes públicos, envio de documentos, etc.

Os advogados, médicos, corretores, contabilistas, engenheiros, agrônomos, farmacêuticos, militares, fiscais, funcionários públicos dos poderes legislativo, executivo e judiciário, etc. possuem carteiras de identidades profissionais, emitidas pelos respectivos órgãos de classe e entidades governamentais, com certificado digital, o que permite a essas pessoas a execução de inúmeras atividades com segurança e sem a necessidade de se deslocar fisicamente.

Cada um dos profissionais acima confecciona e envia documentos eletrônicos (digitais) a vários órgãos públicos. Assim, por exemplo, mediante a implantação do processo eletrônico em 2006, os operadores do Direito envolvidos nos processos judiciais passaram a ter, obrigatoriamente, Certificado Digital para realizarem seus respectivos trabalhos.

Em janeiro de 2007, o Governo Federal instituiu a **Nota Fiscal Eletrônica (NF-e)** como parte do projeto do SPED - Sistema Público de Escrituração Digital (http://sped.rfb.gov.br/).

> "A NF-e tem a sua validade jurídica garantida pela assinatura digital (através de certificado digital do emitente no padrão ICP Brasil, que dá, ao documento, a certeza de sua integridade e de sua autoria) e pela autorização de uso pela administração tributária da unidade federada do

contribuinte, antes da ocorrência do fato gerador." (http://portalnfe.fazenda.mg.gov.br/respostas_VI.html).

"A Nota Fiscal Eletrônica é um arquivo digital, sendo a sua validade jurídica e autenticidade garantida pela assinatura digital através do certificado ICP Brasil NF-e.

O software emissor da Nota Fiscal Eletrônica utiliza o certificado NF-e para assinar digitalmente o arquivo eletrônico da nota fiscal, atestando que foi sua empresa que fez o envio da nota para o portal da Secretaria da Fazenda.

O certificado digital NF-e foi criado para ser utilizado exclusivamente na emissão das notas fiscais eletrônicas (garantindo sua conformidade na Lei)." (https://www.rapidssl.com.br/certificado-digital/nota-fiscal-eletronica.php).

A Nota Fiscal Eletrônica é um modelo nacional (brasileiro) de documento fiscal eletrônico para a substituição da emissão do documento fiscal em papel. Trata-se de um documento de existência apenas digital, emitido e armazenado eletronicamente, com o intuito de documentar, para fins fiscais, uma operação de circulação de mercadorias ou uma prestação serviços, ocorrida entre as partes, e cuja validade jurídica é garantida pela assinatura digital do emissor (garantia de autoria e de integridade) e pela recepção, pela Fazenda, do documento eletrônico, antes da ocorrência da circulação ou saída da mercadoria.

- http://www.nfe.fazenda.gov.br/;
- https://www.fazenda.sp.gov.br/nfe/.

A NF-e (Nota Fiscal Eletrônica) é emitida e armazenada de maneira eletrônica e serve para oficializar as operações de circulação de mercadorias ou de prestação de serviços. Ela é representada por um arquivo XML (*eXtensible Markup Language*) e é identificada unicamente pela Chave de Acesso, um número de 44 dígitos. A validade jurídica da NF-e é garantida pela assinatura digital feita através de um certificado digital.

O **DANFe** (Documento Auxiliar de Nota Fiscal Eletrônica) é uma representação simplificada e impressa em papel legível da Nota Fiscal,

usada geralmente durante o transporte das mercadorias (controle e fiscalização, principalmente, do recolhimento do ICMS - Imposto sobre Circulação de Mercadorias e Serviços). Sua informação mais relevante é a chave da nota, composta por 44 números, que identifica unicamente sua NF-e e permitem a consulta do documento e o download do arquivo XML através do Portal da NF-e (http://www.nfe.fazenda.gov.br/). Pelo fato de não possuir valor fiscal, O DANFe não precisa ser arquivado.

A **Nota Fiscal de Serviços Eletrônica (NFS-e)** é um documento eletrônico que substitui a nota impressa em formulário ou talão. Enquanto a NF-e registra a venda de produtos, enquanto a NFSe (Nota Fiscal de Serviço Eletrônica) tem a função de registrar a prestação de serviços fara fins de cobrança do ISSQN (Imposto Sobre Serviços de Qualquer Natureza). No caso das Notas fiscais eletrônicas, o contribuinte a gera, assinada digitalmente e a transmite para a Secretaria de Fazenda (SEFAZ). Já em se tratando das notas fiscais eletrônicas de serviço, o contribuinte transmite os dados para o Fisco Municipal por meio do Recibo Provisório de Serviços (RPS). A autenticação da NFS-e, portanto, é realizada por meio do envio do arquivo XML do RPS para o webservice do Fisco Municipal. Caso os dados estejam corretos, é gerado o RPS e a comunicação está finalizada.

- http://www.nfedobrasil.com.br/.

O **arquivo XML** é um tipo de arquivo de texto, feito para a leitura pelo (e não através ou no) computador (a linguagem utilizada não é para a leitura humana), com a finalidade de interagir com os sistemas da Secretaria da Fazenda e com os sistemas emissores de NF-e, CTe, CC-e, etc.

O XML é o arquivo padrão de registro na NF-e. Ele é a Nota Fiscal de fato. Seu *layout* (aparência) possui formato padrão em todo país e obedece aos antigos padrões de escrituração fiscal, com a adição de melhorias que visam um maior controle das transações comerciais.

- https://arquivei.com.br/blog/infografico-a-anatomia-da-nfe-e-seus-xmls/.

O arquivo XML depende de programas específicos para serem lidos, como, por exemplo, o DANFE View (http://danfeview.com.br/).

- http://pt.wikihow.com/Abrir-um-Arquivo-XML;
- http://blog.luz.vc/excel/como-importar-e-editar-um-arquivo-xml-para-o-excel/;
- http://www.unimake.com.br/produtos/danfeview/caracteristicas.

Tanto o fornecedor quanto o comprador devem guardar os arquivos XMLs por, no mínimo, 5 (cinco) anos, porque devem ser apresentadas quando solicitados pelo Fisco e, também, em caso de reclamações ou troca de um produto ou serviço. Ressalta-se, entretanto, que não é muito seguro guardar os arquivos em uma pasta no computador, porque, além de dificultar a organização e posterior localização, também o computador pode queimar e, assim, perder tudo. Alguns programas e serviços especializados armazenam as notas e cupons fiscais eletrônicos na nuvem, facilitando a busca desses documentos (NFC-e, NFC-es e CT-es, etc.). Um exemplo é o Arquivei (https://arquivei.com.br/).

Todas as empresas que são obrigadas a emitir a Nota Fiscal Eletrônica, assim como todas as que estão inscritas nos regimes tributários de lucro real ou do lucro presumido e as optantes pelo Simples Nacional com mais de 5 (cinco) funcionários, são obrigadas a ter um certificado digital; vez que sem ele não sequer emitir notas fiscais eletrônicas, muito menos, gerarem e enviarem os demais formulários dos Fiscos (Receitas municipais, estaduais e federal). A partir de 01/01/2017, a obrigatoriedade se estendeu aos empregadores com mais de 3 (três) empregados.

> "Em que etapas da geração da NF-e é necessária a utilização de certificado digital?
> O certificado digital no padrão ICP-Brasil será necessário em dois momentos:
> a) o primeiro é na assinatura digital do documento eletrônico. O certificado digital deverá conter o CNPJ de um dos estabelecimentos da empresa;
> b) o segundo é na transmissão do documento eletrônico. Qualquer certificado digital no padrão ICP-Brasil que identifique uma empresa credenciada a emitir NF-e na unidade federada onde estiver sendo emitida a nota poderá ser utilizado para transmitir o documento eletrônico para a Secretaria da Fazenda e recuperar a resposta com a

autorização de uso, rejeição ou denegação da NF-e, mesmo que não seja de um dos estabelecimentos da empresa emitente.

Importante: apenas o certificado digital que efetuou a transmissão do arquivo eletrônico poderá resgatar a resposta de Autorização de uso, rejeição ou denegação." (http://www.nfe.fazenda.gov.br/portal/perguntasFrequentes.aspx?tipoConteudo=k/E5BakB80o=).

O critério para a obrigatoriedade de emissão de **NF-e – Nota Fiscal Eletrônica** (http://www.nfe.fazenda.gov.br/) é simplesmente o exercício de uma das atividades relacionadas na lista da Obrigatoriedade.

- http://www1.fazenda.gov.br/confaz/confaz/Protocolos/ICMS/2007/pt010_07.htm;
- https://www.confaz.fazenda.gov.br/legislacao/protocolos/2007/pt010_07;
- https://www.fazenda.sp.gov.br/nfe/perguntas_frequentes/respostas_II.asp.

Praticamente todas as empresas estão obrigadas a ter assinatura digital, mediante a utilização de certificado digital válido, para poderem apresentarem declarações às Receitas Federal, Estaduais e Municipais. A exceção, por enquanto, está sendo uma parcela das optantes pelo Simples Nacional (as com menos de 5 funcionários).

- IN RFB 969/2009 - http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=15935.

O certificado digital utilizado para a NF-e pode ser utilizado também no SPED Fiscal.

A **certificação digital do contabilista** (contador e técnico em contabilidade) somente pode ser utilizada para a entrega de obrigações acessórias, que não exigem o E-CNPJ. Entre tais obrigações acessórias, incluem-se a DCTF (Declaração de Débitos e Créditos Tributários Federais), Dacon (Demonstrativo de Apuração de Contribuições Sociais), DIPJ (Declaração de Informações Econômico-fiscais da Pessoa Jurídica),

Decore (Declaração Comprobatória de Percepção de Rendimentos), entre outras.

Para emitir Nota Fiscal Eletrônica (NF-e), transmissão mensal do Sped fiscal e obrigações acessórias, a empresa precisa ter o e-PJ; já para assinatura do conhecimento de transporte eletrônico, é necessário o CT-E. Para a declaração anual Sped contábil o contabilista precisa ter o E-CPF. O e-CNPJ é para empresas e deve ser emitido para o representante legal da companhia. Já o Certificado Digital SSL é somente para os computadores que funcionam como servidores de sistemas ou sites.

> "A Nota Fiscal Eletrônica ou NF-e, é um documento eletrônico fiscal e que tem por fim o registro de uma transferência de propriedade sobre um bem ou uma atividade comercial prestada por uma empresa e uma pessoa física ou outra empresa. A NF-e é a versão eletrônica do documento Nota Fiscal." (https://www.certisign.com.br/certificado-digital/para-empresa/nfe).

> "A NFC-e ou Nota Fiscal de Consumidor Eletrônica é um documento de existência apenas digital, emitido e armazenado eletronicamente, com o intuito de documentar as operações comerciais de venda presencial ou venda para entrega em domicilio o consumidor final (pessoa física ou jurídica) em operação interna e sem geração de crédito de ICMS ao adquirente.
>
> A NFC-e substituirá o tradicional cupom fiscal emitido em lojas, supermercados, drogarias e comércio varejista em geral na maioria dos estados brasileiros." (https://www.certisign.com.br/certificado-digital/para-empresa/nfe).

O **SPED** é a sigla do Sistema Público de Escrituração Digital (http://sped.rfb.gov.br/), que foi instituído através do Decreto 6.022/2007 (http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/Decreto/D6022.htm) e trata-se de um instrumento de unificação das atividades de recepção, validação, armazenamento e autenticação de livros e documentos que integram a escrituração contábil e fiscal dos empresários e das pessoas jurídicas, inclusive as imunes e isentas, mediante fluxo único e computadorizado das informações.

"SPED é a sigla para Sistema Público de Escrituração Digital. Trata-se de um sistema que a Receita Federal disponibiliza para as empresas enviarem informações de natureza fiscal, contábil e previdenciária.

Vamos às diferenças:

SPED Fiscal – substitui a escrituração em papel pela Escrituração Fiscal Digital (EFD), composto por arquivos digitais de documentos fiscais e de informações pertinentes aos fiscos das unidades federadas e da Secretaria da Fazenda, bem como de registros de apuração de impostos referentes às operações e prestações praticadas pelo contribuinte.

SPED Contábil – é a substituição da escrituração em papel pela Escrituração Contábil Digital (ECD). Transmite em versão digital os seguintes livros:

I – Livro Diário e seus auxiliares, se houver;

II – Livro Razão e seus auxiliares, se houver;

III – Livro Balancetes Diários, Balanços e fichas de lançamento comprobatórias dos assentamentos neles transcritos.

Para garantir segurança e validade jurídica às transmissões dos arquivos, a Receita Federal recomenda o uso de um Certificado Digital: e-CPF para o SPED Contábil e o e-CNPJ ou e-CPF para SPED Fiscal. Além disso, o certificado diminui custos operacionais e possibilita a assinatura digital para outras operações via internet." (https://serasa.certificadodigital.com.br/novidades/sped-contabil-e-fiscal-qual-a-diferenca/).

ECF (Emissor de Cupom Fiscal) é um equipamento automatizado que emite cupons e outros documentos fiscais, registrando os dados relativos à quantidade, descrição e valor das mercadorias ou serviços prestados, acumulando-os em totalizadores e contadores específicos, gerando relatórios consolidados e calculando o imposto devido na comercialização de cada produto. Ele é ligado à impressora fiscal e possui um certificado digital próprio. Parece uma impressora comum, mas contém memória extra e programa específico capaz de registrar e acumular vendas (armazena os cupons fiscais criados). O ECF está sendo substituído pelo SAT (projeto exclusivo do Estado de São Paulo). O SAT refere-se ao Sistema Autenticador e Transmissor de Cupons Fiscais Eletrônicos (SAT-CF-e).

Trata-se de um equipamento de baixo custo, com certificado digital, que gera, autentica e transmite para o fisco os Cupons Fiscais Eletrônicos gerados. Esse sistema está operando desde novembro de 2014.

Em síntese, o ECF (Emissor de Cupom Fiscal) é o equipamento instituído pelo Fisco (Receita/Fazenda) para impressão do Cupom Fiscal, que está sendo substituído pelo SAT-CF-e (Sistema de Autenticação e Transmissão de Cupom Fiscal Eletrônico), que emite o CF-e (Cupom Fiscal Eletrônico), um documento eletrônico que substitui o cupom fiscal. Trata-se de um equipamento com certificado digital, que gera, autentica e transmite para o Fisco (SEFAZ - Secretaria da Fazenda) os Cupons Fiscais Eletrônicos gerados.

A **NFC-e (Nota Fiscal de Consumidor Eletrônica)** é o projeto que está substituindo o tradicional Cupom Fiscal emitido por ECF e a Nota Fiscal de venda ao consumidor - modelo 2 - emitida manualmente em lojas, supermercados, drogarias e comércio varejista em geral na grande maioria dos estados brasileiros; exceto São Paulo que implanta o SAT-CF-e (Sistema de Autenticação e Transmissão de Cupom Fiscal Eletrônico) e Santa Catarina que adota o PAF-ECF (programa aplicativo fiscal, emissor de cupom fiscal).

O Projeto NFC-e é um módulo do Projeto do SPED - Sistema Público de Escrituração Digital (http://sped.rfb.gov.br/), do qual fazem parte também a NF-e, o CT-e - Conhecimento de Transporte Eletrônico (http://www.cte.fazenda.gov.br/), Escrita Fiscal Digital e a Escrita Contábil Digital.

- https://mdfe-portal.sefaz.rs.gov.br/;
- https://www.govdigital.com.br/;
- http://idg.receita.fazenda.gov.br/orientacao/tributaria/senhas-e-procuracoes/senhas/certificados-digitais;
- http://www.iti.gov.br/certificacao-digital/certificado-digital;
- http://ascontsistemas.com.br/nfc-e/.

O cupom fiscal impresso passou a ser chamado de DANFE NFC-e (Documento Auxiliar da Nota Fiscal Eletrônica para Consumidor Final). Nele consta as informações dos produtos vendidos, dados do comprador, formas de pagamento e as informações sobre a autorização de uso do Cupom pela Secretaria da Fazenda Estadual.

A NFC-e (Nota Fiscal de Consumidor Eletrônica) visa extinguir o cupom fiscal e substituir a necessidade do ECF (Emissor de Cupom Fiscal), que dependia de impressoras homologadas pelo governo. ECF também pode ser a sigla de Escrituração Contábil Fiscal.

A emissão da NFC-e segue as mesmas regras da NF-e, precisando ter o certificado digital no padrão ICP Brasil e o CNPJ da empresa. Para usar o sistema a empresa precisa estar cadastrada como emitente de nota fiscal eletrônica, estar com a inscrição estadual regularizada, possuir o equipamento do SAT ativo e estar conectada à Internet.

Por outras palavras, a NFC-e é emitida pelo contribuinte utilizando um Programa Emissor, que deve ser instalado nos computadores da empresa. Após ser preenchida e assinada eletronicamente (com “Certificado Digital”) a NFC-e é transmitida pela internet para a SEFAZ do seu Estado. Após a emissão da NFC-e, em fração de segundos os computadores da SEFAZ verificam a autenticidade dos documentos e a consistência das informações. Se não houver nenhum erro, o contribuinte recebe de volta, em seu programa, o número da Autorização de Uso. A partir deste momento a NFC-e tem validade e pode acobertar a venda. Neste momento em que o documento é autorizado, o DANFE poderá ser gerado. O DANFE é a NFC-e impressa, onde contém a chave de acesso da mesma e o QrCode, para que o consumidor possa consultar através do leitor de QrCode a NFC-e na SEFAZ.

Sua validade jurídica é garantida pela assinatura digital (através de certificado digital) feita pelo equipamento SAT. Como o Cupom Fiscal Eletrônico só existe na forma digital, o consumidor receberá como comprovante um extrato chamado Extrato do CF-e-SAT.

Em resumo, o cupom impresso do SAT ou da NFC possui um código de barras bidimensional (chamado QR-Code), que pode ser lido pela câmera

fotográfica de smartphones ou tablets, informando ao consumidor a validade legal do cupom emitido.

Portanto, o Extrato do CF-e-SAT é somente uma referência para que o consumidor final controle suas compras e consulte o Cupom Fiscal Eletrônico.

Independentemente de o consumidor receber a versão impressa, ele poderá consultar os detalhes de sua compra utilizando a Internet para acessar o endereço eletrônico do Portal da Secretaria de Fazenda de Estado do contribuinte. Para facilitar a vida do consumidor o endereço do portal NFC-e para consulta estará impresso no DANFE NFC-e. Aqueles compradores que possuírem smartphones poderão fazer o acesso através da leitura do QR Code impresso no documento ou digitando o número da Chave de Acesso.

Os cupons fiscais, portanto, agora são CF-e-SAT (Cupom Fiscal Eletrônico do Sistema Autenticador e Transmissor); ou seja, as informações são transmitidas via Internet ao banco de dados da Receita Estadual e são passíveis de consulta através do QR Code neles impressos.

- https://www.quantosobra.com.br/cupom-fiscal-eletronico-nfce-nota-fiscal-do-consumidor-eletronico/;
- https://www.fazenda.sp.gov.br/nfe/;
- https://www.fazenda.sp.gov.br/nfe/emissor/emissor.asp;
- https://www.fazenda.sp.gov.br/cte/emissor/emissor.asp;
- https://www.fazenda.sp.gov.br/mdfe/emissor/emissor.htm;
- http://www.pfe.fazenda.sp.gov.br/guia_procedimentos_ecf_10.shtm;
- http://www.fazenda.sp.gov.br/sat/;
- https://satsp.fazenda.sp.gov.br/COMSAT/Public/ConsultaPublica/ConsultaPublicaCfe.aspx;
- http://www.fazenda.sp.gov.br/sat/legislacao/vigentes.asp;
- http://www.fazenda.sp.gov.br/guia/icms/ecredrural.shtm.

A **eFinanceira**, a obrigação acessória do SPED (Sistema Público de Escrituração Digital), que é composta por arquivos digitais referentes ao cadastro, abertura, fechamento e auxiliares, exige o uso de um Certificado Digital do representante legal da empresa ou procurador constituído para o envio das informações.

As empresas que ainda não estejam obrigadas a emitir nota fiscal eletrônica (ou seja, que ainda não tenham certificado digital) podem acessar o diretamente o e-CAC - Centro Virtual de Atendimento (https://cav.receita.fazenda.gov.br/eCAC/publico/login.aspx) e fazer uma procuração eletrônica autorizando um contabilista que tenha o E-CNPJ a entregar as declarações certificadas de tributos.

As sociedades seguradoras, de capitalização e entidades abertas de previdência complementar, também estão obrigadas a utilizarem Certificado Digital junto a SUSEP - Superintendência de Seguros Privados (http://www.susep.gov.br/).

A **Conectividade Social** (http://www.caixa.gov.br/empresa/conectividade-social/Paginas/default.aspx) é um canal eletrônico de relacionamento, utilizado para troca de informações entre a Caixa Econômica Federal e as empresas, escritórios de contabilidade, sindicatos, prefeituras e outros entes. O canal dispõe de diversas funcionalidades para os usuários, como a transmissão do arquivo do Sistema Empresa de Recolhimento do FGTS e Informações à Previdência Social - SEFIP, envio das informações relativas ao CAIXA PIS/Empresa, encaminhamento do arquivo da GRRF (Guia de Recolhimento Rescisório do FGTS), obtenção de extrato da conta vinculada aos trabalhadores, entre muitos outros. Exige Certificado Digital.

O **eSocial** (http://www.esocial.gov.br/) é um sistema do Governo Federal voltado para a unificação da prestação de informações do empregador doméstico com relação aos seus empregados, tais como: cadastramento, vínculos, contribuições previdenciárias e folha de pagamento. O site é responsável pela emissão do DAE (Documento de Arrecadação do eSocial). O sistema é gerido em conjunto pelas seguintes instituições: Caixa Econômica Federal (CEF), Instituto Nacional de Seguro Social (INSS),

Ministério do Trabalho e da Previdência Social e Receita Federal do Brasil (RF). Ainda não é obrigatório o Certificado Digital.

Token é um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB. Existe também a variante para *Smart Cards* (cartões inteligentes) e smartphones, que são capazes de realizar as mesmas tarefas do token.

> "O token é um hardware capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas as chaves, estas estarão totalmente protegidas, pois não será possível exportá-las ou retirá-las do token (seu *hardware* criptográfico), além de protegê-las de riscos como roubo ou violação." (http://www.digitalsecurity.com.br/o-que-e-certificado-digital-para-nota-fiscal-eletronica.aspx).

Um "**smart card**", ou cartão inteligente, é um cartão que geralmente assemelha-se em forma e tamanho a um cartão de crédito convencional de plástico com tarja magnética; mas seu interior é completamente diferente. Primeiramente, ele possui um interior, enquanto um cartão de crédito normal é um simples pedaço de plástico. O interior de um cartão inteligente normalmente contém microprocessador e memória embutidos. Este microprocessador fica sob uma placa de contato de ouro em uma das faces do cartão. Pense no microprocessador como um substituto da usual fita magnética em um cartão de crédito ou débito. É também encontrado também nos celulares GSM (“Global System for Mobile Communications”) no chip da linha de celular. Os cartões inteligentes podem ser utilizados com leitores conectados em um computador pessoal a fim de autenticar um usuário. Softwares de navegação na Internet também podem utilizar a tecnologia do *smart card* para complementar SSL (“Secure Sockets Layer”) utilizado para melhorar a segurança em transações na Internet.

Certificados para Servidores Web ou simplesmente **Certificados SSL** são certificados digitais para identificar um website na Internet. O SSL (*Secure Sockets Layer*) é uma tecnologia de segurança que é utilizada para codificar os dados transferidos entre o computador de um usuário e um web site. O

SSL usa um sistema de criptografia que utiliza duas chaves para criptografar os dados, uma chave pública conhecida por todos e uma chave privada conhecida apenas pelo destinatário. O SSL é a única e eficaz maneira de obter segurança de dados em comércio eletrônico. Quando um SSL – Certificado Digital está instalado no website, um ícone de um cadeado aparece no navegador e o endereço começa com “https://” ao invés de “http://” informando que os dados serão criptografados.

Na prática, o certificado digital funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos.

Detalhe, as moedas criptografas ou matemáticas, como a **bitcoin, na verdade são como os certificados digitais**, só que ao invés desses dados serem a descrição ou qualificação de uma pessoa (nome completo, números da identidade e do CPF, etc.) é uma sequência alfanumérica que passa de pessoa para pessoa. Do mesmo modo que o token (pendrive) ou cartão de plástico com chip não é o certificado digital propriamente dito, mas tão somente o local onde ele está armazenado, o mesmo ocorre com as moedas digitais. De modo semelhante à exigência de a pessoa ter que digitar uma senha para assinar digitalmente com o certificado digital, também é exigido senha para transferir os créditos virtuais.

Tanto é assim que a *Blockchain* também pode e, de fato, emite certificados digitais (http://certificates.media.mit.edu/); inclusive no Brasil (https://originalmy.com/).

Portanto, muitas pessoas já estão utilizando diariamente a tecnologia equivalentes das moedas criptográficas sem saber.

A legislação sobre a certificação digital no Brasil consta em http://www.iti.gov.br/legislacao e http://www.iti.gov.br/legislacao/143-icp-brasil/legislacao/790-doc-icp.

Para entender melhor, ou se profundar, sobre o que são as bitcoins e como elas são feitas, confira os capítulos: "*HASH*", "CERTIFICADOS DIGITAIS",

"*PEER-TO-PEER* (P2P)", "BITCOIN", "COMO A BITCOIN É FEITA?", "*BLOCKCHAIN*" e "COMO MINERAR BITCOINS E ALTCOINS".

LADO NEGRO DAS MOEDAS VIRTUAIS

Como não há bancos ou governos centralizando as operações, as moedas virtuais são praticamente impossíveis de serem rastreadas e isso se torna um grande inconveniente por ser um atrativo para criminosos cibernéticos atuarem, recebendo em bitcoins (ou outras moedas virtuais) e depois fazendo o câmbio em dinheiro do mundo real (físico), sem precisar prestar contas de como, onde, quando, por que ou com quem conseguiram tais valores. Portanto, dado o caráter anônimo das transações, as moedas virtuais são bastante usadas por quem trabalha no âmbito ilegal da Internet.

Algumas criptomoedas foram desenhadas para oferecer completo anonimato, tais como a DarkCoin e a ZeroCoin.

Na ***Deep Web*** (também chamada de *Deepnet*, Web Invisível, *Undernet* ou Web oculta), os pagamentos para compra de drogas e solicitações ilegais, como de assassinos de aluguel, já foram feitos via bitcoins. Afinal, nenhum criminoso quer ser pego oferecendo seus serviços na web e a bitcoin era a única forma de o anonimato para essas transações. Assim, um meio de troca digital como a bitcoin impõe uma barreira quase intransponível, dificultando a atividade de combate a ocultação e "lavagem" do dinheiro "sujo" (ilícito).

- "100 Casos de Lavagem de Dinheiro" - http://www.coaf.fazenda.gov.br/menu/pld-ft/publicacoes/100_Casos.pdf/@@download/file/100_Casos.pdf.

Aliás, existe o *Dark Wallet* que é um software feito especialmente para facilitar a "lavagem de dinheiro" em Bitcoins.

A ***Surface Web*** ("Internet superficial") é a parte da **Web** ("rede") ou WWW - *World Wide Web* ("rede de alcance mundial" ou "teia mundial" = sistema de documentos em **hipermídia/hipermédia** (reunião e fusão de várias mídias [todo suporte de difusão da informação: textos, imagens, sons, etc.] num ambiente computacional, interconectados por **links/hiperlinks** [texto colorido e/ou sublinhado ou elemento gráfico em que o usuário clica para ir para outra página ou tela ou outro lugar da mesma página ou tela], que permite acesso simultâneo de modo interativo, enquanto que **multimídia** é a mera reunião mídias com acesso

linear) interligados e executados na Internet) indexada pelos motores de busca. A parte que não é indexada (catalogada) chama-se ***Deep Web*** ("Internet Profunda"). Motores de busca constroem um **banco/base de dados** (conjunto de arquivos [informações e documentos] indexados e relacionados entre si, de maneira estruturada, à disposição para consulta, introdução e atualização) através de programas chamados ***Web Crawlers*** ("rastreador da web": ***software*** [programa de computador] desenvolvido para realizar uma varredura na internet de maneira sistemática através de informação) ou *spiders* (aranhas) que começam com uma lista de páginas (sites) conhecidas da **internet** (sistema global de redes de computadores interligadas ou imensa quantidade de computadores conectados entre si). Esse programa pega uma cópia de cada página (site) e indexa-a, guardando informações importantes que permitirão que a página seja facilmente localizada e acessada novamente mais tarde. Não se deve confundir com ***Dark Internet***, que se trata da parte da internet que não pode ser acessada ou que está inacessível por meios convencionais e nem com ***Darknet***, que não é uma simples rede de compartilhamento de arquivos, mas uma rede em camadas, onde utiliza um grande esforço para manter os dados dos utilizadores anônimos. Já o ***DarkMarket*** (exemplo, http://darkmarket.bz/), traduzindo, mercado negro, é um protótipo de mercado livre, similar ao ***Silk Road*** (https://pt.wikipedia.org/wiki/Silk_Road), que não pode ser derrubado graças ao seu servidor descentralizado. O **browser** (navegador da Internet) **Tor** (https://www.torproject.org/), acrônimo para ***The Onion Router*** (https://www.onion-router.net/), é um *software* livre e de código aberto que proporciona o anonimato pessoal ao navegar na Internet. Enquanto que o ***PayPub*** (https://github.com/unsystem/paypub) é um aplicativo que utiliza transações em Bitcoins para incentivar pessoas a vazarem documentos sigilosos (tanto públicos como privados), a ***Dark Wallet*** (https://github.com/darkwallet/darkwallet/releases/tag/0.2.0 e https://www.darkwallet.is/) é um conjunto de ferramentas (***plug-in***, *add-in* ou *add-on*: módulo de extensão que adiciona recursos ou funções a um *software*) para armazenar, enviar e receber bitcoins de forma totalmente anônima.

- Como Acessar a *Deep Web* - Atualização - https://www.youtube.com/watch?v=NwzW1FhW8P4.

DOS RISCOS E PERIGOS DAS MOEDAS VIRTUAIS

A popularidade das moedas digitais cresce cada vez mais e, nessa mesma proporção, também as ações mal-intencionadas; já existem vírus, *trojans*, *phishings* e golpes no comércio das moedas eletrônicas.

Uma das garantias de segurança do Bitcoin advém do fato de seu sistema ser de código aberto (*open source*); ou seja, os próprios usuários verificam que não há nenhum conteúdo maligno no sistema.

Entretanto, existem vários riscos para quem quer investir ou criar uma pequena economia em bitcoins; pois eles não têm características de titularidade, dificultando a prova de sua propriedade. Por outras palavras, a propriedade é definida pela posse.

Outro problema é inexistência de seguro contra furto, roubo, perda, dano ou envio para a pessoa errada. Não há a possibilidade de estorno como nos bancos convencionais. Uma vez que as moedas saem da sua carteira, você não tem mais direito sobre elas. Porém, a operadora de bolsa norte-americana de bitcoin, Payward, disse em novembro de 2014 que iria trabalhar para recuperar alguns milhões de dólares perdidos pela japonesa Mt. Gox, que já foi a maior bolsa de bitcoins do mundo antes de quebrar em 2014 por causa de constantes ataques *hackers*.

- http://oglobo.globo.com/sociedade/tecnologia/em-meio-escandalo-gigante-dos-bitcoins-mt-gox-pede-recuperacao-judicial-nos-eua-11835491.

Como a moeda virtual não existe de forma palpável, ela em si, e cada transação dela, são somente códigos alfanuméricos trocados entre quem vende e quem compra algo. Como não há bancos ou governos centralizando as operações, elas são praticamente impossíveis de serem rastreadas. Alguns especialistas, contudo, afirmam que uma negociação de grande valor poderia ser identificada através da triangulação de informações. Existem inúmeras formas de se fazer esta associação e as agências de segurança e governos têm acesso a várias delas.

Toda transação feita via Bitcoin é pública. Ao acompanhar um arquivo público chamado *Blockchain* (links infra), é possível saber, hipoteticamente,

que a Carteira de Bitcoins "X" fez uma transferência para a Carteira de Bitcoins "Y", tornando possível rastrear onde estão as Bitcoins roubadas, mas sem saber quem é o proprietário delas. Contudo, se o espertalhão tentar tirar as Bitcoins daquele ambiente e transformá-la em dinheiro do mundo real, vai precisar fazer um cadastro, e é exatamente nesse momento em que ele é pego. Qualquer criminoso que queira converter uma grande quantidade de dinheiro em bitcoins teria que, em algum momento, fazer uso das casas de câmbio de Bitcoins, e estas têm se esforçado bastante para funcionar dentro da legislação federal norte-americana, que impede práticas que possam ser usadas na lavagem de dinheiro ilegal. O ciberladrão vai ter problemas ao tentar lavar as bitcoins roubadas; pois os serviços que se propõem a fazer esse serviço, como o Bitcoin Laundry ou o Bitmix, no geral não fazem o que prometem ou, pior, roubam as bitcoins que deveriam ser lavadas.

- https://blockchain.info/;
- https://bitcoinchain.com/;
- https://new.bitcoinchain.com/;
- http://block.oklink.com/;
- https://blockchains.io/.

As carteiras e endereços bitcoins não possuem qualquer informação pessoal sobre seus proprietários e são considerados anônimos.

A assinatura criptográfica é um mecanismo matemático que permite que alguém prove ser o proprietário.

Quem portar é o dono naquele momento e não se pode provar de onde veio. Isto gera um interesse muito grande de *hackers* para extrair códigos de Bitcoins de instituições onde são guardados.

> "***Hacker*** é uma palavra em inglês do âmbito da informática que indica uma pessoa que possui interesse e um bom conhecimento nessa área, sendo capaz de fazer *hack* (uma modificação) em algum sistema informático.

> Em inglês, a palavra *hack* é um verbo que significa cortar alguma coisa de forma irregular ou grosseira. Assim, a partir da década de 50 do século XX, a palavra *hack* começou a ser usada para designar uma alteração inteligente em alguma máquina. Mais tarde, este termo passou a ser usado exclusivamente no âmbito da programação informática.
>
> Alguns *hackers* são contratados por grandes empresas para testarem a segurança dos seus sistemas informáticos. Dessa forma, os *hackers* tentam entrar no sistema, descobrindo as suas fragilidades para melhorar a segurança e prevenir futuros ataques.
>
> [...]
>
> Apesar disso, muitas vezes uma pessoa que usa os seus conhecimentos de informática e programação para praticar atos ilegais são conhecidas como *crackers* e não *hackers*.
>
> Enquanto a maioria dos *hackers* usam o seu conhecimento para demonstrar a vulnerabilidade de um sistema, os *crackers* têm como objetivo danificá-lo ou modificá-lo para obter algum tipo de benefício." (http://www.significados.com.br/hacker/). Grifo nosso.

Uma parcela das pessoas entende que a **distinção entre "hacker" e "cracker"** teria caído em desuso. Alegam que o verbo “to hack”, do qual origina a palavra "hacker", teria a conotação de driblar sistemas de segurança ou de invadir um computador ou celular, não importando a finalidade. Desse modo, a palavra "hacker" seria neutra, não diferenciando entre bem e mal. Apesar dessas pessoas alegarem que não haveria necessidade de fazer distinção entre bom e mal ou de usar outra expressão como contraponto, contraditoriamente, para distinguir os diferentes tipos de atividade *hacker* utilizam-se das expressões “white hat” (chapéu branco), significando *hacker* "do bem"; “black hat” (chapéu preto) significando cracker; e, "gray hat" (chapéu cinza), para aqueles que não se encaixam inteiramente em nenhuma das opções anteriores, estando numa zona cinzenta ou situação intermediária.

A maleabilidade de transação permite que o identificador de uma transação seja alterado após ela já ter sido propagada pela rede (P2P). Como o Bitcoin leva cerca de 10 (dez) minutos para validar uma transação e existe a possibilidade de que uma transação tenha de ser refeita caso conste de um chamado "bloco órfão", sistemas que conferem saques em bitcoin

precisam identificar de alguma forma quando uma transação foi finalmente concluída. Alguns sistemas, incluindo o Silk Road, fazem isso procurando apenas o identificador de transação. O problema é que o identificador da transação não faz parte do conteúdo assinado digitalmente e pode ser manipulado.

Dessa forma, um *hacker* pode impedir o sistema de saque de confirmar que a transação ocorreu com sucesso, propagando a mesma transação com um identificador diferente. O sistema não vai encontrar a transação original e tentará então fazer a transferência novamente; a cada vez, o *hacker* receberá mais moedas, e seu saldo nunca será descontado porque, do ponto de vista do sistema, a transação está falhando a cada tentativa.

Não se trata de uma "falha" do Bitcoin, mas sim um funcionamento pouco intuitivo para programadores que estão criando sistemas que interagem com ele. Em quase todo tipo de sistema, um identificador pode ser confiado; no Bitcoin, não. Sistemas de saques podem impedir o ataque realizando uma verificação de transação que não dependa exclusivamente do identificador.

Em síntese, uma transação Bitcoin é normalmente implantada dentro de poucos segundos e começa a ser confirmada nos 10 minutos seguintes. Durante esse tempo, a transação pode ser considerada autêntica, mas ainda reversível. Cada confirmação exponencialmente diminui o risco de uma transação revertida. Entretanto, é possível pagar uma pequena taxa de transação para não ter que ficar na espera das confirmações ou, então, usar um sistema de detecção para as operações inseguras.

Em 2011, o servidor da **Mt. Gox** (https://www.mtgox.com/) foi invadido por uma conta desconhecida que conseguiu faturar 25 mil bitcoins. Em 2014 a Mt. Gox abriu pedido de falência após um roubou astronômico. Dessa vez, os *hackers* conseguiram levar 744.408 Bitcoins, o que dá quase 440 milhões de dólares. Porém, há suspeitas de que os próprios administradores da corretora de câmbio possam estar envolvidos.

O Mt. Gox era o maior local de troca de bitcoins e acabou por entrar em colapso, com o seu dono a ser preso e acusado de fraude. Agora, os utilizadores queixam-se na Justiça, mas podem não ter muita sorte, se todos

os juízes decidirem como foi feito no Japão. O juiz Masumi Kurachi deliberou que as bitcoins não têm as "qualidades tangíveis" para constituírem propriedade de algum utilizador, noticiou o Engadget. A decisão pode prender-se apenas com a legislação do país e as vítimas de outros países até poderão ser indenizadas, no entanto, no Japão poderá servir de indicador.

O site ***Silk Road*** (http://silkroaddrugs.org/) era na verdade um grande mercado de drogas que aceitava bitcoins como forma de pagamento. A página que foi fechada em 2013 pelos federais (FBI) dos Estados Unidos, acabou sendo reaberta algum tempo depois por algum malandro que tinha como única ideia pegar o dinheiro virtual que estava armazenado lá (4.474 bitcoins). Depois que o Silk Road saiu do ar, um novo mercado negro se popularizou na web.

O ***Sheep Marketplace*** (http://www.thesheepmarket.com/) trabalhava de forma similar, fazendo negociações com bitcoins. Logo, ele se tornou um alvo em potencial para os *hackers* de plantão. Em apenas dois meses, a página tinha quase 100 mil bitcoins em caixa e uma enormidade de usuários. Os invasores fizeram um golpe muito bem planejado, levando 96 mil bitcoins.

Em fevereiro de 2015, a **Cavirtex**, maior bolsa Bitcoin do Canadá, encerrou as atividades após ter sofrido uma falha de segurança.

- http://itforum365.com.br/noticias/detalhe/115064/maior-bolsa-de-bitcoin-do-canada-e-encerrada-apos-suspeita-de-ataque.

Em 2015, a companhia de trocas de bitcoins, **My Coin**, foi exposta como fraudulenta; o que custou até 378 milhões de dólares a seus investidores.

- http://elbitcoin.org/el-escandalo-de-mycoin-en-hong-kong-una-leccion-mas/.

Em abril de 2016, a *exchange* australiana **Igot** também provocou um escândalo com suas irregularidades.

Entre julho e agosto de 2016, cerca de 72 milhões de dólares em bitcoins (119.756 bitcoins) foram furtados das contas dos usuários de uma das

maiores plataformas de troca em Hong Kong, a **Bitfinex**. No início de 2016, a empresa foi condenada a pagar 75 mil dólares por participar de operações ilegais fora da bolsa de mercadorias financiadas em bitcoins e outras moedas digitais.

- http://www1.folha.uol.com.br/mercado/2016/08/1798366-bolsa-que-negocia-bitcoin-suspende-operacoes-apos-ataque-de-hackers.shtml;
- http://istoe.com.br/bolsa-de-bitcoin-suspende-operaes-por-roubo-de-hackers/;
- http://economia.uol.com.br/noticias/reuters/2016/08/03/plataforma-de-cambio-bitfinex-sofre-roubo-de-us-72-mi-em-bitcoins.htm;
- http://economia.uol.com.br/noticias/afp/2016/08/03/roubo-milionario-em-plataforma-de-bitcoin-da-novo-golpe-na-divisa-digital.htm;
- http://www.istoedinheiro.com.br/noticias/economia/20160803/roubo-milionario-plataforma-bitcoin-novo-golpe-divisa-digital/399683;
- http://zh.clicrbs.com.br/rs/noticias/noticia/2016/08/roubo-milionario-em-plataforma-de-bitcoin-da-novo-golpe-na-divisa-digital-7132734.html;
- http://noticias.bol.uol.com.br/ultimas-noticias/economia/2016/08/03/roubo-milionario-em-plataforma-de-bitcoin-da-novo-golpe-na-divisa-digital.htm;
- http://economia.uol.com.br/noticias/afp/2016/08/03/roubo-milionario-em-plataforma-de-bitcoin-da-novo-golpe-na-divisa-digital.htm;
- http://economia.uol.com.br/noticias/bloomberg/2016/08/12/traders-de-bitcoin-perdem-milhoes-com-ataque-de-hackers.htm;
- http://www.eleconomista.es/divisas/noticias/7744447/08/16/Unos-hackers-roban-120000-bitcoins-la-cotizacion-de-la-moneda-virtual-se-hunde-un-20-en-solo-una-semana.html.

SCAM é o termo em inglês para designar um esquema fraudulento, algo que é usado apenas para prejudicar, tomar o dinheiro alheio. O desenvolvedor que faz uma *scam* quer furtar e, assim, por exemplo, lança uma *exchange*, uma carteira, uma piscina, uma mineradora e/ou uma nova moeda prometendo mil maravilhas; mas depois de um tempo some com o dinheiro de suas vítimas. Confira uma **lista negra** em http://www.badbitcoin.org/thebadlist/.

Phishing (pescaria), termo derivado da palavra inglesa "fishing" (pesca), é uma forma de fraude eletrônica que, através de iscas ou armadilhas (dados [e-mails, sites, conversas, links, etc.] falsos), objetiva adquirir ("pescar") dados pessoais, confidenciais e sigilosos, tais como, por exemplos, nome de usuário (login), senhas, dados financeiros (contas bancárias, cartões de crédito, etc.)... O *spear phishing* consegue identificar com qual entidade financeira a vítima possui relacionamento, tornando o golpe personalizado. Já o *pharming* é uma evolução do *phishing* que não necessita da isca. O DNS *poisoning* assume o controle de um servidor DNS fazendo com que as requisições de acesso a um certo domínio sejam direcionadas a um endereço IP falso (não corresponde ao endereço ou domínio desejado pela vítima); ou seja, encaminha para um servidor malicioso. Existem softwares com a função de antiphishing.

> "Como o phishing funciona
>
> Na maioria dos casos, os *phishers* (propagadores de *phishing*) enviam uma onda de e-mails de spam, às vezes até milhões de mensagens. Cada e-mail contém uma mensagem que parece ter sido enviada por uma empresa conhecida e confiável. Geralmente, a mensagem inclui o logotipo e o nome da empresa e, quase sempre, tenta provocar uma resposta emocional a uma falsa crise. Contendo uma linguagem comercial e urgente, o e-mail quase sempre solicita informações pessoais do usuário. Algumas vezes, o e-mail direciona o destinatário diretamente para um site falso. O website, assim como o e-mail, parece autêntico e, em alguns casos, o URL pode ter sido mascarado para sugerir que o endereço da Web pareça real.
>
> O website falso solicita, com urgência, que o visitante forneça informações confidenciais, como números de CPF, números de contas bancárias, senhas, etc. Como o e-mail e o site correspondente parecem legítimos, o *phisher* espera que pelo menos uma fração dos destinatários seja convencida a enviar seus dados. Apesar de ser impossível saber a taxa real de resposta das vítimas a todos os ataques de phishing, acredita-se que uma média de um a dez por cento dos destinatários são enganados por uma campanha de phishing bem-sucedida, com uma taxa de respostas de mais ou menos cinco por cento. Para se ter uma ideia

melhor, as campanhas de spam normalmente têm uma taxa de resposta de menos de um por cento." (http://br.norton.com/cybercrime-phishing).

"Os criminosos se aproveitam dos malwares e vírus que andam espalhados pela internet para poder infectar e modificar o browser (navegador de internet) do computador do usuário. Estando infectado, quando o internauta digita o endereço eletrônico de um site, o navegador redireciona a página para um site falso, mas com as mesmas características estéticas do original.

O internauta pensa que está no website correto, já que não clicou em nenhum link estranho e digitou o endereço diretamente na URL do browser, e acaba fornecendo os seus dados bancários e pessoais mais facilmente, sem desconfiar que está sofrendo um golpe." (https://www.significados.com.br/phishing/).

Saiba mais sobre **fraudes em Bitcoin** em:

- http://gizmodo.uol.com.br/maiores-assaltos-a-bitcoin/;
- http://m.tecmundo.com.br/bitcoin/52098-ladroes-digitais-os-maiores-roubos-de-bitcoins-de-todos-os-tempos.htm;
- http://marketingmultinivel.pt/bitcoin-usado-disfarce-de-fraudes-multinivel/;
- https://www.publico.pt/tecnologia/noticia/bitcoin-cai-depois-de-hackers-roubarem-65-milhoes-de-dolares-na-moeda-virtual-1740170;
- https://www.coinbr.net/blog/por-que-as-pessoas-caem-em-golpes-e-fraudes-relacionadas-a-bitcoin/;
- http://economia.estadao.com.br/noticias/geral,bitcoin-fraude-mais-rapida-do-que-a-lei-imp-,1105475;
- http://g1.globo.com/tecnologia/blog/seguranca-digital/post/empresas-de-mineracao-de-bitcoin-sao-acusadas-de-fraude-nos-eua.html;
- http://oglobo.globo.com/economia/negocios/bolsa-de-bitcoin-suspende-operacoes-por-roubo-de-hackers-19842605;
- http://www.badbitcoin.org/;
- http://www.tenhodividas.com/getcoin-mentira-bitcoins;
- http://www.tenhodividas.com/onecoin-e-uma-fraude;

- http://brasil.elpais.com/brasil/2015/06/19/internacional/1434729885_812527.html;
- http://biskates.pt/paymony-golpe-fraude-esquema-ponzi/;
- http://marketingmultinivel.pt/bitcoin-usado-disfarce-de-fraudes-multinivel/;
- http://coinbrasil.blogspot.com.br/p/sites-scams.html;
- http://blog.bitcoin-portugal.com/2011/07/sera-mybitcoin-uma-fraude/;
- http://sobrecoins.blogspot.com.br/2015/05/scam-fraude.html;
- http://www.bitcoinnews.com.br/bitcoinbrasil/mineracao-de-bitcoin-na-nuvem-se-parece-bom-demais-para-ser-verdade-provavelmente-podee-verdade-genesis/;
- Como multiplicar seus bitcoins (É GOLPE) - https://www.youtube.com/watch?v=PULBdgCs--Q;
- http://www.ondeinvestirdinheiro.com/digitalgeneration-coingeneration-nao-paga-aos-founders-e-scam/;
- http://marketingmultinivel.pt/bitcoin-usado-disfarce-de-fraudes-multinivel/;
- Como identificar golpes no ramo de mineracao de bitcoins - https://www.youtube.com/watch?v=IIlptMqHRJ8.

Não é pelo simples fato da cripto moeda não ser regulamenta que seja sinônimo de ilicitude, de crime, de fraude ou de risco. Do mesmo modo que qualquer outra forma de pagamento online (*e-commerce*, comércio eletrônico, comércio virtual ou venda não-presencial) ou operação através do *internet banking*, existem estelionatários, golpistas, crackers e ladrões. Praticamente as mesmas recomendações de cautela, prevenção e segurança aplicáveis a qualquer compra pela Internet (e/ou acesso à conta bancária online se aplica às moedas eletrônicas. Um grande diferencial é a falta de informações que torna as vítimas mais suscetíveis aos golpes ante à crendice ingênua (ou até mesmo gananciosa) em estelionatários.

- http://olhardigital.uol.com.br/fique_seguro/noticia/hackers-roubam-mais-de-us-1-bilhao-de-bancos-em-30-paises/46850;
- http://www.s3commerce.com.br/blog/120/os-diversos-cenarios-da-seguranca-no-e-commerce.

Os grandes problemas das moedas virtuais são a **volatilidade da cotação** (possibilidade de súbita e grande oscilação de seu valor; ou seja, instabilidade monetária), a possibilidade de **efemeridade** (tal como uma moda momentânea ou passageira, pode ocorrer de ser abandonada repentinamente; ou seja, de repente não ser mais aceita ou ter validade), a **eventual má fé de seus desenvolvedores** (golpistas criam moedas eletrônicas com o único propósito de somente eles enriquecerem) e o **risco do Poder Judiciário entender que a moeda virtual não seja um bem** e, em razão disso, não merecer proteção estatal, deixando impunes os golpistas e ladrões.

As **trapaças em moedas digitais** são inúmeras. Senão vejamos algumas hipóteses que os golpistas podem fazer:

- Acessar ou invadir o dispositivo (computador, celular, etc.) da vítima para encontrar as moedas digitais, senhas, chaves e demais informações pessoais (nome completo, números dos documentos pessoais, data de nascimento, etc.);

- Invasões aos sites onde estão os arquivos e/ou informações acima descritas;

- Instalar, ou fazer a vítima instalar, algum programa ou algoritmo malicioso ou infectado;

- Criar um software (cliente, carteira, mineração, etc.) similar (*fake*, falso) ao software usado pela moeda virtual;

- Criar um site falso imitando um site utilizado no manuseio da moeda digital;

- Simular que vende moedas digitais ou presta serviços relacionados à mesma, como, por exemplo, falsa mineração em nuvem (GetEasy, Paymony, etc.);

- Dominar o dispositivo da vítima para que minere moedas digitais;

- Fechamento, súbito e inesperado, de bolsas de investimentos, de mineradoras na nuvem e de outras aplicações em moedas virtuais;

- A moeda eletrônica escolhida para a compra a ou aplicação não existir;

- O investimento em moeda eletrônica ser fachada de uma pirâmide financeira (fraudes multinível), como o VOIP foi usado como isca na TelexFree e os rastreadores de veículos pela BBOM. Exemplos são o Eternyon e o Wings Network (http://tenhodividas.com/eternyon-e-esquema-em-piramide);

- Sites que prometem multiplicar as moedas digitais.

Hoje em dia minerar bitcoins não é tão fácil e é necessário um PC muito caro para poder minerar apenas 1 bitcoin. A cada mês que passa, torna-se cada vez mais difícil minerar esta moeda virtual, por isso, qualquer esquema online que prometa um retorno fixo e elevado proveniente da mineração de bitcoins, é 100% de certeza uma fraude. Existem várias fraudes com o golpe de bitcoin (exemplo, PayMony).

Assim, por exemplo, não são muitas as opções sérias, confiáveis, onde se possa investir com segurança na mineração na nuvem. O mercado está complicado e, para baralhar ainda mais as coisas, aparecem e desaparecem esquemas fraudulentos que mais não fazem do que roubar os menos prevenidos.

- http://www.coinbrasil.net.br/2015/07/cuidados-ter-com-mineracao-na-nuvem.html.

Desde o início a Paymony sempre foi uma fraude. Não começou ontem ou anteontem a ser uma fraude multinível. Este esquema fraudulento foi criado com a intenção de enganar milhares de pessoas sem conhecimentos sobre moedas virtuais, com a ilusão de Marketing Multinível e que iria durar muitos anos. Os seus criadores e os principais promotores ficaram

milionários com toda esta mentira; mas milhares de pessoas perderam dinheiro. A fraude de Marcus França continua com o nome de PowerMony.

O final de 2014 foi traumático para os investidores de Minerações em Nuvem. Vários sites simplesmente fecharam e deixaram investidores na mão. Parece que o pior deles foi a Hashie.co, que além de enganar vários investidores, ainda faz "gozação" com o drama dos mesmos, colocando uma música no site e debochando nos fóruns.

Existem na Internet sites com programas chamados HYIP - *High-Yield Investment Program* (Programa de Investimento de Alto Rendimento), são sites abertos da noite para o dia e que pode durar cerca de 3 meses. Prometem lucros fáceis e altos! No início pagam pontualmente, mas chega um dia em que desaparecem sem deixar vestígios! O HYIP não é muito diferente da pirâmide financeira, falsamente chamada de “Marketing Multi Nível“.

Por exemplo, Onecoin ou “One Coin” é um esquema Ponzi (pirâmide), versão 2.0 do Bigcoin. Não existe nenhuma moeda chamada Onecoin circulando no mercado. Os golpistas desse esquema estabeleceram uma empresa fantasma em Gibraltar, um paraíso fiscal, para fugir de impostos e ocultar o dinheiro arrecadado. Uma vez investido seu dinheiro nesse esquema, nunca mais o terá de volta. No Onecoin não há produtos no varejo para vender. Quem entra apenas é instruído a recrutar novas pessoas para pagar para entrar, e assim, serem remunerados de forma piramidal. O endereço principal da empresa, que fica em Gibraltar, trata-se de uma caixa postal. Na Bulgária há outra empresa do grupo, que faz supostas obras de caridade e ação social. A fundação humanitária do grupo, chamada de One World Fundation existe apenas de fachada e para efeitos de propaganda.

- http://zh.clicrbs.com.br/rs/noticias/noticia/2015/08/luiz-antonio-araujo-criptomoeda-megafraude-4817689.html.

Outro exemplo, é o Mercado Bitcoin Serviços Digitais Ltda, CNPJ 18.213.434/0001-35, que sofre acusação de pirâmide na 39ª Vara Cível de São Paulo - SP (Processo n.º 1047962-71.2015.8.26.0100); podendo ser consultado pelo site do Tribunal de Justiça de São Paulo (https://esaj.tjsp.jus.br/cpopg/open.do).

CUIDADOS EM COMPRAS E PAGAMENTOS PELA INTERNET

Tal como o mundo real, natural ou físico, a Internet não é um lugar seguro, mas torna-se mais perigosa para quem é ingênuo, leigo, desprevenido, desprotegido e descuidado com a segurança.

Este capítulo objetiva dar noções gerais de segurança virtual e dos golpes mais comuns na Internet. Questões estas que são aproveitadas na utilização das moedas criptográficas.

O básico ou mínimo em segurança na Internet envolve **manter o dispositivo** (computador, notebook, tablet, smartphone, etc.) protegido **com o sistema operacional, *drivers* e os *softwares*** (programas) de segurança (antivírus, antispyware, antispam e firewall) **atualizados**.

Outra regra de ouro em informática, é que o usuário não deve **nunca presumir que entende tudo**, mas sim sempre deve pesquisar ou estudar o assunto (no mínimo ler os manuais ou tutoriais) ou consultar quem entende de fato.

É extremamente necessário ter uma boa **senha** (*password*), a qual deve ser composta por letras maiúsculas, minúsculas, números e caracteres especiais (exemplos: #$%&@;₢º!?), de forma que não constitua uma palavra comum e não esteja associada a algo que terceiro possa adivinhar, como, por exemplo, data de nascimento ou outro evento pessoal relevante, nome de algum parente ou animal de estimação, número de telefone ou celular, apelido, número da residência, etc. Também deve-se evitar combinações infantis como "Qwerty" ou "123456". Outro detalhe é evitar de usar a mesma e idêntica senha para tudo. Se a pessoa tem dificuldade de memorizar diversas senhas, deve-se, então, adaptar uma parte base (recomenda-se 4 caracteres) igual que possa incorporar (acrescentar) uma parte (sugere-se de 2 caracteres) consistente numa sigla ou código (no começo, no meio, no final ou misturando-se) que identifique sua finalidade ou local de uso (por óbvio, que esse código do local de uso não pode ser facilmente compreendido por terceiros) e outro eventual acréscimo coringa (de, pelo menos, 2 caracteres especiais) para completar senhas que

necessitem de mais caracteres e em razão de muitos locais de senhas curtas não aceitarem caracteres especiais. Desse modo, o fracionamento da senha em pequenas partes montáveis, facilita o uso em locais onde a senha só pode possuir 4 (quatro), 6 (seis) e/ou 8 (oito) dígitos. Recomenda-se, ainda, trocar a senha com certa frequência ou de acordo com algum cronograma ou método (por exemplo, pode-se inventar uma fórmula matemática ou criptográfica que use dados fixos ou imutáveis [identificação civil ou profissional, algum nome, título de eleitor, serial do equipamento, nº de MAC ou IMEI, IP do servidor de Internet...] e mais dados que constantemente se alteram [mês, ano, estação, termo, grau, político no poder, emprego, cidade, versão de *software* ou *hardware*...]. E, o obvio, a senha é algo pessoal; ou seja, não pode ser divulgada ou ficar à mostra. O grande problema de utilizar programas geradores de senhas, é que a pessoa raramente vai conseguir memorizá-las, mas quando a senha foi criada pela própria pessoa com certa dificuldade (raciocínio) e/ou envolve alguma carga emocional em algum termo utilizado, mais fácil será de ser lembrada.

Sempre que houver a opção de fazer login através de certificado digital, esta será a melhor opção; pois o *cracker* mesmo que, porventura, descubra a senha, de nada adiantará sem o certificado digital.

Outra medida de segurança é **colar uma fita isolante na câmera e no microfone** do dispositivo quando estes não estiverem sendo usados; vez que *crackers* podem ativá-los de forma remota e sem acender qualquer led (luz) indicativo de estarem ligados.

Deve-se **evitar o uso de computadores públicos** (como os de *lan houses* ou *cybercafés*) ou compartilhados (que sejam utilizados por várias pessoas) para operações bancárias ou para fazer compras *online*.

Antes de realizar uma compra, operação bancária *on line*, fornecer qualquer dado, clicar em algum link ou efetuar um download, deve **certificar-se de estar no local ou destino (site, sistema, servidor, rede privada, etc.) correto** (e não em uma imitação criada para furtar dados ou valores). Desse modo, deve-se conferir a barra de endereços do navegador (*browser*) e verificar, atentamente, todos os caracteres do endereço; vez que apenas um caractere a mais, a menos ou diferente pode passar desapercebido

e é o suficiente para ser o site errado. Além disso, deve-se conferir todos os elementos gráficos (*layout*) do site para ver se estão em ordem e sem nenhuma falha de apresentação ou funcionamento. Outro truque simples para confirmar se o destinatário não é falso é, na primeira tentativa, digitar errado os dados de *login* (usuário e senha) ou de identificação; pois se não aparecer a mensagem de que os dados informados estão errados ou não conferem, o destinatário, muito provavelmente, é falso (excepcionalmente pode ocorrer uma falha no destinatário verdadeiro e dar uma falsa mensagem de erro). Outra ressalva é a de que o golpista (seja pessoalmente ou através de um *software* ou algoritmo especialmente programado para esse fim) pode estar intermediando a comunicação com o destinatário verdadeiro; ou seja, à medida que o golpista recebe os dados sigilosos da vítima, ela já testa tais dados para ter o acesso imediato e, desse modo, o golpista ao receber a mensagem de erro no destinatário verdadeiro, ela repassar a mesma à vítima na tentativa de receber os dados corretos. E, ainda, há a possibilidade do golpista estar apenas observando e coletando os dados sigilosos para posterior uso.

O ZULU Web URL Checker (http://zulu.zscaler.com/) avalia se um site é seguro e se os links recebidos são seguros ou não. O site https://quttera.com/ também verifica URLs de graça.

Outra orientação básica é **certificar-se de que o site é seguro**; ou seja, o endereço deve começar com "https://" e, na parte inferior da tela, deve aparecer o desenho de um cadeado fechado. Ao clicar no cadeado, poderá conferir se a informação do certificado corresponde ao do endereço constante na barra do navegador (*browser*).

Sites seguros geralmente utilizam um protocolo de segurança identificado pelas letras "https" (*HyperText Transfer Protocol Secure* = Protocolo de Transferência de Hipertexto Seguro), que aparece no início do “endereço” ou URL (*Uniform Resource Locator* = Localizador-Padrão de Recursos) do site. Esta é uma implementação que adiciona uma camada de segurança através do protocolo SSL/TLS (*Transport Layer Security* = Segurança da Camada de Transporte e, o seu antecessor, *Secure Sockets Layer* = Protocolo de Camada de Sockets Segura) que verifica as autenticidades dos computadores servidor e cliente por meio de certificados digitais e que

criptografa os dados transmitidos pela Internet (WWW - *World Wide Web* = rede/teia de alcance mundial ou rede mundial de computadores através do protocolo TCP/IP [*Transmission Control Protocol - Internet Protocol* = Protocolo de Controle de Transmissão - Protocolo de Interconexão]).

Os **certificados para servidores Web ou simplesmente Certificados SSL/TLS**, são os que identificam os websites e garantem a autenticidade, privacidade e a integridade dos dados de um portal na rede, proporcionando aos visitantes a garantia de que estão realmente acessando um site original e seguro, e não a uma cópia operada por fraudadores.

Pelo protocolo SSL/TLS o servidor do site que está sendo acessado envia uma chave pública ao *browser* (navegador), usada por este para enviar uma chamada secreta, criada aleatoriamente. Uma chave criptográfica é um valor secreto que modifica um algoritmo de encriptação. Exemplificando, a fechadura mecânica (exemplo, da porta de uma casa) tem uma série de pinos (engrenagens). Cada um desses pinos possui múltiplas posições possíveis. Quando alguém põe a chave certa na fechadura, cada um dos pinos é movido para uma posição específica, tal como o segredo giratório de um cofre. Se as posições ditadas pela chave são as que a fechadura precisa para ser aberta, ela abre, caso contrário, não.

Por outras palavras, geralmente, os sites iniciam suas URLs (endereços) com "http" sem o "s". Desse modo, nas páginas de pagamentos, onde é necessário ter segurança, o "s" (de segurança) aparece ao lado do "http" da URL. Assim na página da Internet onde o consumidor digita os dados do cartão de crédito ou outras informações pessoais, aparece um "s" após o "http" no endereço da Web dessa página. Isso indica que a página possui criptografia (medida de segurança que codifica [senha, linguagem secreta] os dados trafegados na Internet).

Para mostrar que a página é segura, a maioria dos navegadores (*browsers*), exibe o desenho de um **“cadeadinho” fechado** (ou um escudo) ao lado do endereço ou no canto inferior direito da janela. Esse é o **Certificado (Digital) SSL/TLS**. Mesmo se o navegador não mostrar esse desenho (cadeado), mas constar "https", presume-se que o site é seguro.

Quando a barra do navegador (Internet Explorer, Firefox, Google Chrome, Opera, KDE, etc.) muda para a cor verde quer dizer que o site visitado tem um Certificado Digital de Validação Avançada (SSL-EV - *Secure Socket Layer* - *Extended Validation* = Protocolo de Camada de Sockets Segura com Validação Estendida) e passou por uma validação de dados muito mais exigente e criteriosa (definidas pelo CA/Browser Fórum) através de autoridades certificadoras como a Certisign, Geotrust, VeriSign, Comodo, etc. Já se ficar vermelho, alerta a existência de algum problema de identidade ou risco de segurança.

Também deve-se ter cuidado com os **links patrocinados (pagos)**, como, por exemplos, do FaceBook e do Google (resultados destacados nas pesquisas/buscas ou no painel direito); bem como com as **propagandas ou anúncios**. Explica-se. Há registros de fraudadores que pagaram pelo serviço publicitário para destacarem suas páginas falsas ou páginas de distribuição de *software* malicioso (*malware*) em um local de credibilidade e com grande quantidade de visitações ou usuários. Uma opção de verificação, é utilizar sites de busca alternativos para conferir o endereço do site, como Dogpile (http://www.dogpile.com/) e Clusty (http://clusty.com/).

Ressalta-se que é comum o recebimento de **mensagens falsas (*spam* ou *phishings*)** que chegam nos e-mails, chats (*softwares* de comunicação instantânea ou salas de bate-papo) e mensagens SMS, objetivando que a vítima clique em algum link, faça algum *download*, abra algum arquivo, entre em algum site ou contate algum número telefônico, que resultará na infecção do dispositivo ou no induzimento em erro e, em ambas as hipóteses, finalizará com a vítima sofrendo algum dano.

Portanto, sites, links, programas e arquivos sugeridos em **mensagens não solicitadas (*spans*)** são perigosos, pois ao clicar em tais itens normalmente estar-se-á abrindo uma caixa de Pandora; ou seja, caindo numa armadilha que ou levará a vítima para sites falsos que tem como objetivo coletar seus dados financeiros ou instalará em seu dispositivo *malwares* (*softwares* de más intenções).

É muito comum encontrar erros grosseiros de português nas mensagens ou sites falsos; além de se notar uma formatação estranha no texto (geralmente

em formato HTML) e, até mesmo, alguns bugs (falhas) no *layout*. Esse é um sinal de, provavelmente, tratar-se de fraude, pois empresas, instituições e profissionais sérios tomam cuidado com os textos, formatação e apresentação.

O pedido para reenviar (encaminhar ou enviar a todos) a mensagem para todos ou o maior número de pessoas possível, deve ser visto com muita desconfiança.

São exemplos disso, as mensagens, mesmo de pessoas conhecidas (pois o conhecido pode ingenuamente reencaminhar a mensagem recebida ou, até mesmo, o vírus pode sozinho fazer isso no nome do conhecido), com descrição que aguçam a curiosidade, o interesse ou uma reação mecânica por confiança, amor, raiva, sentimentalismo, etc. Desse modo, mensagens com a descrição ou assunto, tais como, por exemplos: “Atualização cadastral”, "Você está sendo traído", "Seu nome está na lista de devedores do Serasa (ou do SPC)", "Fotos picantes" ou “Recadastramento necessário”, costumam ser a porta de entrada para programas espiões que furtam os dados do usuário e dão origem às fraudes. Na dúvida, nem se deve abrir o e-mail (muitas vezes o simples ato de abrir o e-mail já carrega o *malware*), mas sim deletá-lo de imediato.

Se a pessoa recebe uma mensagem estranha, diferente, polêmica, chamativa, inesperada, imprevista, incomum ou suspeita de alguma loja conhecida, famosa ou renomada, bem como de seu banco, de algum órgão público ou de algum conhecido, ao invés de abrir referida mensagem, deve-se contatar o suposto remetente da mensagem para confirmar a mesma. Assim, por exemplo, se alguma loja virtual supostamente enviou uma mensagem sobre grande saldão fora de época, basta acessar diretamente a referida loja virtual e conferir se há alguma coisa nesse sentido no site. Quanto aos demais casos, sem abrir a mensagem suspeita, pode-se contatar diretamente o pseudo remetente para saber se ele enviou dita mensagem.

Ressalta-se que, por padrão, nenhuma empresa, entidade ou órgão público envia mensagens sem a prévia solicitação ou permissão.

No mínimo, antes de abrir algum link anexo ou arquivo ou de instalar qualquer programa, **verifique com o antivírus**. E, detalhe, nunca se deve confiar na opinião de um único antivírus, mas consultar, pelo menos, três antivírus diferentes. Existem muitas opções de **verificação *on line* gratuita**.

- http://virscan.org/;
- https://www.metadefender.com/#!/scan-file;
- https://www.virustotal.com/pt/;
- http://housecall.trendmicro.com/br/;
- http://www.windowsecurity.com/trojanscan/;
- http://virusscan.jotti.org/;
- http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym;
- https://www.arcabit.pl/skaner-online.html;
- http://www.bitdefender.com/scanner/online/free.html;
- https://www.f-secure.com/en/web/home_global/online-scanner?icid=1583;
- https://www.f-secure.com/en/web/labs_global/tools-beta;
- http://free.kaspersky.com/br;
- http://online.us.drweb.com/;
- http://www.eset.com.br/online-scanner;
- http://scan.netqin.com/en/;
- http://www.mysecuritycenter.com/be/online-scan;
- https://www.microsoft.com/security/scanner/pt-br/;
- https://support.norton.com/sp/pt/br/threat-removal-solutions/current/info;
- https://home.mcafee.com/downloads/free-virus-scan?culture=pt-br;
- http://www.bullguard.com/pt-br/bullguard-security-center/pc-security/computer-threats/online_virus_scan.aspx;
- http://www.quickheal.co.in/free-online-antivirus-scan;
- https://antivirus.comodo.com/antivirus-for-windows-10/;

- http://activescan.com.ar/;
- http://seguranca.uol.com.br/antivirus/antivirus-online-gratis.html#rmcl.

Existem **listas negras** (*blacklists* - relação de sites e lojas não recomendadas) para servirem de alerta:

- http://sistemas.procon.sp.gov.br/evitesite/list/evitesites.php;
- http://www.buscape.com.br/nao_recomendadas.asp;
- http://www.ebit.com.br/convenio_lojas/html/lojas_irregulares.asp;
- http://www.pokersites.com/pt/lista-negra;
- https://sites.google.com/site/jogosdinheirointernet/Home/lista-negra---sites-scams;
- http://www.supplierblacklist.com/blacklisted-suppliers/;
- http://russian-dating-scams.com/black_lists/black_lists.htm;
- https://sitecheck.sucuri.net/;
- http://www.bannedcheck.com/;
- http://www.badbitcoin.org/thebadlist/#BTC.

Navegadores (como o Google Chrome), servidores de e-mail (como o Gmail) e sites de pesquisas (como o Google), costumam possuir uma lista negra (*blacklist*) própria de sites enganosos para proteger seus usuários, mas essa lista não é perfeita ou suficiente.

Além das listas negras, existem os **sites com registros de reclamações**.

- http://www.reputacao.com.br;
- http://www.reclameaqui.com.br/;
- http://www.denuncio.com.br/;
- https://www.reclamao.com/;
- https://www.empresaavaliada.com/;

- https://www.proteste.org.br/reclame;
- http://www.procon.sp.gov.br/reclamacoes.asp;
- http://sindecnacional.mj.gov.br/SindecNacional/;
- http://www.portaldoconsumidor.gov.br/ondereclamar.asp;
- https://defesa.oglobo.com.br/home.

Detalhe, não se pode confiar nos depoimentos de supostos clientes satisfeitos feitos no próprio site investigado e "recomendações" feitas em outros sites suspeitos, feitas por pessoas desconhecidas ou sem identificação, pois podem ter sido feitos pelo próprio pessoal do site investigado.

Além disso, na Internet existem vários **catálogos de fraudes identificadas**. Assim, por exemplo, no site (https://www.rnp.br/) da RNP - Rede Nacional de Ensino e Pesquisa, existe uma relação de fraudes identificadas pelo CAIS - Centro de Atendimento a Incidentes de Segurança (https://memoria.rnp.br/cais/).

- https://www.rnp.br/servicos/seguranca/catalogo-fraudes;
- http://www.fraudes.org/;
- http://www.tjsp.jus.br/Handlers/FileFetch.ashx?id_arquivo=48764.

Inclusive, pode ser consultado a relação de empresas do CEIS - Cadastro Nacional de Empresas Inidôneas e Suspensas (http://dados.gov.br/dataset/cadastro-nacional-de-empresas-inidoneas-e-suspensas).

Outra atitude recomenda é confirmar a **idoneidade do endereço eletrônico** (URL, site, IP, etc.). E, uma das formas, de descobrir isso é através do site do http://registro.br/. Nele você encontra o formulário de pesquisa e informa a URL (link ou endereço) e após aparecer algumas informações iniciais, clique em “Whois”. Será pedido para você digitar alguns caracteres e após isso você deve clicar em pesquisar. Na próxima tela aparecem dados como nome, e-mail, endereço e CNPJ ou CPF.

O *ENI - Employer Identification Number* (número de identificação do empregador), também conhecido por *Federal Tax Identification Number* (Número de Identificação Fiscal Federal), é o equivalente norte-americano ao CNPJ brasileiro. De modo semelhante, esse número é fornecido pelo equivalente da Receita Federal; ou seja, a *IRS - Internal Revenue Service* (https://www.irs.gov/). *TINs - Tax ID Numbers* (números de identificação fiscal) nos Estados Unidos pode assumir a forma de números de segurança social (*SSNs - Social Security Numbers*), números de identificação fiscal individual (*ITINs - Individual Tax Identification Numbers*), ou números de identificação do empregador (*EINs - Employer Identification Numbers*) e estes números são emitidos pela Administração de Segurança Social (*SSA - Social Security Administration*: https://www.ssa.gov/) ou pelo *IRS - Internal Revenue Service* (https://www.irs.gov/). Portanto, existem diferentes tipos de TINs: *SSN - Social Security Number* (números de seguro social); *EIN - Employer Identification Number* (número de identificação do empregador); *ITIN - Individual Taxpayer Identification Number* (número de identificação individual de contribuinte); *ATINs - Taxpayer Identification Numbers for Pending U.S. Adoptions* (números de identificação de contribuinte para pendentes de adoções norte-americanos); e, *PTIN - Preparer Taxpayer Identification Number* (números preparador de identificação de contribuinte). O site https://www.fraudpredator.com/ presta o serviço de ajudar a conferir a idoneidade de empresas norte-americanas.

Whois ("Quem é") é um protocolo UDP específico para consultar informações sobre domínios (dados dos endereços registrados), de contato e de DNS sobre entidades na Internet. Uma entidade na Internet pode ser um nome de domínio, um endereço IP ou um AS (Sistema Autônomo). O protocolo *Whois* apresenta três tipos de contatos para uma entidade: Contato Administrativo (*Admin Contact*), Contato Técnico (*Technical Contact*) e Contato de Cobrança (*Registrant Contact*). Estes contatos são informações de responsabilidade do provedor de Internet, que as nomeia de acordo com as políticas internas de sua rede.

- http://www.icann.org.br/;
- http://www.icann.org/en/registrars/wdrp.htm;
- http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm.

Há vários outros sites em que se consegue **pesquisa de "Whois"**:

- https://registro.br/cgi-bin/whois/;
- http://www.nomer.com.br/whois/;
- http://www.whois.net/;
- https://registro.br/cgi-bin/whois/;
- http://www.ip-adress.com/whois/;
- http://www.technolojik.net/, http://vogamu.com/;
- http://whois.domaintools.com/;
- http://www.100br.com/whois.completo.php;
- http://www.projecthoneypot.org;
- http://cqcounter.com/whois/;
- http://www.purewhois.com/index.php;
- http://whois.brasilserv.com/;
- http://www.whois.com/;
- http://www.whois-search.com/;
- http://www.domaintools.com/;
- http://www.nomer.com.br/whois/;
- http://network-tools.com/;
- http://whois.igempresas.com/;
- http://whois.bw.org/;
- http://centralops.net/co/;
- http://www.mywhois.us/;
- http://whois.e-dns.org/;
- http://dawhois.com/;

- http://dnstree.com/;
- http://network-tools.com/;
- http://urlpulso.com.br/;
- http://whois.webrankstats.com/.

Pesquise no Google a palavra “Whois” e descubra outros sites de pesquisa de “Whois”.

Também há a opção de descobrir o ***Whois* de IP**:

- http://www.ipgp.net/;
- http://www.ip-address.org/tracer/ip-whois.php;
- http://tools.whois.net/whoisbyip/;
- http://www.ipenquiry.com/Whois.aspx.

Também há *softwares* de Whois (http://technet.microsoft.com/en-us/sysinternals/bb897435).

Caso o endereço seja internacional como “.com” ou “.net” use o http://www.whois.sc ou http://registrar.verisign-grs.com/whois/ para ver os dados de quem registrou o domínio.

Outra opção para pesquisar o *whois* do site, é simplesmente digitar num site de pesquisas (exemplo, https://www.google.com.br/): “Whois” AND “*endereço do site*”.

Detalhe, deve-se pesquisar o *Whois* em mais de um site, pois o resultado é diferente de site para site; ou seja, em alguns as informações são muito resumidas e em outros são bem mais detalhadas.

Outro recurso interessante é o site https://www.changedetection.com/, que fornece serviço de monitoramento e notificação de alteração de páginas na Internet para usuários em todo o mundo.

Algo comum dos **golpistas** é não darem nenhum nome, endereço, CNPJ, CPF ou telefone de contato; ou seja, eles costumam **não fornecer dados de identificação, localização e contato**. E, quando fornecem tais dados, se não são falsos ou de terceiros, são incompletos, como, por exemplo, somente o endereço do site, e-mail ou telefone (se for somente celular, mais evidente tratar-se de golpe). Portanto, quanto menos dados a pessoa fornece, mais suspeito é e maior será o risco de golpe. Desse medo, a regra é desconfiar da falta de informações e de identificação, pois em caso de insatisfação ou fraude de quem vai se reclamar?

Diante disso, deve-se **sempre pedir maiores informações**, tirar todas as dúvidas e procurar saber o maior número de detalhes sobre o produto ou serviço (características, prazos, qualidade, garantia, etc.) e depois confirmar as informações pela Internet. E durante esses questionamentos, avaliar o atendimento, a atenção, a educação, a consistência das informações, etc.

Busque sempre informações prévias sobre manuais do usuário ou tutoriais, prazo para entrega da mercadoria ou execução do serviço e os procedimentos para privacidade, sigilo, segurança, reclamações, devoluções, trocas, desistências, garantias, seguros, assistência técnica, suporte, despesas extras, itens inclusos no pagamento, etc.

A falta de informações de identificação e localização, desperta suspeitas. Se só existem comentários excelentes, é algo surreal ou bom demais para ser verdade. Se todos os comentários são aparentemente feitos por adolescentes, merece a mesma cautela quanto a declarações de pessoas embriagadas ou dopadas. Comentários anônimos também geram desconfiança. Do mesmo modo que o papel aceita tudo (até excremento), a Internet pode ser uma mina de ouro ou uma fossa séptica dependendo de onde o internauta está entrando.

Portanto, **há de se confirmar todos os dados** de identificação, localização e contato fornecidos no site e, caso não conste no site, deve-se perguntá-los. Existem várias listas telefônicas *on line* para conferência e, inclusive, mapas para visualizar o que consta em dito endereço. Ainda mais, em relação aos telefones (e até mesmo os e-mails) deve-se contatá-los para confirmação e, como desculpa, perguntar se eles têm algum produto a pronta entrega e perguntar o endereço físico deles como se fosse comprar ou retirar

o produto pessoalmente no estabelecimento. Deve-se, ainda, pedir os dados bancários da loja virtual para realizar depósito bancário (como se não tivesse conta bancária e nem cartão de crédito para poder pagar *on line*) e, depois, perguntar no banco quem é o titular de tal conta ou, num caixa eletrônico simular um depósito só para ver no terminal quem é o titular da conta.

Por outras palavras, antes de contratar ou efetuar um pagamento on line, deve-se fazer de conta que sofreu um golpe do mesmo e está querendo saber quem é o golpista, como contatá-lo e onde localizá-lo.

Desse modo, deve-se arquivar todos os dados desde o primeiro contato ou acesso ao site (dados do site, anúncio, descrição do produto ou serviço, números de protocolos e de pedido, compra, confirmações de pedido e pagamento, todos os e-mails e mensagens trocadas, etc.) até o final da transação.

Outro ponto importante. **Não se deve fornecer informações pessoais desnecessárias** para realização de alguma compra virtual. Assim, por exemplo, para pagar *on line* com o cartão de crédito, não há nenhuma razão para informar a data de nascimento ou o nome da mãe. Por outras palavras, não há qualquer tipo de confirmação ou verificação de dados extras num pagamento on line. Pode ocorrer de a empresa vendedora ou prestadora de serviço exigir um cadastro prévio do cliente, mas o pagamento on line em si não exige nenhuma informação estranha ou incomum.

Em síntese, a regra na Internet é **desconfiar sempre**!

A regra é desconfiar de tudo e de todos. Todo site, empresa, produto, serviço ou pessoa nova, exige maior cautela. São comuns sites que, do mesmo jeito que surgem do nada com conteúdo atrativo, também do nada saem do ar, sem deixar rastros, mas somente um monte de vítimas que não sabem a quem culpar. Em alguns casos, tais sites fraudulentos duram apenas 24 (vinte e quatro) horas no ar; tempo mais do que suficiente para fazer milhões de vítimas. Portanto, a recomendação é esperar, no mínimo, alguns meses de existência e/ou uma quantidade considerável de clientes para poder avaliar com mais segurança.

Em suma, evite ao máximo sites desconhecidos, principalmente se for para efetuar *downloads* ou realizar pagamentos. Sites que possuem apenas celulares, e-mails ou só o próprio site como meio de contato, não merecem confiança para realizar contratos ou pagamentos.

Infra algumas recomendações básicas de cautela, precaução ou prevenção sobre fraudes pela Internet são as seguintes:

- Sempre desconfiar de quem apresente, sem lhe ser solicitado, alguma oportunidade de ganhar muito dinheiro rapidamente. É de se estranhar que um completo estranho, um total desconhecido ou, no máximo, um conhecido casual, do nada, querer e se empenhar em ajudar alguém a ficar rico e rápido. É muita bondade para ser verdade. Por outras palavras, o negócio parece bom demais para ser verdade;

- O "vendedor" alegar que a informação ou proposta está sendo *stealth* (furtiva, sigilosa) ou in off (não está aberta ao público). Isso é apenas uma desculpa para o fato da pessoa não conseguir encontrar nenhuma confirmação do que lhe está sendo dito;

- O fato de informações básicas (exemplos: endereço, telefone, etc.) não estarem disponíveis ou não serem fornecidas, é um sinal de alerta;

- Uma empresa estar localizada no exterior sempre dificulta as coisas: idioma diferente, outra legislação, distância geográfica, etc.;

- A empresa falar que é altruísta ou se dedicada a uma causa nobre, mas aufere lucros fabulosos, é, no mínimo, algo contraditório;

- Uma característica básica de golpes é prometer uma taxa maior de retorno para quem investir mais dinheiro. A ideia por trás

de "níveis de compromisso" é extrair logo o máximo de dinheiro possível da vítima, antes de "desaparecerem" com o dinheiro das vítimas;

- Somente os vendedores precisam planos de remuneração ou de compensação com várias quotas de "produção" e pagamentos de comissões. Os investidores não vendem; portanto, não são vendedores. O enfoque é "fisgar" a vítima e fazer com que ela traga mais outras "vítimas". Por outras palavras, a ênfase está em recrutar mais "investidores". Se a pessoa que apresenta a tal oportunidade de ouro ou "negócio da China" pressiona o cliente para aprender o negócio e "compartilhar" (divulgar, anunciar ou passar adiante) a oportunidade para outros, normalmente trata-se de um golpe. Se existe alta recompensa de recrutamento, normalmente é um golpe;

- Se o único produto ou serviço que a empresa efetivamente vende ou fornece é o treinamento para recrutar mais pessoas, trata-se de uma pirâmide financeira.

Na Internet, também vale a lei do **"barato sai caro"**. Produtos ou serviços com preço muito abaixo do mercado, promessas de ganhos astronômicos, ofertas espetaculares, promoções imperdíveis, condições de pagamento muito maleáveis... exigem muita desconfiança e cautela. Em sites de leilões, em que o vendedor é uma pessoa física, a atenção precisa ser redobrada; pois na maioria das vezes, o produto é enviado pelos Correios e o pagamento é feito antecipadamente, por depósito bancário.

Em relação à **forma de pagamento**, uma opção de segurança seria optar pelo pagamento no ato da entrega pelos Correios (remessa a cobrar), mas isso não impede de a vítima pagar para receber algo diferente do esperado.

O cartão de crédito é um meio bastante seguro para realizar compras *on line*, pois possibilita ao titular acionar a operadora (contestar o débito tal como uma sustação de cheque) e cancelar o pagamento em caso e fraude ou desavença comercial.

Chargeback é o nome dado ao processo de cancelamento do crédito do lojista de uma venda em que o comprador não reconhece a compra.

O cartão de crédito e/ou débito é muito utilizado em compras na web. Mas, por ser fácil de usar e precisar apenas de alguns números, os cartões de crédito são muito visados pelos cibercriminosos. Pessoas mal-intencionadas tentam interceptar compras em sites não seguros apenas para colherem dados pessoais e o número do cartão. Em outras palavras, não é necessário ter o cartão em mãos para fazer uma compra: basta saber o nome do titular, o número do cartão, a data de vencimento/validade e o código CVV ou de segurança (3 números no verso do cartão).

Como medida extra de segurança, quando o consumidor vai informar dados bancários na Internet, ele sai do site da loja (*e-commerce*) e é remetido para o site da instituição financeira. Esse procedimento é denominado ***gateway*** (ponte de ligação) de pagamento. Exemplificando, o *gateway* de pagamento funciona da mesma forma que uma máquina de cartão de crédito numa loja física. Ela está na loja, onde o consumidor passa o cartão e as informações vão para a operadora de cartões de crédito pela linha telefônica. Se tudo estiver correto, a operadora aprovará a compra, avisando instantaneamente o comerciante, e o produto ou serviço será liberado para o cliente. Em síntese, é um canal de dados entre a máquina ou sistema e a operadora de cartão de crédito.

Gateway de pagamento é, portanto, uma aplicação (que protege as informações bancárias ou de cartões de crédito ou débito, bem como outros dados sensíveis por meio de criptografia) para *e-commerce* instalada em um servidor remoto mantida por uma operadora financeira que autoriza pagamentos de transações feitas online. É um padrão internacional estabelecido pela **Indústria de Cartões de Pagamento (PCI - *Payment Card Industry*)**, cuja função é proteger os dados de transações com cartões.

Os *gateways* de pagamento podem ser implementados de duas maneiras. No primeiro caso pode levar o cliente diretamente para um site de terceiros para processamento do cartão de crédito. No segundo, o pagamento pode ser processado através do chamado *Merchant API* (*Application Program Interface* ou Interface de Programação de Aplicativos) que é integrado com

o servidor que hospeda o site da loja. Em ambos os casos, o consumidor não estará mais no sistema/ambiente da loja, mas da instituição financeira.

Os *gateways*, em resumo, atuam como um conector (como, por exemplo, uma ligação telefônica protegida contra grampo ou interceptação) da loja virtual com as instituições financeiras (bancos e operadoras de cartões de crédito), tal como o aparelho leitor de cartões faz. O ambiente é composto basicamente pelo *browser* do consumidor comprando online com cartão de crédito (*Cardholder*), o servidor web de uma loja virtual (*Merchant*) e o *gateway* de pagamento da instituição financeira (*Acquirer*).

Normalmente quando um cliente envia informações de seu cartão de crédito, a informação é codificada e transmitida através do *gateway* de pagamento. A interface envia as informações para o banco do cliente, confirmando se o cartão é válido e se existem fundos suficientes disponíveis ou de crédito para que se processe o pagamento, enviando a aprovação caso tudo esteja correto. Ele protege os comerciantes contra cartões roubados, falsificados ou sem fundos suficientes para realizar uma transação.

Caso o site não aceite cartão de crédito, deve-se optar pela utilização de algum intermediário no pagamento. A última hipótese com alguma segurança, é o **boleto bancário**, pois já comprova que se tratou de uma relação comercial ao contrário de simples depósitos ou transferências bancárias.

O boleto bancário (ou bloqueto de cobrança) é um documento que representa um título de crédito em cobrança, pagável através da rede bancária. Através desse método de cobrança, o banco é contratado pelo cedente para realizar a cobrança do sacado.

A Circular nº 3.598, de 06/06/2012, do Banco Central do Brasil, é a atual norma que regulamenta o boleto bancário.

- https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=circ&ano=2012&numero=3598.

O cedente (ou tomador) é quem emite a cobrança e vai receber a quantia cobrada; ou seja, é o titular da conta bancária onde o dinheiro será creditado (depositado) após o pagamento. Já o sacado é quem está sendo cobrado e

vai efetuar o pagamento do boleto (consumidor, comprador, tomador do serviço, etc.).

O boleto avulso é um documento que permite cobrar por uma compra à vista, em uma operação avulsa. Já carnê significa uma sequência de boletos, cobrando prestações de uma compra ou valores de uma assinatura; ou seja, uma cobrança recorrente.

A emissão de boleto pode ser feita por ferramentas do próprio banco ou por sistemas externos. Deve-se preferir boleto emitido por ferramentas ou dentro do ambiente da instituição financeira.

Ainda mais. Deve-se preferir a modalidade com registro (ao invés da sem registro).

O boleto simples (sem registro) é emitido por uma empresa (cedente) sem que o banco seja informado sobre quem irá pagar (sacado); nem mesmo valor e data de vencimento precisam estar identificados. O banco só ficará sabendo da existência do boleto quando (e se) ele for pago. Já no caso da cobrança registrada, a empresa que vende precisa identificar e comunicar ao banco o nome e CPF ou CNPJ do cliente (sacado), o valor e a data limite de pagamento. Ao emitir esse tipo de documento, um arquivo é criado e enviado pelo cedente (beneficiário da cobrança) para o banco.

Desde janeiro de 2017 não existe mais no Brasil o boleto sem registro (Comunicado FB - Febraban nº 15/2015). Os ainda existentes somente poderão ser recebidos pelo banco beneficiário (emissor).

O boleto possui um número de identificação para poder ser identificado no extrato bancário.

O DDA (Débito Direto Autorizado) é uma espécie de boleto eletrônico.

A fraude mais comum é a adulteração da linha digitável do boleto, depois que ele é emitido e antes de ser pago. O *layout* do boleto não pode ser no formato HTML por ser muito fácil de um vírus acessar. Deve-se preferir o boleto nos formatos de imagem ou PDF.

No começo os cibercriminosos interceptavam o boleto antes do pagamento para alterarem a numerações do código de barras; mas, recentemente, foram mais criativos e passaram a oferecer a isca do serviço de atualização de boletos vencidos, sem precisar recorrer ao banco ou ao emissor, para efetuar o pagamento. Desse modo, ao usar o falso serviço de atualização, o novo boleto emitido possui os dados alterados para que o pagamento seja efetuado na conta dos cibercriminosos. Esses fraudadores usam campanhas publicitárias, como o Google AdWord e links patrocinados dos resultados de pesquisas. Para impedir consultas públicas de seus dados, eles registram o domínio do site usando um servidor *Proxy* de registro Domains by *Proxy* (DBP), assim, as informações não ficam disponíveis.

Na dúvida da veracidade de um boleto, a pessoa deve verificar se os três primeiros números (código de compensação) da linha digitável correspondem ao código do banco emissor do documento. Se os números não baterem, o pagamento não deve ser feito, pois pode ser fraude.

Se o nome da empresa, o banco, o código de barras, a data de vencimento ou o valor cobrado não confere, deve-se entrar em contato com a empresa e checar as informações e o ocorrido.

O código de barras possui as informações de valor, vencimento e dados da conta credora (para onde o dinheiro será enviado) que são capturadas através de leitor ótico pelas máquinas. Desse modo, a linha digitável é a representação numérica do código de barras.

> "Você sabe o que significa cada campo numérico de um boleto bancário? Já pensou nisso? Tomando como padrão o sentido de leitura da esquerda para a direita, os três primeiros algarismos fazem referência ao banco. Por exemplo, o Santander é identificado pelo número 033, a Caixa é 104, o Itaú é 184 e o Bradesco é 237. Mas, vale lembrar que boletos de cartões de crédito podem ter códigos diferentes, como o Itaúcard, por exemplo, que é outra instituição.
>
> Depois, vem o quarto algarismo, que indica a moeda. No Brasil, será sempre o 9. Há outros números que são mais complexos para entender, como a data de vencimento. Isso porque o Banco Central criou uma

data-base, que é 7 de outubro de 1997. No seu boleto bancário, ao invés de vir a data de vencimento com dia, mês e ano, o que aparece é o número de dias que se passaram desde a data-base. Assim, se a sua conta vence em 10 de junho de 2015, por exemplo, no campo correspondente ao vencimento você verá os números 6455, que o número de dias que se passaram desde então.

Os últimos dígitos indicam o valor do vencimento, sem vírgulas. Por exemplo, se a conta é de R$ 297,68, no último campo você irá visualizar 29768." (http://www.vivoseudinheiro.com.br/entenda-como-funciona-o-codigo-de-barras-dos-boletos/).

"A linha digitável é a sequência de dígitos que identifica o banco, carteira de cobrança, nosso número e valor da cobrança. Os primeiros três dígitos referem-se ao código de compensação do banco emissor. O quarto indica a moeda (para cobranças em reais, o número é o 9, outras moedas: 8). A data vencimento está também definida com o cálculo de dias corridos a partir de 7 de outubro de 1997, a chamada data-base (dia fixado pelo Banco Central como marco para esse tipo de cobrança). Os últimos dígitos indicam o valor do vencimento, sem vírgulas. No total a linha digitável costuma ser uma sequência de 48 algarismos." (https://blog.contaazul.com/boleto-bancario-o-que-e-como-funciona-e-como-emitir).

- https://boletocloud.uservoice.com/knowledgebase/articles/321057-o-boleto-partes-principais.

Após a leitura ou digitação do código de barras, deve-se verificar se o beneficiado informado na tela corresponde ao fornecedor do produto ou serviço contratado.

- http://www.bcb.gov.br/Fis/CODCOMPE/Tabela.pdf;
- https://portal.febraban.org.br/pagina/3164/12/pt-br/associados;
- http://www.buscabanco.org.br/AgenciasBancos.asp.

Quando uma loja virtual utiliza um intermediário ou facilitador de pagamentos, quem recebe o pagamento do comprador é o intermediário; que

é o responsável pela aprovação da venda e pelo repasse do valor à loja virtual conforme suas regras.

- Pagseguro (https://pagseguro.uol.com.br/comprar/);
- PayU (https://www.payu.com.br/compradores);
- Bcash, atual PayU (http://bcash.com.br/compradores/);
- MOIP (https://moip.com.br/);
- MercadoPago (https://www.mercadopago.com.br/);
- F2B (http://www.f2b.com.br/);
- PayPal (https://www.paypal.com/br/webapps/mpp/home).

O Mercado Pago (https://www.mercadopago.com.br/), utilizado no site Mercado Livre (http://www.mercadolivre.com.br/), recebe o valor da compra e somente libera o mesmo ao vendedor com a autorização do comprador após este confirmar que recebeu o produto e que este está de acordo com o contratado ou anunciado pelo vendedor.

Em sites estrangeiros, deve-se conferir as taxas de importação e se o fornecedor possui representante no Brasil, o que lhe possibilitará contar com assistência técnica no país. Se a empresa não tiver representante no Brasil e a importação foi direta, fica impossível pedir um ressarcimento ou entrar com uma ação judicial no país. Quem não quer assumir riscos, deve optar pela importação através de uma importadora.

Através de **sites de cotações ou comparações de preços**, é possível ter noção rápida do preço de mercado e, muitas vezes, até conhecer as avaliações dos clientes.

- Buscapé (http://www.buscape.com.br/);
- Bondfaro (http://www.bondfaro.com.br/);
- Shopping Uol (http://shopping.uol.com.br/);
- Google Shopping Brasil (http://www.google.com.br/shopping);
- Zoom (https://www.zoom.com.br/);

- JáCotei (http://www.jacotei.com.br/);
- ComparePreços (http://www.compareprecos.com.br/);
- Shopbot (http://www.shopbot.com.br);
- Zura! (http://www.zura.com.br);
- Preço Mania (http://www.precomania.com);
- Cata Preço (http://www.catapreco.com.br);
- Baixou (http://www.baixou.com.br/).

Ainda mais, como dizem os norte-americanos "There is no free lunch" **("Não existe almoço grátis"**); ou seja, é impossível conseguir algo sem dar nada em troca. No bom português brasileiro, nada é de graça! Diante disso, ninguém se daria ao trabalho de "piratear" ou "crackear" programas e vídeos para depois fornecê-los de graça a todos na Internet. Portanto, na enorme maioria dos casos, os sites que fornecem tais tentações estão repletos de *malwares* e, inclusive, os programas com *crack* costumam possuir *trojans*.

É recomendável **pesquisar na Internet** (tanto através de sites de pesquisas comuns, como em específicos como o http://www.yasni.com.br/) pelo nome do site, serviço, empresa, etc. para verificar se existem reclamações denúncias, relatos e advertências a respeito. Mas não se pode limitar a acreditar nessas informações isoladas; pois pode tanto ser o próprio que simulou relatos favoráveis, bem como pode ser reclamações falsas feitas pela concorrência. Assim, é necessário verificar em vários sites maiores informações.

Existem vários **outros sites de pesquisas além do Google** (https://www.google.com.br/):

- Sputtr (http://www.sputtr.com/);
- 100 Search Engines (http://www.100searchengines.com/);
- Tendencia (http://tendencia.cc/);
- Web Search (http://www.websearch.com/);

- Aliweb (http://www.aliweb.com/);
- Bing (http://www.bing.com/);
- Uol busca (http://busca.uol.com.br/);
- Ponteiro (http://ponteiro.com.br/);
- Sites no Brasil (http://sitesnobrasil.com/);
- Achei (http://www.achei.com.br/);
- @onde (http://www.aonde.com.br/);
- Buscaki (http://buscaki.com.br/);
- Baidu (http://br.hao123.com/);
- Qwant (https://www.qwant.com/?l=pt_pt);
- Yahoo (https://br.yahoo.com/);
- DuckDuckGo (https://duckduckgo.com/);
- Yandex (https://www.yandex.com/);
- Dogpile (http://www.dogpile.com/);
- WolframAlpha (https://www.wolframalpha.com/);
- Ask (http://br.ask.com/);
- StartPage (https://www.startpage.com/);
- Ixquick (https://www.ixquick.eu/);
- ChaCha (http://www.chacha.com/);
- Metager (https://metager.de/);
- Yippy (http://yippy.com/);
- Internet Archive (https://archive.org/);
- Kartoo (http://www.kartoo.com/);
- Teoma (http://www.teoma.com/);
- Ecosia (https://www.ecosia.org/);

- SpeedyBit (http://home.speedbit.com/);
- O Leme (http://www.leme.pt/motores-de-busca/);
- Motor de pesquisa (http://www.motordepesquisa.com/);
- Search Iminent (http://search.iminent.com/pt-BR/search/);
- Science Research (http://scienceresearch.com/scienceresearch/);
- Creativecommons (https://search.creativecommons.org/);
- Bigbusca (http://bigbusca.com.br/br/);
- Blackle (http://br.blackle.com/).

Sempre é útil **consultar pessoas conhecidas e de confiança** se elas conhecem tal site ou se já ouviram algum relato de algum conhecido a respeito (e não que simplesmente leram na Internet sobre tal site). Portanto, uma forma de segurança é a indicação de pessoas conhecidas. Desse modo, uma das recomendações de segurança é prefira as indicações feitas por amigos e/ou parentes e/ou optar pelos sites conhecidos, tradicionais e de idoneidade reconhecida para fazer as compras ou negócios *on line*.

Outro fator de referência são os **selos de reputação**. Estes selos para serem recebidos passam por avaliação em uma série de critérios antes de ter o *status* de loja qualificada. A consultoria e-bit, por exemplo, oferece "medalhas" às lojas virtuais (ouro, prata e bronze), enquanto que sites de comparação de preços, como o Buscapé, também avaliam as lojas segundo as respostas positivas dos usuários.

O site Mercado Livre é o melhor exemplo do sistema de avaliação e reputação dos vendedores virtuais através dos *feedbacks* (comentários pós-vendas) dos compradores (http://www.mercadolivre.com/seguro_calif.html).

Além dos selos de qualidade, há os de identificação e de blindagem do site contra os ataques de *hackers*. Portanto, deve-se saber o que cada tipo de selo significa, não confundir um com outro e, ainda, confirmar se os selos são verdadeiros, clicando-se neles para ser direcionado à entidade emitente do mesmo e que o valida.

- https://empresa.ebit.com.br/certificacao-ebit.asp;
- http://www.ebit.com.br/medalhas-e-bit;
- http://www.reclameaqui.com.br/como-funciona/selo/;
- https://www.siteblindado.com/pt/produtos-e-servicos/blindagem-site-blindado/;
- https://www.certisign.com.br/seal/splashcerti.htm;
- https://www.dualstore.com.br/blog/selo-de-qualidade-loja-virtual;
- https://www.google.com/trustedstores/.

Empresas de selos de segurança realizam auditorias diárias, testando a vulnerabilidade em IPs e URLs para garantir a segurança das informações, detalhando os possíveis riscos e apresentando as formas de solucionar as falhas. Isso significa que o website está protegido contra tentativas de exploração e obtenção de informações confidenciais não autorizados através das técnicas de invasão mais conhecidas e do cumprimento das exigências do padrão de segurança PCI-DSS (*Payment Card Industry Data Security Standard* = padrão internacional de segurança para a indústria de cartões de pagamento) da indústria de cartões de crédito relativas a *scans* remotos de vulnerabilidades em servidores de Internet. Normalmente junto a tais selos constam expressões como: *secure by*, *secure site*, site seguro, site auditado, etc.

Malware, palavra resumida de "malicious software" (*software* nocivo ou *software* malicioso), é um programa de computador projetado para infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo ou de softwares. *Malware*, portanto, designa de forma genérica as ameaças que podem atacar os computadores.

Tanto os **vírus** como os ***worms*** são softwares maliciosos que se propagam enviando cópias de si mesmos de computador para computador. Enquanto que o vírus depende da atuação do usuário (vítima) consistente na execução do arquivo hospedeiro para poder se tornar ativo e continuar o

processo de infestação e propagação da epidemia, o *worm* se propagar automaticamente (não depende de nenhum ato da vítima).

Alguns exemplos de **antivírus** são: Avast (https://www.avast.com//pt-br/index), Trend Micro (http://www.trendmicro.com.br/), ThreatTrack Vipre (https://www.vipreantivirus.com/), F-Secure (https://www.f-secure.com/pt_BR/welcome), McAfee (https://home.mcafee.com/), Norton (http://www.nortonsecurityonline.com/ns-br/), Panda (http://www.pandasecurity.com/brazil/), Bitdefender (http://www.bitdefender.com.br/) e Avira (https://www.avira.com/pt-br/index).

O termo **"Internet Security"** se refere aos programas (suítes) que fornecem proteção, teoricamente, completa ou máxima aos dispositivos conectados a redes e à Internet.

- http://www.avg.com/br-pt/internet-security;
- https://www.avast.com/pt-br/internet-security;
- https://www.avast.com/pt-br/premier;
- http://www.pandasecurity.com/brazil/homeusers/solutions/internet-security/;
- https://www.f-secure.com/pt_BR/web/home_br/internet-security.

Ransomware, derivado da palavra inglesa "ransom" (resgate), é um *malware* que restringe o acesso ao sistema infectado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido. É como se fosse um sequestro, mas virtual.

Spywares são programas espiões. Eles coletam informações sobre as atividades realizadas no dispositivo (computador, notebook, tablet, celular, etc.) e transmitem essas informações a terceiros, sem o conhecimento e o consentimento do usuário (vítima).

Existem programas específicos com a função de ***antispyware***, tais como, por exemplos, Malwarebytes Anti-Malware (https://br.malwarebytes.com/), Emsisoft Anti-Malware (https://www.emsisoft.com.br/pt/), Super

AntiSpyware (http://www.superantispyware.com/), Spybot - Search & Destroy (https://www.safer-networking.org/) e Spyware Terminator (https://www.spywareterminator.com/pt-BR/).

> "Um exploit (em português explorar, significando "usar algo para sua própria vantagem") é um pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto a ocorrer no software ou hardware de um computador ou em algum eletrônico (normalmente computadorizado). Tal comportamento frequentemente inclui coisas como ganhar o controle de um sistema de computador, permitindo elevação de privilégio ou um ataque de negação de serviço." (https://pt.wikipedia.org/wiki/Exploit_(seguran%C3%A7a_de_computadores)).

- http://www.s3commerce.com.br/blog/120/os-diversos-cenarios-da-seguranca-no-e-commerce.

Malwarebytes Anti-Exploit Premium blinda navegadores e programas de software contra ataques que exploram as vulnerabilidades em seus códigos (https://br.malwarebytes.com/antiexploit/).

Adware é qualquer programa de computador que executa automaticamente e exibe uma grande quantidade de anúncios personalizados sem a permissão do usuário. Para apresentar os anúncios personalizados, o *adware* antes verifica as visitas e pesquisas feitas pelo usuário na Internet. Alguns programas para a remoção de adwares são Adwcleaner (https://toolslib.net/) e BitDefender Free Adware (http://www.bitdefender.com/solutions/adware-removal-tool-for-pc.html).

Sniffer é um *malware* usado para capturar e armazenar dados trafegados numa rede de computadores desprotegida ou sem criptografia.

Phishing (palavra inglesa que significa "pescaria") é uma forma de fraude eletrônica que visa, através de uma isca ou armadilha consistente em dados ou arquivos falsos, enganosos ou fraudulentos (link, URL, e-mail, mensagem, site, servidor, promoção, software, etc.), adquirir dados

pessoais, confidenciais e sigilosos (documentos de identidade, nomes de usuários [login], senhas, contas bancárias, cartões de créditos, etc.). Portanto, o phisher ("pescador") usa esse método para "pescar" os dados das vítimas (pessoas ingênuas, desatentas, desavisadas e/ou desinformadas) que "mordem o anzol" lançado. O spear phishing ("pesca com arpão"), é uma variante mais eficaz do phishing, que consegue identificar com quais instituições financeiras as vítimas mantêm relacionamento e, assim, realizarem uma isca personalizada. Existe, ainda, o **pharming** que é uma evolução do phishing, que não necessidade da "isca". O **keylogger** captura as teclas digitadas pelo usuário (vítima) no teclado do aparelho. O **screenlogger** é uma forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado. Os instaladores dos sites Baixaki e Superdownloads instalam outros programas além do pretendido pelo usuário. Existem ferramentas ***antiphishing*** como o MetaPhish (http://www.metacompliance.com/products/phishing-and-ransomware/) e o Unchecky (https://unchecky.com/).

Em razão disso é aconselhável, sempre que possível, ao digitar dados de *login*, utilizar teclados virtuais e, de preferência, com cliques através da tela sensível ao toque em computadores.

Nas piscinas convencionais, o ***skimmer*** (coaderia), possui a função de aspiração. Ele trabalha na superfície da piscina, deixando-a livre de impurezas como folhas, insetos, cabelos e até da própria gordura liberada pelos banhistas na água da piscina. Em informática, *skimming* é uma técnica com que os cibercriminosos copiam a tarja magnética de um cartão de crédito ou de débito para poderem cloná-lo (duplicá-lo). Desse modo, os *skimmers* utilizam diversos aparelhos para ler e copiar os dados gravados na tarja magnética dos cartões de crédito e de débito.

O ***DNS poisoning*** consiste em dominar um servidor DNS fazendo com que as requisições de acesso a um certo domínio (site, URL, IP ou endereço) sejam direcionados a um destino diferente (servidor malicioso ou *fake* [falso]), que finge ser o correto, fazendo com que o host (máquina ou computador) da vítima acredite que está realmente “conversando” com o servidor correto.

"O phishing é uma estratégia muito usada na propagação de malwares, como vírus e trojans. Ele, frequentemente, usa táticas de engenharia social para abordar as vítimas, fazendo com que suas contas de redes sociais sejam infectadas e usadas para espalhar o golpe. Seu método mais comum de espalhar softwares maliciosos é através do o envio de e-mails de spam, que direcionam o usuário para sites contaminados. Com o tempo, os golpes foram se diversificando e, até mesmo, usando eventos reais para se aproveitar da curiosidade dos internautas desprevenidos."
(http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-phishing-e-malware.html).

"Como o phishing funciona

Na maioria dos casos, os phishers (propagadores de phishing) enviam uma onda de e-mails de spam, às vezes até milhões de mensagens. Cada e-mail contém uma mensagem que parece ter sido enviada por uma empresa conhecida e confiável. Geralmente, a mensagem inclui o logotipo e o nome da empresa e, quase sempre, tenta provocar uma resposta emocional a uma falsa crise. Contendo uma linguagem comercial e urgente, o e-mail quase sempre solicita informações pessoais do usuário. Algumas vezes, o e-mail direciona o destinatário diretamente para um site falso. O website, assim como o e-mail, parece autêntico e, em alguns casos, o URL pode ter sido mascarado para sugerir que o endereço da Web pareça real.

O website falso solicita, com urgência, que o visitante forneça informações confidenciais, como números de CPF, números de contas bancárias, senhas, etc. Como o e-mail e o site correspondente parecem legítimos, o phisher espera que pelo menos uma fração dos destinatários seja convencida a enviar seus dados. Apesar de ser impossível saber a taxa real de resposta das vítimas a todos os ataques de phishing, acredita-se que uma média de um a dez por cento dos destinatários são enganados por uma campanha de phishing bem-sucedida, com uma taxa de respostas de mais ou menos cinco por cento. Para se ter uma ideia melhor, as campanhas de spam normalmente têm uma taxa de resposta de menos de um por cento." (http://br.norton.com/cybercrime-phishing).

"Os criminosos se aproveitam dos malwares e vírus que andam espalhados pela internet para poder infectar e modificar o browser (navegador de internet) do computador do usuário. Estando infectado, quando o internauta digita o endereço eletrônico de um site, o navegador redireciona a página para um site falso, mas com as mesmas características estéticas do original.

O internauta pensa que está no website correto, já que não clicou em nenhum link estranho e digitou o endereço diretamente na URL do browser, e acaba fornecendo os seus dados bancários e pessoais mais facilmente, sem desconfiar que está sofrendo um golpe." (https://www.significados.com.br/phishing/).

- https://www.oficinadanet.com.br/post/17053-malware-finge-ser-whatsapp-para-roubar-dados-de-cartao-de-credito.

Trojan, abreviatura de *Trojan horse* (cavalo de Troia), é um *malware* (programa malicioso) que entra em um dispositivo computacional, disfarçado como um programa comum e legítimo, com a finalidade de possibilitar a invasão e dominação do equipamento através da abertura de porta, tornando-o um zumbi (máquina escravizada sem autonomia, que faz tudo o que o *cracker* ordena, seja de forma automatizada e/ou por acesso remoto) ou num ***bot*** (abreviação de robot, que significa robô). Quando o *cracker* domina vários computadores, ele cria uma rede de zumbis denominada de ***botnet*** (*zombie army*). Uma *botnet* chamada Rustock chegou a controlar mais de um milhão de computadores zumbis. Os dois tipos mais comuns de *Trojans* são os Keyloggers (que normalmente são utilizados para roubar senhas) e os Backdoors (arquivos que possibilitam aberturas de portas para invasão). Os famosos programas piratas ou ativadores ilegais de programas genuínos, costumam instalar *trojans* nos computadores. ***Firewall*** ("parede de fogo") é o meio (pode ser software ou hardware) usado para controlar todos os acessos (entradas e saídas ou transmissão e recepção) e o tráfego de um dispositivo ligado em rede. Exemplos são o Zone Alarm (https://www.zonealarm.com/), Comodo Firewall (http://www.comodobr.com/firewall/comodo_firewall.php) e o NetGuard Pro (https://www.netguard.me/).

- http://canaltech.com.br/noticia/seguranca/Botnets-descubra-se-o-seu-computador-faz-parte-de-uma-e-saiba-como-se-proteger/.

Backdoor (RAT - *Remote Administration Tools*) é uma aplicação através da qual cibercriminosos entram no computador, instalam e lançam outros programas, enviam *keyloggers*, descarregam ou apagam ficheiros, ativam microfones ou a câmera dos dispositivos. O *Backdoor* permite que o *cracker* comande o computador remotamente e execute qualquer tarefa nele. *Backdoor* significa porta dos fundos. Confira, ainda *Backdoor* no glossário.

Rootkit são *malwares* que escondem a sua própria presença e a de outros *malwares* coligados (normalmente alterando as chamadas ou APIs do sistema operacional para que seus arquivos e processos não sejam mostrados) tornando impossível a sua detecção pelos mecanismos convencionais. Podem ser instalados no kernel (módulos carregáveis, device drivers) ou nas bibliotecas do Sistema Operacional (DLLs).

Downloader é um programa malicioso (*malware*) que instala outros *malwares*.

Hijacker altera a página inicial do navegador e as preferências de pesquisa.

Cybersquatting consiste em registrar um domínio na Internet com o nome de uma pessoa, empresa, entidade, organização, instituição ou marca renomada ou conceituada com o objetivo de vender esse registro ao proprietário legal do nome. Essa prática também pode ser utilizada para capturar dados confidenciais das pessoas que acessarem o domínio pensando se tratar de um site verdadeiro.

O ***scam*** (ou "golpe") é qualquer esquema ou ação enganosa e/ou fraudulenta que, normalmente, tem como finalidade obter vantagens financeiras. Já ***scammer*** é o responsável pela ação de enviar e/ou desenvolver *scams* (ou *phishing scams*). Enquanto que o *scam* objetiva informações pessoais e intimidade com a vítima através de um falso relacionamento, o *spam* normalmente anuncia uma venda, prêmio ou concurso. O *scam* se desenvolve em etapas e o *spam* normalmente envolve um único ato da vítima como um simples clique. Apesar de ser uma prática

relativamente antiga, o termo correto não é muito difundindo e, muitas vezes, acabam denominado de *spammer* quem praticante *phishing scam*.

Não confundir com *scan*, palavra inglesa que traduzida significa "examinar de perto". Em informática, *scan* significa escanear; ou seja: a) digitalizar imagens, fotos e textos impressos para o computador; b) detectar e eliminar vírus de computador; c) testar as portas de um dispositivo; d) reconhecimento ótico de caracteres ou padrões; etc.

Em geral, um *scam* pode ser um e-mail, torpedo SMS, página ou perfil falso, bem como qualquer outra forma de contato que o *scammer* possa ter com a vítima pelo meio digital solicitando informações pessoais e/ou efetuarem algum pagamento.

Scammers, portanto, são pessoas que criam perfis, contas, mensagens e/ou relatos (estórias) falsos, para obter vantagens financeiras às custas das vítimas. Explica-se. Os *scammers* inventam estórias, dossiês, relatos, acontecimentos, etc. para cativar, sensibilizar, comover, impressionar, seduzir, apaixonar, atrair... a vítima. Os exemplos mais comuns são de viúvas milionárias e caridosas, de herdeiros de grandes fortunas, de jovens deuses gregos solteiros, de heróis de guerra em procura de um amor verdadeiro, de um prêmio ou recompensa que exige o pagamento prévio de uma taxa, etc. Além do conto, utilizam-se de jogos psicológicos para fazer com que a vítima seja incentivada a continuar trocando e-mails, mandando informações, etc.

Os blogs http://meg-golpistasvirtuais.blogspot.com.br e http://forascammer.blogspot.com.br e o site http://scforum.info/ contêm dicas para identificar *scammers*, as mensagens mais comuns utilizadas pelos golpistas, fotos utilizadas em falsos perfis e relatos de vítimas do crime virtual, entre outros tópicos.

Scam baiting é a prática de fingir interesse em uma fraude *online* para manipular o golpista por trás dela. O objetivo em fisgar golpistas pode ser fazer com que percam tempo, embaraçá-los, levá-los a revelar informações que possam ser úteis às autoridades legais para que os investiguem e os

capturem, levá-los a gastar dinheiro ou simplesmente se divertir (fazerem sentir o gosto do próprio veneno).

Pelo site https://denuncia.uol.com.br/ e através dos e-mails crime.internet@dpf.gov.br, mail-abuse@cert.br, webpol@policia-civ.sp.gov.br, phishing@cais.rnp.br e artefatos@cais.rnp.br é possível relatar e denunciar as mensagens falsas disparadas por *scammers*.

Em caso de perda de dinheiro significativo, o FBI - *Federal Bureau of Investigation* ("Departamento Federal de Investigação" - https://www.fbi.gov/) investiga o crime e através do site https://www.ic3.gov/default.aspx pode-se comunicar o fato às autoridades americanas.

Por outras palavras, **antes de efetuar a compra, solicitação do serviço ou o pagamento, deve-se se preparar para o pior**; ou seja, se armar de todas as informações e provas para poder ingressar na Justiça. Depois que a vítima percebe o golpe, raramente consegue as provas do mesmo, pois os sites podem sair do ar, mudarem o teor dos anúncios, apagarem os comentários *on line*, etc.

Sempre que possível, **deve-se optar por uma empresa, loja ou site estabelecido no pais**, ou que tenha representante ou intermediário no pais para garantir a aplicação da legislação interna e de poder acionar a Polícia e o Judiciário.

O que determina a legislação aplicável e a respectiva competência policial e jurisdicional é o local onde o site está registrado, pouco importando onde se encontra o servidor (hospedagem) do mesmo.

O Código Civil (http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm) assim reza no artigo 435: "Reputar-se-á celebrado o contrato no lugar em que foi proposto". De igual modo, a LINDB - Lei de Introdução às Normas do Direito Brasileiro, antiga LICC - Lei de Introdução ao Código Civil (Decreto-lei nº 4.657/1942 - http://www.planalto.gov.br/ccivil_03/decreto-lei/Del4657.htm), prescreve no artigo 9º e § 2º:

"Art. 9º. Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituírem.
[...]
§ 2º A obrigação resultante do contrato reputa-se constituída no lugar em que residir o proponente.".

Ainda que assim não fosse, as partes contratantes podem pactuarem qual será o foro (local competente) para eventual discussão judicial (CPC/2015 - Lei nº 13.105/2015, art. 63 e 47, § 1º). De igual modo, também pode ser estabelecido em contrato que as partes dispensam o uso da via judicial convencional e adotam o juízo arbitral (Lei nº 9.307/1996, Lei nº 13.129/2015 e CPC/2015 - Lei nº 13.105/2015, arts. 42, 337 - X, 485 - VII, 515 - VII e 960, § 3º). Pode ocorrer de tais cláusulas (foro de eleição e justiça privada) serem anuladas em se tratando de consumidor (CDC, arts. 6º, inciso VII, 46, 47, 51, inciso I e VII, e 101, inciso I), mas sendo pessoa jurídica ou profissional liberal não; ou seja, em regra, o foro competente é o do domicílio do requerido (CPC/2015, art. 46), da localização do bem (CPC/2015, arts. 47 e 53, inciso III) ou do lugar do ato ou fato (CPC/2015, art. 53, inciso IV).

- Código de Processo Civil - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm;
- CDC - http://www.planalto.gov.br/ccivil_03/leis/L8078.htm.

O CDC amplia a quantidade de responsáveis para prevenir a ocorrência de algum deles ser pessoa estrangeira (CDC, artigos 3º, 12 e 13). De forma similar, mas com menor alcance, o Código Civil de 2002 (arts. 75, § 2º, 1.137 e 1.138) e o CPC/2015 ampliam a representação de pessoa jurídica estrangeira no Brasil (art. 75, inciso x e § 3º). Em ambos dispositivos, se não houver nenhuma pessoa, física ou jurídica, envolvida, representante ou intermediária no Brasil, nada se poderá fazer por aqui.

É indispensável **exigir nota fiscal**, pelo fato desta dar maior garantia de idoneidade do vendedor se precaver de o produto ser objeto de crime e possibilitar eventual reclamação ou troca.

Também é fundamental acompanhar a entrega do produto, que normalmente é feita por empresa que dispõe de "tracking" (rastreamento) da

encomenda; ou seja, o acompanhamento da entrega do produto mediante o uso de um código fornecido pelo vendedor.

Numa compra *on line* o consumidor possui até 7 (sete) dias para devolver um produto que não o tenha agradado, com direito à restituição de todo o valor pago (CDC - Código de Defesa do Consumidor, artigo 49; http://www.planalto.gov.br/ccivil_03/leis/l8078.htm). Assim, é importante imprimir, ou salvar no computador, todas as conversas, anúncios, respostas, imagens do produto, número de protocolo da compra ou do pedido, comprovantes de pagamentos, confirmação do pedido e de seu envio, etc.; enfim todos os passos desde o pedido até a entrega do produto; bem como todos os dados necessários para identificar o vendedor e sua localização física.

Recomenda-se, depois de sofrer um golpe ou algum crime pela Internet, procurar um cartório de notas para registrar uma Ata Notarial (http://www.atanotarial.org.br/ata_notarial.asp) das provas (teor do site, do anúncio ou oferta, das mensagens públicas e comentários em sites de terceiros e dos dados do *Whois*, os endereços e os IPs dos sites, as datas e horários das informações inseridas ou divulgadas na Internet, os nomes e apelidos usados pelo golpista ou criminoso, os meios de contato e localização fornecidos pelo golpista, os dados bancários do golpista, etc.) antes que tais provas sumam da Internet, para ser usada em processo judicial. Depois disso, deve-se fazer um Boletim de Ocorrência levando-se cópias de tudo e todos os dados de identificação, contato e localização do golpista; bem como do pagamento efetuado ou valor furtado e do produto comprado ou do serviço contratado e como foi o cumprimento desse contrato pelo golpista.

> "As comparações entre escritura pública e ata notarial são inevitáveis; naquela, o tabelião é responsável pela elaboração de um documento contendo a manifestação de vontade, constituindo um negócio jurídico. Na ata notarial, o tabelião faz a narrativa dos fatos ou a materialização de algo em forma narrativa do que presencia ou presenciou, vendo e ouvindo com seus próprios sentidos e lavrando um documento qualificado com a mesma força probante da escritura pública e fé pública inerente do tabelião.
>
> É de ressaltar que o tabelião, na elaboração da ata notarial, deverá cumprir a objetividade dos fatos, vedada sua apreciação ou emissão de opinião pessoal a respeito dos fatos presenciados." (http://www.notariado.org.br/index.php?pG=X19leGliZV9ub3RpY2lhcw==&in=MzM5Mg==&filtro=9&Data=).

Assim reza a Lei Federal nº 8.935/1994 (http://www.planalto.gov.br/ccivil_03/leis/L8935.htm), nos artigos 6º e 7º:

"Art. 6º Aos notários compete:
I - formalizar juridicamente a vontade das partes;
II - intervir nos atos e negócios jurídicos a que as partes devam ou queiram dar forma legal ou autenticidade, autorizando a redação ou redigindo os instrumentos adequados, conservando os originais e expedindo cópias fidedignas de seu conteúdo;
III - autenticar fatos."

"Art. 7º Aos tabeliães de notas compete com exclusividade:
I - lavrar escrituras e procurações, públicas;
II - lavrar testamentos públicos e aprovar os cerrados;
III - lavrar atas notariais;
IV - reconhecer firmas;
V - autenticar cópias.
Parágrafo único. É facultado aos tabeliães de notas realizar todas as gestões e diligências necessárias ou convenientes ao preparo dos atos notariais, requerendo o que couber, sem ônus maiores que os emolumentos devidos pelo ato."

O Código Civil de 2002 (Lei nº 10.406/2002 - http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm), no artigo 215, assim prescreve:

"Art. 215. A escritura pública, lavrada em notas de tabelião, é documento dotado de fé pública, fazendo prova plena.
§ 1º Salvo quando exigidos por lei outros requisitos, a escritura pública deve conter:
I - data e local de sua realização;
II - reconhecimento da identidade e capacidade das partes e de quantos hajam comparecido ao ato, por si, como representantes, intervenientes ou testemunhas;
III - nome, nacionalidade, estado civil, profissão, domicílio e residência das partes e demais comparecentes, com a indicação, quando necessário, do regime de bens do casamento, nome do outro cônjuge e filiação;
IV - manifestação clara da vontade das partes e dos intervenientes;
V - referência ao cumprimento das exigências legais e fiscais inerentes à legitimidade do ato;
VI - declaração de ter sido lida na presença das partes e demais comparecentes, ou de que todos a leram;
VII - assinatura das partes e dos demais comparecentes, bem como a do tabelião ou seu substituto legal, encerrando o ato.
§ 2º Se algum comparecente não puder ou não souber escrever, outra pessoa capaz assinará por ele, a seu rogo.
§ 3º A escritura será redigida na língua nacional.
§ 4º Se qualquer dos comparecentes não souber a língua nacional e o tabelião não entender o idioma em que se expressa, deverá comparecer tradutor público para servir de intérprete, ou, não o havendo na localidade, outra pessoa capaz que, a juízo do tabelião, tenha idoneidade e conhecimento bastantes.
§ 5º Se algum dos comparecentes não for conhecido do tabelião, nem puder identificar-se por documento, deverão participar do ato pelo menos duas testemunhas que o conheçam e atestem

sua identidade."

O CPC - Código de Processo Civil (Lei n.º 13.105/2015 - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm), no artigo 384 assim diz:

"Art. 384. A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião.
Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial."

E se o site não tiver o CNPJ? **Como descobrir número CNPJ** pelo nome da Empresa? Uma forma simples, é digitar no Google (ou outro site de pesquisas) a palavra CNPJ e o nome da empresa entre aspas; assim, por exemplo: CNPJ AND "nome da empresa".

Se conhece o NIRE ou a Inscrição Estadual da empresa pode descobrir o CNPJ pelo site do Sintegra (http://www.sintegra.gov.br/), do Cadastro Estadual do ICMS (exemplo, https://www.cadesp.fazenda.sp.gov.br/(S(lavd3245p2qoo555slazkd45))/Pages/Cadastro/Consultas/ConsultaPublica/ConsultaPublica.aspx) ou da Junta Comercial de cada Estado (exemplo, https://www.jucesponline.sp.gov.br/BuscaAvancada.aspx).

O órgão equivalente à Junta Comercial nos Estados Unidos se chama SOS - *Secretary Of State* (Secretário de Estado) ou *Secretary of State's office* (Gabinete do Secretário de Estado) ou alguma nomenclatura semelhante, variando de Estado para Estado; pois, como no Brasil, cada Estado da União possui a sua. Normalmente é possível realizar pesquisas online sobre as empresas.

- http://kepler.sos.ca.gov/;
- https://www.sosnc.gov/search/;
- http://www.ct.gov/sots/site/default.asp;
- http://www.sos.state.tx.us/;
- http://www.sos.state.co.us/;

- http://sos.oregon.gov/;
- http://sos.tn.gov/;
- http://nvsos.gov/sos;
- http://www.sos.ne.gov/;
- http://sos.mt.gov/business/;
- http://sos.alabama.gov/;
- http://www.in.gov/sos/;
- https://www.sec.state.ma.us/.

Outra forma de descobrir o CNPJ da empresa é consultando o site http://www.juntadigital.com.br/. Normalmente, os serviços de consulta de cheques e de CPF/CNPJ (proteção ao crédito) possuem o serviço de descobrir o CNPJ da empresa ou o CPF da pessoa.

Também é possível a **identificação de CNPJ**:

- Através do *Whois*;
- Na lista de doadores de campanhas eleitorais no site do Tribunal Superior Eleitoral (http://www.tse.gov.br);
- Na relação de pessoas e empresas que receberam dinheiro do governo federal, no Portal da Transparência (http://www.transparencia.gov.br);
- No site Políticos do Brasil, de todos os candidatos das últimas eleições (http://www.politicosdobrasil.com.br);
- No site Registro-BR, que mantém uma base de dados de todos os detentores de domínios de internet no Brasil (http://registro.br);
- Na relação de companhias abertas no site da CVM - Comissão de Valores Mobiliários

(http://cvmweb.cvm.gov.br/SWB/Sistemas/SCW/CPublica/CiaAb/FormBuscaCiaAbOrdAlf.aspx).

Há vários **sites que informam o CNPJ** através da razão social da empresa e, até mesmo, do nome fantasia:

- http://cnpj.info/;
- http://receitaws.com.br/;
- http://www.cnpjbrasil.com/;
- http://www.empresascnpj.com/;
- http://empresasdobrasil.com/;
- https://www.infoplex.com.br/;
- http://www.buscacnpj.com.br/;
- http://www.foneempresas.com/;
- http://brazilianenterprises.com/;
- http://trade.nosis.com/pt;
- http://prospect.econodata.com.br/;
- http://www.inscricaoestadual.com/;
- https://wooki.com.br/;
- http://www.escavador.com/.

Conhecendo o CNPJ, bastar consultar os sites da Receita Federal (http://www.receita.fazenda.gov.br/PessoaJuridica/CNPJ/cnpjreva/Cnpjreva_Solicitacao.asp) e do Sintegra (http://www.sintegra.gov.br/).

Detalhe, nos sites da correlata Junta Comercial (exemplo, https://www.jucesponline.sp.gov.br/BuscaAvancada.aspx), obtêm-se as informações cadastrais da empresa.

Recomenda-se, ainda, consultar a existência de processos judiciais junto aos sites dos tribunais (http://www.cnj.jus.br/poder-judiciario/portais-dos-

tribunais). Há de se consultar, principalmente, o site do Tribunal de Justiça do Estado da empresa ou pessoa investigada (por exemplo, http://www.tjsp.jus.br/) para verificar a existência de ações judiciais.

Já se for pessoa física, **consulte o CPF** em http://www.receita.fazenda.gov.br/Aplicacoes/ATCTA/cpf/ConsultaPublica.asp.

Também é possível conferir, gratuitamente, se existem protestos contra o CNPJ e o CPF através do site https://www.ieptb.com.br/.

Caso queira informações mais detalhadas sobre CNPJ ou CPF, há vários sites para isso, tais como:

- http://www.scpc.com.br/;
- https://www.consultaserasa.com.br/;
- https://www.spcbrasil.org.br/;
- http://scpcjuridico.com.br/;
- http://www.olhonocredito.com.br/;
- https://www.spcprotesto.com.br/;
- http://www.consultebr.com.br/;
- http://www.checkmaster.com.br/;
- http://www.checkexpress.com.br/;
- https://www.megaconsultas.com.br/;
- https://www.brasilconsultas.com.br/;
- http://www.consultaok.com.br/;
- https://www.spcprepago.com.br/;
- http://inforbusca.com.br/;
- http://www.spcmix.com.br/;
- https://www.foregon.com;

- http://www.previnity.com.br/;
- http://institucional.checkcheck.com.br/;
- http://www.icheck.com.br/;
- http://www.checkok.com.br/;
- https://consultacheck.com.br;
- https://www.consultcheck.com.br;
- http://www.checkcred.com.br/;
- http://www.ccfacil.com.br/;
- http://www.mixconsultas.com.br/;
- https://www.consultanet.com.br/;
- http://www.totalconsultas.com.br/;
- http://www.consultacpf-cnpj.com/;
- http://www.informacred.com.br/;
- http://cpfcheck.com.br/;
- https://www.cquery.com.br/;
- https://www.fenixconsultas.com.br/;
- http://www.checkcheck.com.br/;
- http://www.chequefacil.com.br;
- http://www.ccfacil.com.br;
- http://www.f2b.com.br;
- http://cpfcheck.com.br/;
- https://spcnet.com.br/;
- https://www.consultasflex.com.br/.

Uma dica é pedir para alguém que assine, ou que no trabalho possua, o serviço de consulta de cheques ou de restrição de crédito (SPC, Serasa,

Cadin, etc.) para verificar os números de telefones, nomes, CPFs e CNPJs fornecidos pelo site. Dependendo do relacionamento que a pessoa tem no banco, pode-se pedir para o gerente da conta fazer essa gentileza.

Sobre a questão, o CDC - Código de Defesa do Consumidor (http://www.planalto.gov.br/ccivil_03/leis/l8078.htm), assim prescreve:

"Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que:

I - impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos. Nas relações de consumo entre o fornecedor e o consumidor pessoa jurídica, a indenização poderá ser limitada, em situações justificáveis;

II - subtraiam ao consumidor a opção de reembolso da quantia já paga, nos casos previstos neste código;

III - transfiram responsabilidades a terceiros;

IV - estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a eqüidade;

V - (Vetado);

VI - estabeleçam inversão do ônus da prova em prejuízo do consumidor;

VII - determinem a utilização compulsória de arbitragem;

VIII - imponham representante para concluir ou realizar outro negócio jurídico pelo consumidor;

IX - deixem ao fornecedor a opção de concluir ou não o contrato, embora obrigando o consumidor;

X - permitam ao fornecedor, direta ou indiretamente, variação do preço de maneira unilateral;

XI - autorizem o fornecedor a cancelar o contrato unilateralmente, sem que igual direito seja conferido ao consumidor;

XII - obriguem o consumidor a ressarcir os custos de cobrança de sua obrigação, sem que igual direito lhe seja conferido contra o fornecedor;

XIII - autorizem o fornecedor a modificar unilateralmente o conteúdo ou a qualidade do contrato, após sua celebração;

XIV - infrinjam ou possibilitem a violação de normas ambientais;

XV - estejam em desacordo com o sistema de proteção ao consumidor;

XVI - possibilitem a renúncia do direito de indenização por benfeitorias necessárias.

§ 1º Presume-se exagerada, entre outros casos, a vantagem que:

I - ofende os princípios fundamentais do sistema jurídico a que pertence;

II - restringe direitos ou obrigações fundamentais inerentes à natureza do contrato, de tal modo a ameaçar seu objeto ou equilíbrio contratual;

III - se mostra excessivamente onerosa para o consumidor, considerando-se a natureza e conteúdo do contrato, o interesse das partes e outras circunstâncias peculiares ao caso.

§ 2° A nulidade de uma cláusula contratual abusiva não invalida o contrato, exceto quando de sua ausência, apesar dos esforços de integração, decorrer ônus excessivo a qualquer das partes.

§ 3° (Vetado).

§ 4° É facultado a qualquer consumidor ou entidade que o represente requerer ao Ministério Público que ajuíze a competente ação para ser declarada a nulidade de cláusula contratual que contrarie o disposto neste código ou de qualquer forma não assegure o justo equilíbrio entre direitos e obrigações das partes.".

"Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.

§ 1° O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais:

I - sua apresentação;

II - o uso e os riscos que razoavelmente dele se esperam;

III - a época em que foi colocado em circulação.

§ 2º O produto não é considerado defeituoso pelo fato de outro de melhor qualidade ter sido colocado no mercado.

§ 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:

I - que não colocou o produto no mercado;

II - que, embora haja colocado o produto no mercado, o defeito inexiste;

III - a culpa exclusiva do consumidor ou de terceiro.".

"Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

§ 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:

I - o modo de seu fornecimento;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - a época em que foi fornecido.

§ 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.

§ 3° O fornecedor de serviços só não será responsabilizado quando provar:

I - que, tendo prestado o serviço, o defeito inexiste;

II - a culpa exclusiva do consumidor ou de terceiro.

§ 4° A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.".

"Art. 22. Os órgãos públicos, por si ou suas empresas, concessionárias, permissionárias ou sob qualquer outra forma de empreendimento, são obrigados a fornecer serviços adequados, eficientes, seguros e, quanto aos essenciais, contínuos.

Parágrafo único. Nos casos de descumprimento, total ou parcial, das obrigações referidas neste artigo, serão as pessoas jurídicas compelidas a cumpri-las e a reparar os danos causados, na forma prevista neste código.".

A responsabilidade do fornecedor ou do prestador de serviço, portanto, é objetiva (independe da existência de culpa ou dolo), pelos danos que causar ao consumidor, bastando para tanto a existência de nexo de causalidade entre o evidente defeito do serviço prestado e o dano suportado.

Em complemento, no Código Civil (Lei nº 10.406/2002 - http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm) também

existem expressas vedações ao descumprimento contratual (vez que o contrato faz lei entre as partes [*Lex inter partes*] e os contratos são feitos para serem cumpridos - *Pacta sunt servanda*), com a cominação da indenização pertinente ao contratante inadimplente:

> "Art. 247. Incorre na obrigação de indenizar perdas e danos o devedor que recusar a prestação a ele só imposta, ou só por ele exeqüível.".
>
> "Art. 389. Não cumprida a obrigação, responde o devedor por perdas e danos, mais juros e atualização monetária segundo índices oficiais regularmente estabelecidos, e honorários de advogado.".
>
> "Art. 395. Responde o devedor pelos prejuízos a que sua mora der causa, mais juros, atualização dos valores monetários segundo índices oficiais regularmente estabelecidos, e honorários de advogado.
> Parágrafo único. Se a prestação, devido à mora, se tornar inútil ao credor, este poderá enjeitá-la, e exigir a satisfação das perdas e danos.".

Portanto, todo aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito, gerando a obrigação de repará-lo, ao teor dos artigos 186, 187 e 927 do Código Civil.

> “Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.”.
>
> “Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.”.
>
> “Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.”.

Confira-se, ainda, a Súmula 479 do STJ - Superior Tribunal de Justiça: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.".

Desse modo, em caso de fraude, mesmo sendo causada por terceiros, as instituições financeiras têm responsabilidade objetiva (independe da existência de culpa, de dolo ou de prova); vez que é seu dever garantir a segurança do serviço prestado, bem como é sua responsabilidade indenizar

os consumidores por qualquer defeito ou falha na prestação dos serviços, mesmo que for cometida por terceiro.

- "Responsabilidade civil dos bancos nos casos de fraudes pela internet que lesam as contas de seus clientes" - http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9110;

- "RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES BANCÁRIAS POR DANOS CAUSADOS A CORRENTISTAS E A TERCEIROS" - http://sergiocavalieri.com.br/administrativo/artigos/imagens/RESPONSABILIDADE%20BANCA%CC%81RIA%202.pdf.

Trata-se da aplicação do risco do empreendimento; ou seja, quem aufere o bônus deve suportar o ônus.

ESPLANAÇÃO SOBRE PIRÂMIDES FINANCEIRAS

Recorda-se, por oportuno, que a pirâmide financeira consiste, na maioria das vezes, na revenda ou repasse do mesmo tipo de contrato para terceiros (novos membros do esquema), repartindo-se os valores recebidos das novas adesões entre os organizadores do sistema e os demais participantes que se encontram hierarquicamente acima dos novatos (iniciantes ou mais novos) no esquema. Como resultado, o verdadeiro lucro auferido advém do capital passado pelos novos aderentes, que, por se encontrarem na base (posição inferior) da referida pirâmide não conseguem recuperar o investimento feito no negócio, salvo se forem “promovidos” na estrutura e, assim, passarem a receber “comissões” pelo trabalho ou dinheiro alheio. Desse modo, a receita ou faturamento dos golpistas é muito maior sobre as vendas internas que faz para seus próprios “parceiros” do que para os clientes externos; sendo que uma empresa normal aufere renda com a venda e/ou prestação de serviços a clientes externos.

Em apertada síntese, o esquema de pirâmide financeira se caracteriza pela captação financeira altamente lucrativa para os que estão no topo da pirâmide, em desvantagem daqueles que estão na base dela, o que contraria todo o sistema jurídico. Desse modo, na pirâmide financeira, o foco está em recrutar mais pessoas, em vez de vender o produto ou prestar o serviço em si. Na verdade, ganha-se muito mais no recrutamento (novos membros ou usuários) do que na venda ou prestação do serviço: isso cria uma cadeia infinita de pessoas motivadas a atrair mais interessados.

São, assim, evidências da pirâmide financeira a obrigação do aderente, por conta própria e auferindo comissão em múltiplos níveis, efetuar divulgação e prospecção visando conseguir novos usuários para a atividade de fachada e de novos aderentes ao esquema para poderem terem realmente lucro.

As atuações de "representantes" sem exclusividade, num verdadeiro sistema canibal onde é cada um por si e todos contra todos, similar à uma guerra civil, é uma das características utilizadas pelas pirâmides financeiras, tais como, por exemplo, os conhecidos casos da TelexFree INC (Ympactus Comercial S/A), Priples Ltda, BBOM, etc.

A pirâmide financeira é crime contra a economia popular, contra o consumidor e de lavagem de dinheiro.

O crime é o de pirâmide financeira consistente na exploração fraudulenta de credulidade pública e só se diferencia do crime de estelionato (**Código Penal, art. 171** - http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm) em razão do número de vítimas ser indeterminado.

A **Lei 1.521/1951** (http://www.planalto.gov.br/ccivil_03/leis/L1521.htm), que trata dos crimes contra a economia popular, dispõe em seu **art. 2º, inciso IX**, que constitui crime contra a economia popular: "obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos ("bola de neve", "cadeias", "pichardismo" e quaisquer outros equivalentes)".

O Código de Defesa do Consumidor (http://www.planalto.gov.br/ccivil_03/leis/l8078.htm), por sua vez, preceitua que **configura crime**:

> "Art. 66. Fazer afirmação falsa ou enganosa, ou omitir informação relevante sobre a natureza, característica, qualidade, quantidade, segurança, desempenho, durabilidade, preço ou garantia de produtos ou serviços:"
>
> "Art. 67. Fazer ou promover publicidade que sabe ou deveria saber ser enganosa ou abusiva:"
>
> "Art. 68. Fazer ou promover publicidade que sabe ou deveria saber ser capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa a sua saúde ou segurança:"

Já a **Lei nº 5.768/1971** (http://www.planalto.gov.br/ccivil_03/leis/L5768.htm), dispõe sobre a distribuição gratuita de prêmios, mediante sorteio, vale-brinde ou concurso, a título de propaganda, estabelece normas de proteção à poupança popular, e em seu **artigo 7º**, versa sobre a **captação antecipada de poupança popular**.

A **Lei nº 9.613/1998** (http://www.planalto.gov.br/ccivil_03/leis/l9613.htm), por sua vez, dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores:

"Art. 1º. Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

(...)

§ 1º. Incorre na mesma pena quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de infração penal:

(...)

§ 2º. Incorre, ainda, na mesma pena quem:

I - utiliza, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal;

II - participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática de crimes previstos nesta Lei."

A existência e atuação das pirâmides financeiras é muito maior do que se possa imaginar.

- http://gizmodo.uol.com.br/piramides-antes-telexfree/;
- http://economia.ig.com.br/2013-07-13/piramides-alem-de-telexfree-e-bbom-outras-16-empresas-estao-sob-suspeita.html;
- http://blog.andersonferro.com.br/lista-de-33-supostas-piramides-financeiras-no-brasil/;
- https://blogvalis.wordpress.com/2013/08/19/conheca-as-50-empresas-que-sao-suspeitas-de-ser-piramide-financeiras/;
- http://www.gazetaonline.com.br/_conteudo/2013/08/noticias/dinheiro/1457189-lista-de-piramides-nao-para-de-crescer.html.

Em suma, para ser marketing multinível (MMN) ou de venda direta legítimos, o dinheiro que circula na rede e paga as comissões e bonificações dos "associados" deve ser proveniente de consumidores finais de produtos da empresa no varejo. Se, ao invés de dinheiro de consumidores finais, usar-se dinheiro dos próprios associados para pagar os associados mais antigos, fica configurado o **esquema de pirâmide financeira**, que vai desmoronar quando diminuir o ingresso de novos associados, deixando muita gente no prejuízo.

- http://www1.folha.uol.com.br/mercado/1247952-empresas-prometem-riqueza-facil-e-usam-esquema-piramide.shtml;
- http://www.folhaweb.com.br/?id_folha=2-1--2927-20130324;
- http://www.seae.fazenda.gov.br/noticias/nt60seae.pdf;

- http://www.seae.fazenda.gov.br/noticias/nt60seae.pdf/view;
- http://www.dinheiroganhar.net/bbom-como-saber-se-e-piramide-ou-nao/;
- http://www.youtube.com/watch?feature=player_embedded&v=NC9Cdd6pNg0;
- http://www.contabilidade-financeira.com/2013/08/esquema-ponzi-priples-bbom-e-telexfree.html;
- http://atualidadesdodireito.com.br/fabriciocorrea/2013/07/12/piramide-financeira/;
- http://economia.ig.com.br/2013-08-03/entenda-o-que-e-piramide-financeira.html;
- http://economia.terra.com.br/noticias/noticia.aspx?idNoticia=201307261030_TRR_82378613;
- http://www.infomoney.com.br/onde-investir/fundos-de-investimento/noticia/2702775/entenda-que-piramide-financeira-relembre-casos-famosos;
- http://oglobo.globo.com/defesa-do-consumidor/cartilha-explica-diferenca-entre-piramide-financeira-marketing-multinivel-9992514;
- http://www.justica.gov.br/portal/ministerio-da-justica/cartilha-explica-a-diferenca-entre-piramide-financeira-e-marketing-multinivel.htm;
- http://imagem.band.com.br/zoom/f_186303.jpg;
- http://andremansur.com/blog/empresas-prometem-riqueza-facil-e-usam-esquema-piramide/;
- http://carodinheiro.blogfolha.uol.com.br/2013/03/18/o-segredo-da-piramide/;
- http://tvuol.uol.com.br/assistir.htm?video=pratica-da-piramide-financeira-e-enganosa-e-ilegal-no-brasil-04028D19376EDCA94326;
- http://tvg.globo.com/programas/mais-voce/O-programa/noticia/2013/09/crime-com-prejuizos-irrecuperaveis-nao-caia-no-conto-da-piramide-financeira.html;
- http://www.portal730.com.br/economia/o-golpe-da-piramide-financeira-esta-de-volta-agora-pela-internet;
- http://www.comofazer.com.br/por-que-a-telexfree-e-uma-piramide-financeira/;
- http://www.youtube.com/watch?v=dyuN-xUdCG4&list=PL4gp_1sxrdHskrduvPaUP60AfBmXbURPh;
- http://www.youtube.com/watch?v=nLMI010lrBU;

- http://www.contilnetnoticias.com.br/Conteudo.aspx?ConteudoID=27963;
- http://colunas.cbn.globoradio.globo.com/platb/files/621/2013/03/Boletim-CVM-DPDC-2-fraude.pdf;
- http://www.youtube.com/watch?v=hb2yikq77AY;
- http://www.youtube.com/watch?v=yGHkFdnPHVk;
- http://www.youtube.com/watch?v=1hrAnvxf8zA;
- http://www.youtube.com/watch?v=HetU668aUqk;
- http://www.youtube.com/watch?v=dyuN-xUdCG4;
- http://www.marcosduda.com.br/marketing-multinivel-piramide-financeira/;
- http://www.vozdoacre.com/portal/07/saiba-diferenciar-marketing-multinivel-de-piramide-financeira/;
- http://globotv.globo.com/tv-anhanguera-go/bom-dia-go/v/entenda-a-diferenca-entre-piramide-financeira-e-marketing-multinivel-em-goias/2687905/;
- http://www.youtube.com/watch?v=z3DclABrL0k;
- http://www.consumidor.caop.mp.pr.gov.br/arquivos/File/nota_tecnica/1162013.pdf;
- http://industriadadecepcao.wordpress.com/;
- http://www.youtube.com/watch?v=ofxJhHP2g_Q;
- http://archive.is/U2SD9.

A essência do *marketing* multinível consiste em comercializar produtos/serviços por meio da formação de rede; isto é, um conjunto de pessoas engajadas se associam em prol da distribuição e divulgação de produtos de uma determinada empresa e com isso obtém bonificações. Assim MMN não possui associação a investimento e, muito menos, possui retorno garantido. Dessa forma, qualquer menção a investimento e garantia não tem validade alguma no *marketing* multinível; vez que toda empresa está sujeita a ter momentos de ascensão, estagnação ou queda e nenhuma está imune às vicissitudes inerentes ao mercado.

- http://marketingmultinivel.pt/lista-de-esquemas-em-piramide/.

A atratividade do sistema consiste no pagamento de bonificações, pela Requerida, por cada novo associado recrutado, de forma que quem se encontra no início da rede, ou topo da pirâmide, recebe premiações que superam o valor que pagou para associar-se, ao passo que 90% dos associados (a base da pirâmide) não consegue recuperar o valor do 'investimento', amargando prejuízo. E é justamente o prejuízo da imensa maioria dos 'investidores' que possibilita o lucro de uma pequena minoria; vale dizer: é o dinheiro de 90% dos associados, que nunca verão retorno algum, que paga o rendimento de um grupo de 10%, o qual cuida de fazer imensa publicidade do próprio enriquecimento e da lucratividade do esquema.

- https://www.youtube.com/watch?v=hg0taheAKSM;
- http://www.youtube.com/watch?v=S8PZNVItoLc.

Como em outros casos emblemáticos de pirâmide financeira, isso é apenas uma isca para recrutar novos associados, como ocorreu nos casos da **Avestruz Master**, **Boi Gordo**, clube de investimento Alpha Clube, rede Dinastia (que deu origem ao "Madoff mineiro") e tantas outras.

- http://gizmodo.uol.com.br/piramides-antes-telexfree/;
- http://pt.wikipedia.org/wiki/Boi_Gordo;
- http://pt.wikipedia.org/wiki/Avestruz_Master;
- http://www.guiainvest.com.br/publicacao/default.aspx?publicacao=128201;
- http://dicasemgeral.xpg.uol.com.br/curiosidades/22052/os-golpes-financeiros-boi-gordo-e-avestruz-master/;
- http://mktrelacionamentonatalrn.blogspot.com.br/2013/07/os-golpes-financeiros-boi-gordo-e.html;
- http://www.damiao1.com/2013/07/os-golpes-financeiros-que-enganaram_11.html;
- http://agricultura.ruralbr.com.br/noticia/2009/08/vitimas-de-golpe-da-fazenda-boi-gordo-aguardam-julgamento-do-processo-2624932.html;
- http://veja.abril.com.br/141101/p_118.html;

- http://economia.uol.com.br/ultimas-noticias/infomoney/2012/05/17/esquema-ponzi-entenda-e-fuja-deste-golpe-com-investimentos.jhtm;
- http://roubosonline.blogspot.com.br/2009/08/boi-gordo-frbg-credores-aguardam.html;
- http://economia.ig.com.br/mercados/com-promessa-de-dinheiro-facil-rede-dinastia-quer-ganhar-o-pais/n1300150616287.html;
- http://g1.globo.com/Noticias/SaoPaulo/0,,MUL144067-5605,00-POLICIA+INVESTIGA+EMPRESA+DE+LOJAS+VIRTUAIS+QUE+APLICARIA+GOLPE+DA+PIRAMIDE.html;
- http://www.youtube.com/watch?feature=player_embedded&v=2CV59vk2Maw;
- http://www.youtube.com/watch?feature=player_embedded&v=nQcRgObdyX4;
- http://www.youtube.com/watch?feature=player_embedded&v=2CV59vk2Maw;
- http://tj-rj.jusbrasil.com.br/noticias/51525/omni-international-e-condenada-por-divulgar-esquema-de-piramide;
- http://tj-rj.jusbrasil.com.br/noticias/51504/tj-condena-omni-international-a-pagar-indenizacoes-por-esquema-de-piramide-financeira;
- http://roubosonline.blogspot.com.br/2009/07/omni-condenada-por-ser-piramide.html;
- http://ow.ly/i/1gISM/original;
- Presidente da BBom fez parte do golpe aplicado pela Omni - http://www.eumilionario.com/presidente-da-bbom-telexfree/;
- http://economia.ig.com.br/mercados/2012-07-10/cvm-multa-e-suspende-o-empresario-thales-maioline-o-madoff-mineiro.html;
- As confissões de Madoff - http://epocanegocios.globo.com/Revista/Common/0,,ERT223322-16642,00.html.

A expressão “esquema Ponzi” deriva de famoso golpe aplicado nos EUA (Estados Unidos) pelo italiano Carlo Pietro Giovanni Guglielmo Tebaldo Ponzi, mais conhecido como Charles Ponzi, na década de 1920. O golpe causou perdas de cerca de US$ 20 milhões, uma grande fortuna para a época (cerca de US$ 225 milhões em 2011, em estimativa do site Bloomberg Businessweek). Ele prometia ganhos de 50% em 45 dias, ou 100% em 90 dias, na negociação de cupons postais internacionais, muito usados na época.

Depois de ter cumprido pelo menos duas condenações à prisão e de ter aplicado novos golpes nos EUA (Estados Unidos da América) e na Itália, Ponzi veio morar no Brasil, onde morreu pobre, no Rio de Janeiro, em 1949.

Um dos casos mais célebres dessa forma de atividade foi comandado por anos pelo financista Bernard Madoff, de Nova York, que causou perdas superiores a US$ 17 bilhões e está preso desde dezembro de 2008, hoje condenado à pena de 150 anos de reclusão. Esse modelo não tem a mesma lógica das pirâmides, mas caracteriza os chamados esquemas Ponzi. Nestes não há produto envolvido, nem o organizador paga comissão ou prêmio aos investidores pela captação de novos participantes. O esquema é basicamente uma "corrente" financeira, em que o organizador capta investidores prometendo-lhes altas taxas de retorno, naturalmente acima das pagas pelo restante do mercado (pois, se não fosse assim, dificilmente conseguiria captá-los). Ocorre que esse elevado retorno é pago à custa de parte do dinheiro dos investidores mais recentes, até que chega o momento em que o ingresso de novos investidores cai bruscamente ou cessa, e todo o esquema desmorona. Em outras palavras, o administrador do esquema tira dinheiro de uns investidores para pagar outros. Os estadunidenses chamam esse sistema de "tirar de Pedro para pagar Paulo" ("rob Peter to pay Paul").

Algumas perguntas iniciais que devem ser feitas para verificar se uma empresa é realmente uma MMN:

- Qual o(s) produto(s) da empresa e a aceitação do(s) mesmo(s) no mercado? Se não ficar claríssimo como água cristalina, desconfie!

- Quem comercializa esses produtos para os clientes finais, os distribuidores ou a própria empresa? Se for a própria empresa, desconfie! Os distribuidores é que tem que fazer o trabalho para ver que o produto realmente é vendável.

- Se o valor de adesão for alto, então é referente a aquisição de quê? Chegará algo na casa do aderente, ou este apenas terá a promessa de algo que nunca terá em mãos?

- Os ganhos diretos do aderente serão proporcionais a seus resultados ou proporcional ao valor que investiu? Se for proporcional ao valor que investiu, sem fazer nada mais, nem precisa desconfiar, é pirâmide! Se o ganho vem na maior parte da adesão de outros "distribuidores", é pirâmide! Em MMN de verdade a pessoa não "investe" para receber fixo durante 1 ano sem fazer nada; mas sim um valor relacionado com o que a rede produziu trabalho árduo.

Outro detalhe, se for um MMN puro, dificilmente colocará comercial na mídia ou alguém importante ou famoso para divulgar; pois MMN de verdade poupa dinheiro com essas coisas e paga o distribuidor para fazer a divulgação, as vendas e as indicações.

- http://www.youtube.com/watch?v=cAwzYf9_sRQ;
- http://www.youtube.com/watch?v=jYs58nvTDj4;
- http://www.youtube.com/watch?v=eMPZQvbvkyQ;
- http://www.youtube.com/watch?v=u2JTQPAXZcU.

Analisando o plano de recompensas das empresas de suposto *marketing* multinível de recrutamento, é possível identificar esses cinco **fatores evidenciadores de pirâmide**:

- O recrutamento de participantes é ilimitado, numa cadeia interminável de recrutadores motivados a recrutar novos recrutadores;
- O avanço na hierarquia de múltiplos níveis de participantes (vendedor, distribuidor, associado…) é alcançado pelo recrutamento, ao invés de nomeação ou seleção;
- Aquisição periódica de produtos (produtos da empresa ou venda de ferramentas, seguros, treinamentos…) pelos participantes é pré-requisito para receber comissões e avançar no negócio (pagar para participar);
- A empresa paga comissões e/ou bônus pela mesma venda para mais de um participante;
- Para cada venda, o pagamento da empresa para os participantes acima na cadeia iguala ou excede o que a pessoa realmente vender o produto, criando um incentivo insuficiente para vender produtos diretamente e um incentivo excessivo para recrutar novos participantes.

As pirâmides financeiras (ou “esquemas de pirâmide”; *pyramid schemes*, em inglês); também denominadas, às vezes, como “esquemas Ponzi” (*Ponzi schemes*, em inglês), possuem as seguintes **características:**

a) Associação a investimento: MMN não pode fazer qualquer tipo de promessa relacionada ou semelhante a investimento.

A essência do *marketing* multinível consiste em comercializar produtos/serviços por meio da formação de rede; isto é, um conjunto de pessoas engajadas se associam em prol da distribuição e divulgação de produtos de uma determinada empresa e com isso obtém bonificações. Contudo, existem aqueles que tratam o negócio como investimento financeiro e com retorno garantido. Ora, quem estiver interessado em ter um montante em dinheiro para investir há instituições regulamentadas para isso e aplicações diversas como caderneta de poupança, CDB, fundos de investimento, previdência privada, além de ações na bolsa de valores.

b) Dinheiro rápido e fácil: Promessas de dinheiro rápido ou fácil, sem fazer nada ou quaisquer variações que expressem facilidades exageradas e/ou irreais.

Quem já atua no *marketing* multinível há algum tempo sabe o quanto se trabalha neste ramo, são horas e horas na frente do computador, visitando pessoas, fazendo reuniões, estudando estratégias de divulgação e dando suporte a equipe.

c) Inconsistência do modelo de negócio. O primeiro fator a ser considerado, é a sustentabilidade da empresa. A expectativa de retorno do capital investido não decorre da comercialização ou da industrialização de produto ou serviço viável do ponto de vista do mercado, mas se baseia na captação de novos clientes–investidores (perdedores, na verdade).

Exemplo relativamente recente disso é que a TelexFree (Ympactus Comercial Ltda ME, CNPJ 11.669.325/0001-88) após ser impedida judicialmente de captar novos membros, entrou com pedido de recuperação judicial:

- http://www.conjur.com.br/2013-set-20/empresa-controla-telexfree-entra-pedido-recuperacao-judicial;
- http://g1-globocom.jusbrasil.com.br/noticias/100688791/telexfree-entra-com-pedido-de-recuperacao-judicial;
- http://g1.globo.com/economia/noticia/2013/09/telexfree-entra-com-pedido-de-recuperacao-judicial.html;

- http://www.valor.com.br/empresas/3278396/telexfree-entra-com-pedido-de-recuperacao-judicial;
- http://exame.abril.com.br/brasil/noticias/justica-nega-pedido-de-recuperacao-judicial-da-telexfree;
- http://economia.ig.com.br/2013-09-24/caso-telexfree-justica-nega-pedido-de-recuperacao-judicial.html;
- http://www.jb.com.br/economia/noticias/2013/09/24/justica-nega-pedido-de-recuperacao-judicial-da-telexfree/;
- http://veja.abril.com.br/noticia/economia/justica-nega-pedido-de-recuperacao-judicial-da-telexfree;
- http://economia.uol.com.br/noticias/redacao/2013/09/24/telexfree-tem-pedido-de-recuperacao-judicial-negado.htm;
- http://www.infomoney.com.br/onde-investir/renda-fixa/noticia/2975785/justica-nega-recuperacao-judicial-telexfree.

Os esquemas de pirâmide diferem do *marketing* multinível (MMN – "multilevel marketing", ou MLM, em inglês) lícito e viável porque neste a rentabilidade do negócio decorre da comercialização lícita de bens ou serviços, não dos aportes de novos investidores. Em suma, para ser *marketing* multinível ou de venda direta legítimos, o dinheiro que circula na rede e paga as comissões e bonificações dos "associados" deve ser proveniente de consumidores finais de produtos da empresa no varejo. **Se, ao invés de dinheiro de consumidores finais, usar-se dinheiro dos próprios associados para pagar os associados mais antigos, fica configurado o esquema de pirâmide**, que vai desmoronar quando diminuir o ingresso de novos associados, deixando muitas pessoas no prejuízo.

Obviamente, o fato de uma empresa se denominar de MMN não significa que ela seja lícita nem viável. No caso do MMN, porém, quando ocorre a relativa estabilização da rede de participantes, o negócio pode continuar de forma viável, porque está baseado na venda do(s) produto(s) ou serviço(s) ofertado(s) pela empresa. A rede de distribuidores ou vendedores perderá velocidade de crescimento, sem que isso ponha a atividade em risco. Já nas pirâmides, quando os níveis inferiores param de crescer, o negócio começa a entrar em colapso, já que se amparava exatamente no crescimento indefinido (mesmo que impossível) de novos participantes.

Os esquemas de pirâmide costumam cobrar caro pela adesão, incluindo taxas de treinamento, kit inicial e uma taxa de inscrição não reembolsável.

Em Portugal, os esquemas de pirâmide efetuados pelas empresas perante os consumidores são considerados prática comercial desleal e como tal proibidos por lei, nos termos do artigo 8.º do Decreto-Lei nº 57/2008, que estabelece que é considerada prática enganosa (e consequentemente desleal): "Criar, explorar ou promover um sistema de promoção em pirâmide em que o consumidor dá a sua própria contribuição em troca da possibilidade de receber uma contrapartida que decorra essencialmente da entrada de outros consumidores no sistema" (http://dre.pt/pdf1sdip/2008/03/06000/0174701754.pdf).

Outra característica do MMN autêntico é que neste a maior parte da receita advém da comercialização do(s) produto(s) ou serviço(s) para pessoas que estejam fora da rede, ou seja, para consumidores finais, não para os próprios participantes.

d) Promessa de retorno rápido e elevado do capital para os clientes, muito acima das taxas de retorno habituais da economia. De fato, durante algum tempo, muitas pirâmides e esquemas Ponzi geram ganhos para os primeiros níveis de participantes, pois a promessa de lucro elevado e o exemplo – freneticamente alardeado – desses primeiros (e poucos) bem-sucedidos levam centenas ou milhares de desavisados a investir no esquema.

A remuneração exacerbada de alguns investidores serve para dar aparência de sucesso anormal do investimento e, com base nisso, para angariar clientes desavisados. Há de se ter cautela quanto a pessoas que tentam convencer os outros das vantagens de uma suposta MLM alardeando sua riqueza pessoal. Perceba que muitas pessoas que dizem ter ganho milhões com MLM, na verdade, ganham dinheiro vendendo livros e vídeos sobre MLM. Em resumo: se parece bom demais para ser verdade, deve ser mentira.

e) Propaganda agressiva, frequentemente enganosa, por omitir aspectos fundamentais do negócio e menosprezar ou ignorar completamente

os riscos, de maneira deliberada.

f) Associação a empresas sem tradição no mercado: como em geral as pirâmides duram pouco tempo, não costumam ser aplicadas por empresas consolidadas ao longo do tempo.

g) Necessidade de explicações sobre a (aparente) legalidade do esquema: como os esquemas de pirâmide são mirabolantes e estranhos ao funcionamento normal do mercado, são comuns explicações veementes para convencer os participantes da legitimidade do negócio, com artifícios variados que procuram mascarar a fraude.

Já o *marketing* de múltiplos níveis (em inglês: MLM - *Multi-Level Marketing* ou MML - *Marketing Multi Level*), ou marketing de rede, é uma atividade lícita. Empresas como Amway, Tupperware, Herbalife, Avon, Mary Kay e The Pampered Chef empregam imensas redes de distribuidores e vendedores que comercializam toda espécie de produto, de suplementos vitamínicos a utensílios de cozinha e produtos de beleza. Os vendedores são conhecidos como proprietários independentes de negócios (IBO, sigla em inglês) e em geral trabalham de suas casas.

Detalhe, a Herbalife para não sofrer condenação de pirâmide financeira, precisou propor um acordo de alterações substanciais e, ainda, pagar uma multa astronômica.

- http://www.curapelanatureza.com.br/post/09/2016/herbalife-pagara-multa-milionaria-nos-eua-acusada-de-enganar-consumidores;
- http://g1.globo.com/economia/negocios/noticia/2016/07/herbalife-pagara-us-200-milhoes-e-tera-que-reestruturar-operacoes.html.

Entretanto, **a associação de uma pirâmide à venda de um produto ou serviço não é suficiente para descaracterizá-la como fraude**. Ao contrário, muitos esquemas de pirâmide usam produtos justamente para disfarçar seu caráter ilícito e até para obter dinheiro dos investidores. Para o negócio ser sustentável, é preciso que o produto ou serviço seja a fonte principal do faturamento da empresa e seja suficiente para gerar a maior parte da renda a ser distribuída entre os participantes. Se esta decorrer principalmente dos aportes de dinheiro efetuados por novos investidores, o

negócio caracterizará uma pirâmide e, portanto, será economicamente inviável.

A existência de produto ou cesta de produtos nos esquemas pirâmides pode servir não somente para mascarar a essência do negócio, mas, também, como forma adicional de lesar os investidores. Por meio da imposição a estes da aquisição de diversos produtos (que não têm aceitabilidade suficiente no mercado para se venderem), os administradores e os níveis superiores da pirâmide abarrotam os graus inferiores de mercadorias que, na maior parte, jamais serão vendidas. Essa imposição de compra de produtos por parte dos novos investidores é a maneira pela qual eles perderão seu investimento, pois adquirirão bens que não conseguirão vender, seja porque têm pouca aceitação no mercado, seja porque já foram vendidos a preços inflados. É o que os americanos chamam de *inventory loading*, algo como "carregamento de estoque". Diversos esquemas de pirâmide que usam produtos não seguem a "regra americana dos 70%", segundo a qual um distribuidor só deve obrigar seus representantes a comprar novos produtos quando ao menos 70% do estoque destes houver sido vendido aos consumidores finais.

Nos Estados Unidos, uma forma de diferenciar os dois sistemas é a chamada regra dos 70%: se a empresa tem 70% ou mais de seu rendimento advindo dos produtos, é marketing em rede, senão é pirâmide. Essa regra surgiu de uma decisão histórica, em 1979, pela qual a Comissão Federal do Comércio dos EUA determinou que a Amway não era um esquema de pirâmide. Isso abriu caminho para que centenas de empresas seguissem seu modelo de negócios. O site da Amway destaca as diferenças entre as "oportunidades únicas de negócios" que a empresa representa e um esquema de pirâmide.

A *Securities and Exchange Commission* (Comissão de Valores Mobiliários), frequentemente abreviada SEC (http://www.sec.gov/), é uma agência federal dos Estados Unidos que detém a responsabilidade primária pela aplicação das leis de títulos federais e a regulação do setor de valores mobiliários, as ações da nação e opções de câmbio, e outros mercados de valores eletrônicos nos Estados Unidos.

A Amway não paga distribuidores por recrutar novos vendedores. A única maneira de ganhar dinheiro, na Amway, é vender produtos diretamente ao consumidor ou administrar uma equipe de vendas. Os executivos recebem uma porcentagem das vendas de cada um de seus recrutas. A Amway não requer que seus vendedores comprem kits iniciais ou impõe encomenda mensal mínima a quem deseja se manter como membro. Ela enfatiza que a principal diferença entre um modelo de MLM legítimo e um esquema de pirâmide é que uma empresa que usa o MLM de forma honesta está concentrada em vender produtos, não em recrutar mais vendedores. Em uma empresa que utilize o MLM de maneira legítima, deve ser possível ganhar dinheiro pela simples venda direta de produtos aos consumidores. Com esse critério básico em mente, eis algumas outras maneiras de identificar esquemas de pirâmide baseados em produtos: Esquemas de pirâmide oferecem dinheiro pelo simples recrutamento de pessoas. O dinheiro pode vir como comissão pela venda do kit inicial ou como um "bônus" de recrutamento. Assim supostas empresas de MLM que enfatizam mais o recrutamento de vendedores do que a venda do produto são suspeitas de serem pirâmides.

> "Esquemas de pirâmide agora vêm em tantas formas que podem ser difíceis de reconhecer imediatamente. No entanto, todos eles compartilham uma característica primordial. Eles prometem consumidores ou investidores grandes lucros com base principalmente no recrutamento de outras pessoas para participar do seu programa, e não com base em lucros de qualquer investimento real ou venda real de bens para o público. Alguns sistemas podem pretende vender um produto, mas que muitas vezes basta usar o produto para esconder a sua estrutura piramidal. Há dois sinais indicadores de que um produto está sendo usado simplesmente para disfarçar um esquema de pirâmide: carregamento de estoques e uma falta de vendas no varejo. Carregamento de estoques ocorre quando as forças de programa de incentivo da empresa recruta para comprar mais produtos do que jamais poderia vender, muitas vezes a preços inflacionados. Se isso ocorre em todo o sistema de distribuição da empresa, as pessoas no topo da pirâmide colher lucros substanciais, apesar de pouco ou nenhum produto se move para o mercado. As pessoas no fundo fazer pagamentos excessivos de inventário que simplesmente se acumula nos seus porões. A falta de vendas no varejo também é uma bandeira vermelha que existe uma pirâmide. Muitos esquemas de pirâmide vão alegar que seu produto está vendendo como pão quente. No entanto, uma análise mais aprofundada, ocorrem as vendas apenas entre as pessoas dentro da estrutura de pirâmide ou para os novos recrutas juntam a estrutura, não para os consumidores no público em geral. (*omissis*). A Comissão considerou que esquemas de pirâmide participantes da força de pagar o dinheiro em troca de duas coisas. Em primeiro lugar é "o direito de vender um produto", o segundo é "o direito de receber, em troca de recrutar outros participantes no programa, recompensas que não estão relacionados com a venda do produto para os usuários finais." ("Esquemas de pirâmide", Palestra de Debra A. Valentine, Conselheiro Geral da Comissão Federal do Comércio dos Estados Unidos, ao FMI no seminário sobre questões jurídicas atuais que afetam bancos centrais, Washington, em 13/05/1998 - http://www.ftc.gov/speeches/other/dvimf16.shtm).

A falta de informações claras, a obscuridade no seu funcionamento e a necessidade de maiores e detalhadas explicações der como funciona, são sinalizadores iniciais do esquema de pirâmide.

No MMN a própria empresa não comercializa os seus produtos ou serviços. Outro detalhe, no esquema de MMN, impera a informalidade; ou seja, os vendedores são pessoas físicas que trabalham em suas próprias residências e sem usarem uniformes.

A receita/faturamento da pirâmide advêm, principalmente, das comissões recebidas sobre o trabalho alheio dos demais integrantes da rede que se encontram em posição hierárquica inferior.

Senão vejamos as principais características identificadoras de um esquema Ponzi.

O primeiro requisito é o recrutamento indiscriminado ou ilimitado, sem se importar ou preocupar com a saturação do mercado; ou seja, coloca os novatos para disputarem entre si no mesmo território. Desse modo, a oportunidade para cada pessoa ganhar dinheiro é cada vez menor, à medida que entra mais alguém na pirâmide. Assim, se a empresa permite novos membros para disputarem os mesmos pretensos clientes em troca de baixas comissões nas vendas, mas paga considerável comissão dessas mesmas vendas para aqueles que estão em posição hierarquicamente superior no organograma da empresa, já configura uma forte evidência de esquema Ponzi. Outra premissa, é que o faturamento somente de comissões de vendas acaba tornado o negócio inviável, mas se for promovido na pirâmide, começará a receber comissões sobre as vendas alheias sem nenhum trabalho e nenhuma despesa.

Segundo requisito, a promoção, ascensão ou progresso na hierarquia é conseguido primeiramente por conseguir efetuar quantidades milagrosas de vendas por um determinado tempo e com uma infraestrutura extravagante, exagerada e supérflua (espaço físico, computadores, telefones, veículos, equipamentos, funcionários, uniformes, propagandas, materiais promocionais, equipamentos e materiais com logotipos, etc.), o que implica

em ter que trabalhar por vários meses no vermelho como reles vendedor de quem o colocou no esquema para poder custear essa aparência suntuosa. Mesmo depois da primeira promoção, a pessoa ainda continua trabalhando no vermelho. Somente depois da segunda promoção (de parceiro para espelho) passa a ser priorizada e comissionada a quantidade de pessoas que coloca no nível inferior.

Em resumo, este requisito é um dos mais conhecidos dos esquemas de pirâmide, ou seja, pagar mais dinheiro a quem recruta mais pessoas para o esquema. Assim, à medida que o recrutador recruta mais pessoas para o esquema, vai subindo para novos níveis, que incentivam a recrutar ainda mais, com a oferta de comissões elevadas ou outros bens materiais de luxo. Tudo isso é pago às custas do trabalho e dos investimentos dos novos "investidores".

O terceiro requisito serve de reforço ao segundo; ou seja, o pagamento de gratificações a mais de dois níveis na estrutura (supervisor estadual e representante nacional) sobre a mesma venda e/ou o percentual ou o valor dessas gratificações ser inversamente proporcional ao trabalho e despesa despendidas para a concretização da venda (enriquece os que estão acima, à custa dos que estão na base).

O quarto elemento é a imposição de aquisição periódica e exagerada de produtos, materiais e recursos; bem como a participação em cursos, eventos, convenções, campanhas e promoções. Um agravante é que tais compras e participação nos eventos é premissa (condição ou pré-requisito) para poder receber as comissões e/ou premiações e avançar no negócio. É o conhecido esquema do pagar para poder participar.

O quinto elemento é a imposição de cotas de vendas a quem deveria ter liberdade de atuação. Por outras palavras, a pessoa sofre controle, fiscalização e cobrança como se funcionário fosse, mas sem a devida contraprestação.

Diante dessas explicações, o leitor terá condições de identificar falsas moedas digitais e falsas empresas de mineração que são idealizadas por golpistas para enganarem pessoas gananciosas, preguiçosas e ignorantes.

DAS MANIFESTAÇÕES ESTATAIS SOBRE AS CRIPTOMOEDAS

A maioria dos governos (países) já se pronunciou de alguma forma sobre a Bitcoin e as demais moedas digitais. Poucos são os que realmente baniram a moeda (Bolívia, Bangladesh, Equador, Quirguistão e Islândia). Outros tantos restringiram a sua utilização, entre eles China, Índia e Rússia. Já Brasil, Estados Unidos e União Europeia (https://europa.eu/european-union/index_pt) estão entre os que instruíram suas autoridades tributárias a reconhecer a moeda e definir procedimentos para declaração e taxação de operações em BTC (Bitcoin).

- https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country.

O Ministério Federal de Finanças da **Alemanha** já reconhece a bitcoin como uma moeda privada; mas insiste que não haverá isenção do pagamento de tributos para quem realizar atividades comerciais aceitando bitcoins.

- http://www.welt.de/finanzen/geldanlage/article119086297/Deutschland-erkennt-Bitcoin-als-privates-Geld-an.html;
- http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html;
- http://www.spiegel.de/netzwelt/netzpolitik/finanzministerium-erkennt-bitcoins-als-zahlungsmittel-an-a-917151.html.

A t3n (http://t3n.de/) é a primeira empresa alemã a pagar salários em bitcoin.

- https://jornalbitcoin.pt/index.php/item/512-a-t3n-e-a-primeira-empresa-alema-a-pagar-salarios-em-bitcoin.

Apesar da Alemanha, em agosto de 2013, ter reconhecido a bitcoin como "dinheiro privado", alguns governos, como o da **Noruega**, se negam a reconhecer a moeda digital como dinheiro.

- http://softwarelivre.org/revistaespiritolivre/blog/governo-da-noruega-diz-que-bitcoin-“nao-e-dinheiro-de-verdade”;

- http://www.elfinanciero.com.mx/archivo/bitcoin-sufre-nuevo-reves-ahora-en-noruega.html.

Mas, contraditoriamente, a Noruega possui seu próprio projeto de eliminação das cédulas como dinheiro.

- https://www.oroyfinanzas.com/2015/11/banco-noruega-deja-dinero-efectivo/;
- http://www.bbc.com/portuguese/noticias/2015/05/150518_dinamarca_fim_cedulas_moedas_dinheiro_rb;
- http://noticias.bol.uol.com.br/ultimas-noticias/internacional/2014/07/15/noruega-devera-extinguir-o-dinheiro-em-seis-anos.htm;
- http://ansabrasil.com.br/brasil/noticias/mundo/noticias/2014/07/15/Noruega-nao-utilizara-mais-dinheiro-em-seis-anos_7927486.html.

A Dinamarca e a Suécia trilham o mesmo caminho da Noruega sobre extinguir as cédulas.

- http://hojeemdia.com.br/opini%C3%A3o/blogs/opini%C3%A3o-1.363900/o-fim-do-dinheiro-1.363623;
- http://www.gazetadopovo.com.br/mundo/dinheiro-de-papel-pode-ser-extinto-na-dinamarca-a92441d61jst7tpsdypiqqzys;
- http://www.bbc.com/portuguese/noticias/2016/04/160411_sociedade_sem_dinheiro_cw_rb;
- http://g1.globo.com/economia/noticia/2016/04/dinheiro-pode-sair-de-circulacao-na-suecia-ate-2030.html.

O governo indiano, na segunda semana de novembro de 2016, subitamente, baniu as cédulas de 500 e de 1.000 rúpias, tornando-as sem valor e sem aceitação. Essas duas cédulas representavam quase 80% de todo o dinheiro vivo em circulação no país. Desse modo, da noite para o dia, a população se viu na posse de um dinheiro que não valia mais nada, com o que muitas pessoas perderam seus recursos, economias e poupanças.

- http://money.cnn.com/2016/11/08/news/economy/india-rupee-notes-ban-currency/.

Sobre o dinheiro físico ou convencional, ressalta-se que uma cédula dura, em média, de 18 (dezoito) a 36 (trinta e seis) meses, dependendo do valor e do grau de circulação (manuseio). Desse modo, as cédulas de menor valor duram muito menos por circularem mais de mão e mão e, assim, se desgastam mais rápido. Já as cédulas de maior valor, por normalmente serem guardadas, possuem uma durabilidade maior.

- Cédulas Inadequadas à Circulação - http://www.bcb.gov.br/htms/mecir/inadequadas/cedinadeq.asp;

- "Em 2006, foram gastos R$ 136 milhões com a fabricação de 1,21 bilhão de cédulas, dos quais 80% foram destinados à substituição das notas desgastadas e danificadas." (http://www.bcb.gov.br/textonoticia.asp?codigo=822&idpai=noticias).

Em relação às moedas metálicas no valor de 1, 5, 10 e 25 centavos, o custo da cunhagem supera muito o do valor que as mesmas estampam.

Um fator que encarece ainda mais a emissão de cédulas e cunhagem de moedas metálicas são as medidas antifalsificação.

O dinheiro físico também agride o meio ambiente; vez que além do papel não reciclado utilizado nas cédulas e dos metais nas moedas (ambos bens finitos), também há: a papelada envolvida na burocracia correlata; as tintas, solventes e plásticos usados na impressão; o combustível fóssil queimado no seu transporte; etc. Ainda mais, há a questão da higiene. Ao pegar dinheiro em um caixa eletrônico, a pessoa se expõe a bactérias tal como usar o pior dos banheiros públicos. Desse modo, 94% das notas de dólar têm vestígios de estafilococos, bactérias causadoras de doenças como pneumonia e meningite.

O Vietnã liga as criptomoedas com atividades criminosas, como a lavagem de dinheiro, e, assim, as tornou ilegais para todas as instituições financeiras e todos os cidadãos. Também são ilegais na Bolívia e no Quirguistão.

- https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/;

- http://www.diariobitcoin.com/index.php/2015/05/27/10-paises-en-los-que-bitcoin-esta-prohibido/;

- http://es.panampost.com/belen-marty/2014/06/19/bolivia-el-primer-pais-americano-en-prohibir-bitcoin/.

Embora os governos da Bolívia e do Equador têm ambos proibidos a bitcoin em seus países, o presidente da Venezuela não deixou clara sua posição. Além disso, segundo a lei venezuelana, bitcoin é considerado como propriedade e não moeda.

- http://observador.pt/2016/08/11/perante-o-caos-venezuelanos-viram-se-para-a-bitcoin/.

A negociação com bitcoin foi proibida na **Islândia**, mas, contraditoriamente, uma nova criptomoeda chamada AuroraCoin (http://en.auroracoin.is/ e http://auroracoin.org/) foi lançada na Islândia.

- http://oglobo.globo.com/sociedade/tecnologia/islandia-ganha-moeda-virtual-propria-cada-habitante-tem-direito-resgatar-equivalente-us-380-11990023;
- http://fin-tech.es/2016/07/auroracoin-la-divisa-alternativa-de-los-islandeses-contra-las-restricciones-de-su-gobierno.html;
- http://elcomercio.pe/insolito/tecnologia/auroracoins-moneda-virtual-gratuita-todos-islandia-noticia-1719000;
- http://www.prisonplanet.pl/ekonomia/islandia_wprowadza,p770345098;
- http://www.bankier.pl/wiadomosc/Islandia-odbierze-bankom-wladze-nad-pieniadzem-7244367.html;
- https://actualidad.rt.com/actualidad/view/115268-descubren-islandia-minas-bitcoin.

O Banco Central da **Nova Zelândia** (*Reserve Bank of New Zealand* - http://www.rbnz.govt.nz/) disse que somente eles possuem autorização legal para a emissão de moedas e que o Bitcoin seria apenas um meio de pagamento, podendo qualquer instituição não financeira operar com a moeda virtual, com uma peculiar condição: desde que não haja circulação física de bitcoins, em formato de notas ou moedas metálicas.

A **Rússia** que já chegou a declarar ilegais as transações envolvendo bitcoins, contraditoriamente planeja introduzir a sua própria moeda virtual. E parece que já percebeu que é melhor tributar do que proibir.

- http://economia.uol.com.br/noticias/infomoney/2014/02/11/governo-russo-proibe-uso-de-bitcoin-no-pais.htm;
- http://exame.abril.com.br/economia/noticias/russia-quer-prender-quem-usar-bitcoin;
- http://guiadobitcoin.com.br/russia-esta-oficializando-o-bitcoin-como-uma-moeda-de-cambio-no-pais/;
- http://forklog.net/russia-abandons-bitcoin-penalization-plans/;
- http://csef.ru/en/ekonomika-i-finansy/508/minfin-uzakonit-bitkoiny-kak-inostrannuyu-valyutu-6885;
- http://br.sputniknews.com/mundo/20160527/4793280/russia-moeda-virtual.html;
- https://criptonoticias.com/bancos/mayor-banco-ruso-cerca-de-unirse-al-consorcio-blockchain-creado-por-el-banco-central-de-rusia/#axzz4Hu6yNo00.

Apesar da intenção russa inicial de querer proibir a emissão e o uso de moedas digitais na troca de bens e serviços, passou-se a querer proibir a bitcoin (moeda), mas não a *Blockchain* (protocolo da bitcoin). Depois suspendeu-se o projeto de lei que iria criminalizar as moedas digitais e começaram a pensar em permiti-la; vez que passaram a entender que seria melhor criarem a própria moeda digital.

- https://www.cryptocoinsnews.com/proposed-bitcoin-ban-russia-revised-future/;
- http://www.coindesk.com/russias-bitcoin-ban-draft-bill-withdrawn/;
- http://www.coindesk.com/russia-ban-bitcoin-not-blockchain/;
- https://news.bitcoin.com/russias-central-bank-officially-announces-blockchain-work-group/;
- http://www.coindesk.com/russian-bitcoin-penalties-abandon-report/;
- https://www.cryptocoinsnews.com/russia-reverses-plan-to-penalize-bitcoin-use/;
- https://cointelegraph.com/news/russia-to-treat-bitcoin-as-foreign-currency-and-enable-trading;
- http://www.newsbtc.com/2016/07/19/russia-treat-bitcoin-foreign-currency/;
- http://www.coindesk.com/russia-ministry-finance-bitcoin-foreign-currency/;

- http://bravenewcoin.com/news/amidst-bitcoin-boom-russia-plans-its-own-cryptocurrency-banning-all-others/;

- http://sputniknews.com/russia/20160527/1040338067/russia-cryptocurrency-finances-national.html.

A primeira *exchange* *offline* de Bitcoin já foi inaugurada em Moscou. Detalhe, a empresa iniciou sem registro formal. Notícia divulgada em 16/08/2016 pelo https://lenta.ru/news/2016/08/16/bitcoins/.

De modo semelhante, a **China**, no início, em dezembro de 2013, proibiu que instituições financeiras utilizassem a bitcoin, por temerem que a criptomoeda fosse utilizada em atividades ilegais e especulação monetária. Inclusive ameaçou as empresas que negociavam o câmbio de bitcoins por yuans (moeda chinesa), que elas teriam a conta congelada e, em consequência, perderiam todo o dinheiro negociado. No entanto, os indivíduos poderiam continuar utilizando-o normalmente. Depois, contraditoriamente, divulgou que está estudando a possibilidade de emitir sua própria moeda digital.

- http://www.spiegel.de/forum/netzwelt/virtuelle-waehrung-verbote-und-technische-probleme-setzen-bitcoin-zu-thread-113125-1.html;

- http://www.spiegel.de/netzwelt/netzpolitik/chinas-notenbank-verbietet-finanzbranche-bitcoin-transaktionen-a-937413.html;

- http://www.spiegel.de/forum/netzwelt/internetwaehrung-chinas-notenbank-verbietet-banken-bitcoin-geschaefte-thread-107837-1.html;

- https://www.oficinadanet.com.br/post/12168-bitcoin-perde-valor-apos-china-bloquear-cambio;

- http://g1.globo.com/tecnologia/noticia/2014/04/china-fechara-contas-bancarias-de-empresas-que-trocam-bitcoin.html;

- http://economia.uol.com.br/noticias/bloomberg/2016/01/21/china-avalia-resposta-ao-bitcoin-com-estudo-sobre-moeda-digital.htm;

- https://www.oroyfinanzas.com/2016/01/banco-central-chino-quiere-emitir-bitcoin-criptomoneda-estatal-pronto/.

Na Assembleia Popular Nacional (http://www.npc.gov.cn/) ou Congresso Nacional do Povo (□□□□□□□□ , em chinês; *Quánguó Rénmín Dàibiǎo Dàhuì*, em pinyin), está em trâmite o projeto de lei do Código Civil (□□□),

que deve ser aprovado em 2017. Após o início de sua vigência, se não sofrer alterações, propriedades e dados virtuais, incluindo moedas digitais, podem ser oficialmente "Direitos das Pessoas".

- http://www.npc.gov.cn/npc/zgrdzz/2016-08/03/content_1994723.htm;
- http://www.npc.gov.cn/npc/zgrdzz/2016-08/03/content_1994732.htm;
- http://www.npc.gov.cn/npc/zgrdzz/2016-08/03/content_1994730.htm;
- http://www.npc.gov.cn/npc/zgrdzz/2016-08/03/content_1994731.htm.

Em 20/01/2014, o **Taobao** (uma versão chinesa do eBay), o maior *marketplace* online da China, proibiu a venda de todos os equipamentos de mineração de criptomoedas e tutoriais de mineração.

- https://rule.taobao.com/detail-1358.htm?spm=0.0.0.0.RLx3a1&qq-pf-to=pcqq.group.

Uma juíza da Flórida, nos **Estados Unidos**, já recusou as acusações de um caso de lavagem de dinheiro envolvendo uma suposta venda ilegal de bitcoins devido ao fato da moeda digital não ser dinheiro real sob as leis do estado.

- https://nakedsecurity.sophos.com/pt/2016/07/27/is-bitcoin-real-money-florida-judge-says-no/;
- http://www.miamiherald.com/news/local/crime/article91682102.html?rel=nofollow;
- https://www.washingtonpost.com/news/morning-mix/wp/2016/07/26/bitcoins-not-money-judge-rules-as-she-tosses-money-laundering-charge/.

Já outro juiz americano, do tribunal distrital no Texas, descreveu a bitcoin como sendo "uma forma de dinheiro".

- http://www.spiegel.de/netzwelt/web/us-richter-stuft-bitcoins-als-regulaere-waehrung-ein-a-915445.html.

Em 2013, nos Estados Unidos, a competência para regulamentação da bitcoin foi transferida aos Estados. Em Nova York exige-se uma licença especial (*bitlicense*) das organizações que prestam serviços, no Estado, em

moedas virtuais com recursos de clientes. Assim, as regras são semelhantes às adotadas por serviços de transferência internacional de dinheiro, como a Western Union.

- http://idgnow.com.br/internet/2015/06/05/nova-york-anuncia-novas-regras-de-regulamentacao-do-bitcoin-para-o-estado/.

O itBit Trust Co. (https://www.itbit.com/trust-company) obteve a primeira licença nos Estados Unidos para a troca de bitcoin.

- http://economia.uol.com.br/noticias/afp/2015/05/07/nova-york-concede-primeira-licenca-a-um-operador-de-bitcoin.htm.

Nos Estados Unidos a bitcoin é oficialmente uma *commodity*; ou seja, uma propriedade e não uma moeda.

- https://www.theguardian.com/technology/2014/mar/25/bitcoin-property-currency-irs-rules;

- http://economico.sapo.pt/noticias/bitcoin-passa-a-ser-considerada-uma-commodity_229266.html.

A Nasdaq (http://www.nasdaq.com/topic/bitcoin) anunciou, em 23/03/2015, a sua entrada, mesmo que indireta, no mercado de moedas virtuais como a bitcoin.

- http://www.wsj.com/articles/nasdaq-to-provide-trading-technology-for-bitcoin-marketplace-1427140006;

- http://www.nasdaq.com/symbol/gbtc/stock-chart.

Do mesmo modo, é possível conferir a cotação da bitcoin no *Yahoo finance* (http://finance.yahoo.com/quote/BTCUSD=X?ltr=1).

Em contrapartida, além de permitir as moedas virtuais, o Estados Unidos possui várias agências governamentais trabalhando na prevenção ou redução do uso delas para transações ilegais.

O Departamento de Tesouro dos Estados Unidos (*U.S. Department of Treasury's* - https://www.treasury.gov/), através da rede de combate a

crimes financeiros (*FinCEN - Financial Crimes Enforcement Network* - https://www.fincen.gov/), tem emitido orientações sobre bitcoin desde o início de 2013. O Tesouro americano definiu a bitcoin não como uma moeda, mas como uma empresa de serviços de pagamento (MSB - *Money Services Business*). Isso coloca-o sob a Lei de Sigilo Bancário (*Bank Secrecy Act* - https://www.fincen.gov/statutes_regs/bsa/), com o que possui certas responsabilidades como emitir relatórios, realizar registros e manter os registros. Além disso, o Estados Unidos classificou a bitcoin como propriedade para fins de tributação pela Receita Federal americana (IRS - *Internal Revenue Service* - https://www.irs.gov/).

Em 07/03/2014, o **Japão** decidiu classificar a bitcoin não como divisa, mas como mercadoria similar aos metais preciosos que não podem ser manuseados pelos bancos japoneses e nem pelas casas de câmbio do país. Explica-se, sendo mercadoria não pode ser trocada em bancos ou casas de câmbio. Referida decisão de regulamentar a bitcoin ocorreu em razão da quebra da Mt.Gox; conhecida casa de câmbio de bitcoin sediada em Tóquio. Dentre as determinações ficou decido que os lucros derivados do mercado online de bitcoins, os processos de compra realizados com a moeda criptografada e as rentabilidades obtidas por empresas nessa moeda seriam tributadas no Japão.

- http://exame.abril.com.br/tecnologia/noticias/japao-reforca-que-bitcoin-nao-e-considerado-moeda.

O japonês Mt. Gox encerrou suas atividades depois do desaparecimento de 388 milhões de dólares em bitcoins. Do mesmo modo, o canadense Flexcoin depois do furto de mais de 600 mil dólares.

- https://tecnoblog.net/152275/mtgox-concordata-japao-bitcoin/.

Depois, em junho de 2014, o governo japonês desistiu da legislação para regulamentar a bitcoin.

- http://www.valor.com.br/internacional/3588818/governo-japones-desiste-de-legislacao-para-regulamentar-o-bitcoin.

Mas, em fevereiro de 2016, o Japão cedeu novamente e declarou estar considerando regulamentar a bitcoin como moeda convencional.

- http://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-eyes-treating-bitcoins-the-same-as-real-money.

E, finalmente, o governo japonês cedeu à tecnologia alheia.

- http://www.hashbtcbrasil.com.br/2016/06/japao-reconhece-oficialmente-o-bitcoin.html;
- https://gracianoconstantino.com/2016/06/16/maior-banco-do-japao-testa-moeda-digital/;
- http://www.timeslive.co.za/scitech/2016/05/26/Japan-regulates-virtual-currency-after-Bitcoin-scandal.

Em 2013, o governo **tailandês**, por meio de membros do comitê de relações internacionais e de departamentos de polícia, decidiu aprovar uma regulamentação proibindo o uso do Bitcoin (protocolo) em território nacional.

- http://g1.globo.com/tecnologia/noticia/2013/07/por-falta-de-lei-especifica-tailandia-proibe-moeda-virtual-bitcoin.html;
- http://www.theverge.com/2013/7/29/4569126/bitcoin-tries-to-become-legal-currency-in-thailand-gets-outlawed.

No dia 23/07/2014, o governo do **Equador** proibiu bitcoin, junto com todas as outras *cryptocurrencies*. Mas, criou sua própria moeda digital.

- https://cryptoid.com.br/banco-de-noticias/equador-proibe-bitcoin-e-cria-sua-propria-moeda-digital/;
- http://www1.folha.uol.com.br/mundo/2014/09/1509563-equador-anuncia-planos-para-criacao-de-moeda-digital.shtml;
- http://bandnewstv.band.uol.com.br/noticias/727525/mundo-equador-anuncia-uso-de-aparelhos-celulares-como-moeda.html.

Em 2014, o **Canadá** se tornou o primeiro país a regular a bitcoin e outras moedas virtuais sob suas leis contra a lavagem de dinheiro (AML - *Anti-*

Money Laundering) e de combate ao financiamento do terrorismo. E, agora, lançou a sua própria moeda digital, o MintChip (https://mintchip.ca/).

- http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/;
- http://www.mnp.ca/en/posts/canada-implements-first-bitcoin-legislation;
- http://veja.abril.com.br/tecnologia/canada-inaugura-primeiro-caixa-automatico-de-bitcoins/;
- http://www.techradar.com/news/internet/bitcoin-atms-ready-to-go-in-canada-only-for-now-1194298;
- http://www.reuters.com/article/us-canada-cenbank-payments-idUSKCN0Z22F9;
- http://www.fastcompany.com/1829662/canada-launch-its-own-version-bitcoin-called-mintchip.

A bitcoin é vista como uma mercadoria pela Agência da Receita do Canadá (CRA - *Canada Revenue Agency* - http://www.cra-arc.gc.ca/). Isto significa que as transações Bitcoins são vistos como escambo operações, e a renda gerada é considerado como o rendimento das empresas. As *exchanges* que trabalham com Bitcoin precisam estar registradas na FINTRAC (*Financial Transactions and Reports Analysis Centre* - http://www.fintrac-canafe.gc.ca/) e devem relatar quaisquer transações suspeitas.

A **Austrália** também manifestou a intenção de regulamentar a bitcoin sob as leis antiterrorismo e de prevenção e combate à lavagem de dinheiro. Mas também prometeu a isenção de dupla tributação através do imposto sobre bens e serviços (GST). Após a decisão de tratar a bitcoin como um ativo intangível, o Senado australiano decidiu tratá-lo como uma moeda regular para fins de Imposto de bens e serviços em razão do grande número de empresas emergentes deixando a Austrália para outros países com regimes mais favoráveis à criptomoeda.

- https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/;
- http://insidebitcoins.com/news/australia-ready-to-treat-bitcoin-as-a-regular-currency/34219;

- http://bitcoinist.net/additional-gst-bitcoin-digital-currencies-australia/;
- https://thestack.com/world/2016/03/21/australia-promises-to-remove-tax-on-bitcoin-support-fintech-innovation/;
- http://www.investopedia.com/articles/investing/032316/bitcoin-will-avoid-double-taxation-australia.asp;
- http://bravenewcoin.com/news/australian-government-committed-to-ending-bitcoin-double-taxation/.

A ilha britânica, **Ilha de Man** ("Isle of Man", em inglês; "Mannin", em manês), em maio de 2016, criou legislação para o uso de bitcoins em casinos on-line.

- https://www.gov.im/lib/news/fsc/virtualcurrencie.xml.

Em novembro de 2013, o Banco Central de **Portugal** (https://www.bportugal.pt/) emitiu um comunicado de imprensa abordando o Bitcoin onde se faz referência a um estudo recente do BCE - Banco Central Europeu (https://www.ecb.europa.eu/ecb/html/index.pt.html). O estudo afirma que o Bitcoin é considerado um modelo de pagamento moeda virtual bidirecional, no qual os utilizadores podem comprar e vender moeda virtual e com o qual eles podem comprar bens e serviços em ambos os mundos real e virtual. O comunicado afirma que por não existir nenhuma autoridade central para garantir a responsabilidade das ordens de pagamento e por não existir nenhuma certeza de sua aceitação como meio de pagamento, a bitcoin não pode ser considerada uma moeda segura. Como a emissão é feita por entidades não reguladas e sem vigilância, não é, portanto, sujeito a quaisquer requisitos prudenciais. O sistema também não está sujeito a qualquer atividade de supervisão. Os utilizadores suportar todo o risco, já que não há fundo para proteger os depositantes/investidores. A bitcoin não tem enquadramento legal específico em Portugal, nem a nível da sua criação ou na sua utilização. Não há direitos claros ou responsabilidades das partes envolvidas no modelo de pagamento. Como se trata dum sistema descentralizado e sem proprietário, é difícil definir a jurisdição sob a qual devem ser estabelecidos procedimentos e regras aplicáveis ao modelo.

No seu relatório, o BCE reconheceu a existência da bitcoin como uma moeda virtual inovadora. No entanto, nem o BCE nem o Banco de Portugal

se responsabilizaram pela emissão ou utilização de bitcoins em Portugal ou na Europa.

- https://www.bportugal.pt/pt-PT/OBancoeoEurosistema/ComunicadoseNotasdeInformacao/Paginas/combp20131219-1.aspx;
- https://www.bportugal.pt/pt-PT/OBancoeoEurosistema/Esclarecimentospublicos/Paginas/meiosdepagamento.aspx;
- https://www.ecb.europa.eu/press/key/date/2016/html/sp160707_1.en.html;
- https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf;
- https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

Detalhe, os portugueses lançaram o CryptoEscudo (https://cryptoescudo.org/).

Antes, ao rigor das normas do Banco Central Europeu, bitcoin não era considerado moeda eletrônica por deixar de preencher alguns dos requisitos exigidos pela diretiva que orienta as transações com e-money, a Electronic Money Directive (2009/110/EC - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF). De acordo com o documento, para ser considerada moeda eletrônica, faz-se necessário que tenha a capacidade de ser armazenada eletronicamente, ser aceita como forma de pagamento por instituições diversas da que a originou e ser emitida com base na recepção de fundos em quantidade não inferior ao valor monetário emitido. As duas condições iniciais estão satisfeitas, ao contrário da última, que conflita com a dinâmica de geração da moeda, denominada “mineração”, que mais se assemelha a uma competição matemática do que a uma operação financeira.

Em 2014 foi noticiado que a França decidiu limitar o anonimato em compra de bitcoins e impor um teto.

- http://www.gazetadopovo.com.br/tecnologia/franca-decide-limitar-anonimato-em-compra-de-bitcoins-e-impor-um-teto-earau6c7h46me5l97ralz8kzy.

Na França, a Frente Nacional, pouco tempo atrás, divulgou a intenção de proibir a bitcoin para impedir que os cidadãos esvaziem as contas bancárias com receio das taxas de juro negativas.

- https://jornalbitcoin.pt/index.php/item/624-frente-nacional-pretende-proibir-bitcoin-em-franca-para-impedir-que-os-cidadaos-esvaziem-as-contas-bancarias-com-receio-das-taxas-de-juro-negativas.

O Banco (central) da **Itália** mostrou-se neutro e aberto aos intermediários bancários que pretendem usar a tecnologia *Blockchain*.

- http://www.ilfoglio.it/economia/2016/06/22/bitcoin-bankitalia-nulla-osta-a-esplorazione___1-v-143527-rubriche_c349.htm.

Em 30/01/2015 o Banco (central) da Itália fez uma declaração oficial sobre as moedas digitais (“valute virtual”), concedendo o uso de criptomoeda como legal dentro do país.

- https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf.

Saiba mais sobre a moeda eletrônica ("criptovaluta elettronica") na Itália em:

- https://www.bitdigital.it/aiuto.html;
- https://bitcoin.org/it/;
- https://www.bitcoin-italia.org/;
- https://github.com/Bitcoin-Foundation-Italia;
- http://faucet.bitcoinclub.eu/italia/;
- http://paymeabit.com/home/top;
- https://coinmap.org/#/world/39.20033382/15.79284668/8;
- https://localbitcoins.com/country/IT;
- https://www.coinbase.com/places/italy.

E na **Comunidade Europeia**, apesar de ainda não existir um entendimento unificado ou uma regulamentação única, cada país aplica seu próprio entendimento, mas a tendência é todos os países do bloco entrarem num consenso sobre a questão. A tendência é que seja aceito, ao menos, como forma de pagamento. Por enquanto já existe a BitcoinETI (https://bitcoineti.com/).

- http://www.dci.com.br/financas/primeiro-produto-regulado-da-europa-de-investimento-em-bitcoin-estreia-em-gibraltar-id563241.html;
- http://www.ibtimes.co.uk/gibraltar-stock-exchange-welcomes-bitcoineti-1572361.

O Tribunal de Justiça da União Europeia, em outubro de 2015, isentou de tributação a compra e venda de bitcoin.

- http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CC0264;
- http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1471683450835&uri=CELEX:62014CJ0264;
- http://www.jornaldenegocios.pt/mercados/cambios/detalhe/bitcoin_nao_paga_imposto_como_as_outras_moedas.html.

A DGT - *Dirección General de Tráfico* (http://www.dgt.es/es/), na Espanha, afirmou que as moedas virtuais, atuando como forma de pagamento, deve ser classificado no domínio das transações financeiras e, conseguinte, ser objeto de isenção de IVA (Imposto de Valor Acrescentado [ou Agregado]), similar ao ICMS (Imposto sobre Circulação de Mercadorias e Serviços) no Brasil.

- http://www.bitchain.eu/en/public-key-certificates/bitcoin-legality/.

O G7 (grupo dos sete países mais industrializados) planejou regulamentar as moedas digitais, com a desculpa de que elas estariam sendo usadas pelo Estado Islâmico para arrecadar fundos.

- https://jornalbitcoin.pt/index.php/noticias/item/291-der-spiegel-grupo-dos-sete-paises-industrializados-planeia-apertar-a-regulamentacao-das-moedas-digitai;

- http://www.spiegel.de/wirtschaft/islamischer-staat-so-finanziert-sich-der-is-a-1063522.html;
- http://shifter.pt/2015/11/europa-em-vias-de-banir-a-circulacao-de-bitcoins/;
- http://www.redetv.uol.com.br/jornalismo/tecnologia/ue-propoe-regras-mais-rigidas-sobre-bitcoin-e-cartoes-pre-pagos-na-luta-con.

De igual forma, a União Europeia possui a preocupação com a questão da segurança e do terrorismo. Tudo culpa dos malditos fanáticos e extremistas religiosos.

- http://www.hashbtcbrasil.com.br/2016/07/uniao-europeia-quer-estabelecer-novas.html;
- http://noticias.uol.com.br/ultimas-noticias/reuters/2016/07/05/ue-propoe-regras-mais-rigidas-sobre-bitcoin-e-cartoes-pre-pagos-na-luta-contra-o-terrorismo.htm;
- http://www.redetv.uol.com.br/jornalismo/tecnologia/ue-propoe-regras-mais-rigidas-sobre-bitcoin-e-cartoes-pre-pagos-na-luta-con;
- https://ec.europa.eu/transparency/regdoc/rep/1/2016/PT/1-2016-50-PT-F1-1.PDF.

Já na **Inglaterra**, após o economista-chefe do Banco central britânico (*Bank of England*) ter proposto a eliminação do dinheiro por uma criptomoeda própria, o Banco central britânico criou uma moeda digital similar a bitcoin, a RSCoin (https://github.com/serokell/rscoin), que será totalmente administrada pelo *Bank of England*.

- https://www.oroyfinanzas.com/2015/09/economista-banco-central-inglaterra-propone-eliminacion-efectivo-dinero-criptomoneda-centralizada/;
- http://criptonoticias.com/opinion/el-banco-de-inglaterra-explica-las-caracteristicas-de-bitcoin/#axzz4Hu6yNo00;
- https://gracianoconstantino.com/2016/07/23/banco-da-inglaterra-instiga-bancos-centrais-a-criarem-as-suas-proprias-moedas-digitais/;
- http://www.telegraph.co.uk/business/2016/03/13/central-banks-beat-bitcoin-at-own-game-with-rival-supercurrency/;
- http://www.cronicasgeek.com/2016/03/banco-inglaterra-prepara-version-del-bitcoin-llamada-rscoin/;

- http://criptonoticias.com/bancos/banco-central-inglaterra-emitir-moneda-digital/#axzz4Hu6yNo00;

- https://www.technologyreview.es/informatica/49614/el-banco-de-inglaterra-encarga-otra-copia-de/.

Através dos exemplos citados, percebe-se que a primeira reação dos governantes ao que lhes era desconhecido, estranho, diferente ou moderno foi de desconfiança, receio, medo e contrariedade. Mas, depois de se inteirarem do assunto, conhecerem melhor e terem realizado uma análise adequada, passaram a estudar as possibilidades que tinham para "não ficarem para trás" e qual dessas hipóteses lhes seria melhor.

Praticamente todo Estado ou governo possui o olhar de cobiça sobre tudo o que possa gerar riqueza ou ser equivalente a dinheiro. Explica-se. O Estado possui um fome insaciável de tributar tudo; ou seja, de arrecadar recursos sobre o trabalho e a fonte alheias. Alguns governos podem até deixar de regulamentar muita coisa, deixando a iniciativa privada ser livre, mas é praticamente impossível de deixar de tributar. Desse modo, as moedas criptográficas representam uma ameaça à arrecadação aos cofres públicos porque muitas pessoas iriam diminuir o recolhimento de tributos ao aderirem a elas. Portanto, mesmo que o Estado não veja nenhum valor, credibilidade, estabilidade, confiança ou segurança nas moedas virtuais, ele enxerga como sendo uma possível forma de sonegação fiscal, evasão de divisas e uma nova fonte de receita.

> "Um dos aspectos essenciais, para regular a moeda refere-se à classificação tributária dada pelo Estado. Essa sistematização é importante tanto no sentido de evitar evasão fiscal quanto, para dar uma noção mais exata ao Estado dos investimentos dos cidadãos. É seguro afirmar, por isso que a positivação de normas tributárias com relação ao dinheiro virtual deve ser prioritária.
>
> A moeda, nesse aspecto, lança questionamentos sobre o Direito de propriedade, pois serve não somente como sistema de pagamento, mas foi classificada pelo Internal Revenue Service dos Estados Unidos (órgão tributário nos Estados Unidos) como uma propriedade (IRS, 2014).

> Da mesma forma, o Canadá também considerou a moeda como propriedade e obrigou as empresas a declararem as vendas efetuadas por meio de bitcoins e os lucros com a especulação da moeda (DESCÔTEAUX, 2014). A maioria dos países provavelmente evitará classificar o bitcoin como dinheiro virtual, devido às consequências desconhecidas de tal ação, preferindo se ater a termos mais seguros, contrariamente ao que foi feito pela Alemanha, que classificou a moeda como dinheiro privado e não como propriedade." (Bitcoin: consequências jurídicas do desenvolvimento da moeda virtual, Gabriela Isa Rosendo Vieira Campos, Revista Brasileira de Direito n.º 11, jul/dez 2015, p. 77/84; *in* https://seer.imed.edu.br/index.php/revistadedireito/article/viewFile/769/719).

O Estado somente deve se intrometer em certas questões quando a iniciativa privada não o faz ou quando está fracassando. Assim, a regra de ouro é a de que o Estado não deve atrapalhar a iniciativa privada quando ela está agindo e obtendo êxito. Mas, muitos governos não pensam assim e, por inveja ou cobiça, acabam atrapalhando a iniciativa privada para forçar a dependência e submissão ao Estado.

Diversos governos mundiais planejam regulamentar o uso da bitcoin, com a desculpa de impedir crimes financeiros. É a velha prática estatal de "crescer o olho" onde está tendo riquezas para poder tributar. Portanto, o real motivo em querer regulamentar o Bitcoin (protocolo), na verdade, se trata do interesse de se apossar da criação alheia, dominá-lo, controlá-lo, lucrar em cima do trabalho de outrem e tributá-lo.

Constata-se pelos exemplos supra que os países estão querendo acompanhar a evolução dos meios de pagamentos, mas sem perderem as rédeas do controle da economia. Desse modo, os bancos centrais estudam criarem e adotarem as suas próprias moedas digitais.

- https://gracianoconstantino.com/2016/07/23/banco-da-inglaterra-instiga-bancos-centrais-a-criarem-as-suas-proprias-moedas-digitais/;
- http://br.wsj.com/articles/SB10976246733703014248504581414453127520000;

- https://jornalbitcoin.pt/index.php/artigos/item/340-bancos-centrais-equacionam-emissao-de-dinheiro-digital.

Se realmente o interesse fosse proteger os investidores, bastava o governo exigir que as empresas que negociam e guardam moedas virtuais tivessem seguro para dar garantia aos clientes.

A *Great American Insurance Group* (http://www.greatamericaninsurancegroup.com/), uma grande companhia de seguros, lançou um seguro para proteger as empresas que trabalham com Bitcoin, reduzindo os prejuízos com roubos de bitcoins. Se empresas como a MtGox ou o MercadoBitcoin tivesse feito um seguro destes, muitos clientes não estariam amargando prejuízos.

- http://www.businesswire.com/news/home/20140602006331/en/Great-American-Insurance-Group-Offer-Bitcoin-Coverage;

- http://www.coindesk.com/great-american-insurance-bitcoin-coverage-businesses/.

A questão da legalidade da bitcoin em cada país, pode ser conferida em https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country.

Além dos governos, existem algumas instituições bancárias que não sabem como se adaptarem ou continuarem lucrando, que acabam por demonizarem as moedas virtuais ou exigirem regulamentação para que não percam sua exclusividade e, assim, poderem continuarem sendo essenciais.

- http://www.spiegel.de/wirtschaft/unternehmen/bitcoin-eu-bankenaufsicht-warnt-vor-virtuellen-waehrungen-a-938797.html.

Porém há outras instituições financeiras que sabem acompanhar a evolução. "Bancos como JP Morgan, *Bank of America*, Citi, *Deutsche Bank*, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, *Royal Bank of Canada* e agora o Itaú, fazem parte de um grupo seleto de bancos globais, com o propósito de discutir e investir na distribuição de tecnologia de cripto moedas." (https://pagamento.me/itau-se-rende-vamos-ao-bitcoin/, postado em 25/04/2016).

- http://m.tecmundo.com.br/mercado/107406-grandes-bancos-efetuam-transacoes-utilizando-bitcoins.htm.

DA REGULAMENTAÇÃO DAS MOEDAS VIRTUAIS

Um dos grandes problemas da bitcoin não é a falta de regulamentação estatal ou do Estado não validar e aceitar as moedas virtuais. O fato de o Estado ser alheio ou indiferente a bitcoin não lhe tira o valor e não pode desrespeitar o negócio feito entre os particulares. Em síntese, a convenção social, os costumes, a tradição e o acordo entre as partes é fonte de direitos e de obrigações. Se o Estado não proibiu é permitido. Assim, por exemplo, se algumas pessoas valorizam e negociam autógrafos, o fato do Estado não regulamentar o autógrafo, e nem considerar o autógrafo uma moeda, não é capaz de mudar a realidade, os fatos e como as coisas são.

Do mesmo modo, se algumas pessoas julgam que fotos possuem valor econômico, se alguém se apodera ilicitamente de foto alheia, o Estado tem a obrigação de proteger a propriedade, mesmo que não veja nenhum valor nela. Aliás, no meio forense é conhecido o caso de uma pessoa que foi processada criminalmente por ter pego algumas garrafas pet vazias no quintal do vizinho. Não é porque determinada coisa, objeto ou bem possa ser vista por outras como não tendo valor, não tendo utilidade nenhuma ou sendo lixo que o Estado irá deixar de proteger a propriedade e de punir os ladrões. O que para uns, e até para muitos, pode ser lixo, pode ser comercializado como peças usadas, sucata ou reciclagem; bem como pode ser transformado por artesões em objetos úteis.

Não é porque uma determinada pessoa, local, cidade ou país possui algo em exagero, que não lhe daria valor por ter demais ou de sobra. Em algum lugar existe pessoas que justamente possuem falta, carência ou extrema necessidade dessa mesma coisa. Assim, num exemplo hipotético, imagine um país que possui areia aos montes e que o território de seu vizinho é formado puramente de rochas. O país sobre as rochas não tem areia e necessita desta para as obras de construção civil e, até mesmo, de terra para poder plantar, já que nas rochas é praticamente impossível o cultivo de qualquer planta. De outro lado, se o país cheio de areia não possui rochas ou pedras, terá carência destas para as obras de construção civil.

Nos tradicionais bazares de garagens nos Estados Unidos ou nas feiras de usados no Brasil, as pessoas vendem justamente aquilo que não lhes

possuem mais nenhum uso, utilidade ou proveito.

Qualquer coisa lícita que tenha tido um custo ou tenha valor para seu dono é merecedora da proteção do direito de propriedade. Desse modo, por exemplos, óleo de cozinha usado, lixo orgânico e, até mesmo, estrume (excremento, fezes), merecem proteção estatal se o proprietário comprou ou se vende. Explica-se. O óleo de cozinha usado pode ser utilizado para fazer sabão, combustível ecológico e outras coisas que podem ser vendidas. O lixo orgânico e o estrume podem ser utilizados para adubar a plantação do proprietário ou fazer adubo e até gás butano para ser vendido; já garrafas plásticas, potes, vidros e pedaços de madeira podem ser utilizados em artesanato e uma infinidade criativa de reaproveitamento. Pneus estragados também são passíveis de reaproveitamento e reciclagem.

Em suma, um local, dependendo de quem está vendo, pode ser um depósito de lixo, um local de reciclagem ou um "ferro velho" (local de venda de peças usadas ou de sucata).

O mesmo não pode ser dito se alguém invade o quintal de uma propriedade privada para "roubar" o ar do lugar; vez que o proprietário do imóvel não pagou pelo ar e nem vende esse ar. Aliás, o ar não é um bem escasso ou raro e, em qualquer lugar do mundo, ninguém paga para poder respirar o ar naturalmente; entretanto é comercializado quando colocado em cilindros para uso subaquático ou purificado para uso hospitalar. De igual forma, a luz solar também é insuscetível de apropriação e, por esse motivo, não é comercializada. As exceções ficam por conta das substituições artificiais de alguns dos efeitos ou utilidades da luz solar: vitamina D, operador de fotossíntese, fonte de energia elétrica, aquecedor, bactericida, etc.

Portanto, não é exatamente tudo o que existe em abundância na natureza que não tem valor econômico ou que não é passível de apropriação. A água, por exemplo, apesar de existir bastante, pode ser captada, armazenada, quantificada, qualificada e comercializada. De igual modo até mesmo a terra em geral, que pode ser usada na fabricação de tijolos, telhas e em artesanatos (vasos, potes, etc.), na argamassa nas construções, em aterramentos de buracos e desnivelamentos, etc.

Na mesma linha de raciocínio, não é tudo que é escasso, raro, que exista pouco ou esteja em extinção, que implique em ter valor ou valer muito. Há de coexistir os requisitos da possibilidade de apropriação, a possibilidade de manuseio e a utilidade ou a beleza. Assim não adianta existir pouco, mas ser impossível, ao menos, de se apossar da coisa e não ter nenhum atrativo ou utilidade para que alguém possa querer tal coisa.

"Coisa" é gênero e "bem" é espécie de coisa. "Coisa" é tudo que existe objetivamente, com exclusão do homem. Quando uma coisa passa a ser objeto de direito, se trata de um "bem". Os bens são coisas, porém, nem todas as coisas são bens. Os bens são coisas úteis ou raras, suscetíveis de apropriação e que contêm valor econômico (pecuniariamente estimado, ou seja, avaliado em dinheiro ou o próprio dinheiro). E, pelo ponto de vista subjetivo, algo pode ser bem para um e não ser para outro.

Em resumo, bens juridicamente protegidos são as coisas úteis, com expressão econômica e suscetíveis de apropriação.

O Protocolo KY trata-se do primeiro protocolo para a regulação da crypto moeda - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2735267.

POSIÇÃO DO BRASIL SOBRE AS MOEDAS VIRTUAIS

A definição jurídica de moeda é aquela definida por lei. A Constituição Federal da República Federativa do Brasil (http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm), no artigo 21, inciso VII, aduz que compete (somente) à União a emissão de moeda. Outrossim, o artigo 164 expõe que somente o Banco Central (Bacen) que realizará tais emissões.

A Lei n.º 9.069 de 1995 (http://www.planalto.gov.br/CCivil_03/leis/L9069.htm) estabelece as regras e condições de emissão da moeda brasileira. Emitir moeda significa editar e colocar em circulação a moeda nacional. Isto significa que a moeda no ordenamento jurídico brasileiro é aquela que é instituída por imposição legal; neste caso, é o Real (Unidade Real de Valor), como determina a Lei n.º 8.880 de 1994 (http://www.planalto.gov.br/CCIVIL_03/leis/L8880.htm).

No Brasil, a moeda eletrônica está prevista na Lei n.º 12.865 de 2013 (http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm), no artigo 6º, inciso VI: Consiste nos "recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento". Contudo, não se confunde com moeda virtual, pois esta possui denominação própria e unidade diversa, e acima de tudo, não é um sistema eletrônico de armazenamento da moeda corrente nacional (no caso o Real). Cabe salientar, ainda, que a emissão de moedas virtuais não é através de uma autoridade governamental. Ou seja, as entidades emissoras destas moedas não reguladas pela autoridade monetária do país. Os próprios usuários destes ativos é que garantem a sua credibilidade.

- http://www.bcb.gov.br/pt-br/Paginas/bc-esclarece-sobre-os-riscos-decorrentes-da-aquisicao-das-chamadas-moedas-virtuais-ou-moedas-criptografadas.aspx.

A Resolução do Bacen, n.º 4.282, de 4 de novembro de 2013, estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento.

- http://www.bcb.gov.br/pre/normativos/res/2013/pdf/res_4282_v1_O.pdf;

- http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=res&ano=2013&numero=42.

Já a Lei nº 9.613, de 3 de março de 1998, versa sobre os crimes de "lavagem" ou ocultação de bens (http://www.planalto.gov.br/ccivil_03/leis/L9613.htm).

Também no Brasil, conforme permissão do Código Civil (http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm), no parágrafo 3º do artigo 889, e, na Lei n.º 9.492/1997 (http://www.planalto.gov.br/ccivil_03/leis/L9492.htm), no parágrafo único do artigo 8º, já existem títulos de crédito (duplicata, nota promissória, cheque, etc.) eletrônicos (meio magnético ou gravação eletrônica de dados) através da utilização de assinatura ou certificados digitais (http://www.iti.gov.br/).

Assim, pela legislação brasileira, a bitcoin e demais moedas virtuais constituem bem móvel incorpóreo que é utilizado na troca de bens e serviços. Por outras palavras, não pode ser considerado como título de crédito eletrônico por não possuir os requisitos de criação e circulação (Código Civil, artigos 887 a 926); muito menos como moeda, já que esta é definida por de lei exclusiva da União.

- História do Dinheiro no Brasil: http://www.bcb.gov.br/htms/album/default.asp?idpai=HISTDIN;

- "É CRÍVEL UMA ECONOMIA MONETÁRIA BASEADA EM BITCOINS?" - http://www12.senado.gov.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td163;

- "INCERTEZAS JURÍDICAS E ECONÔMICAS DA BITCOIN COMO MOEDA" - http://www.publicadireito.com.br/artigos/?cod=1ecccc0718eb6582.

Pela legislação vigente no Brasil, não há nenhuma lei que dê tratamento diferenciado à bitcoin. A Receita Federal do Brasil costuma considerar como rendimento bruto do contribuinte todo o produto do capital, do trabalho ou da combinação de ambos, os alimentos e pensões percebidos em dinheiro, os proventos de qualquer natureza; assim também entendidos os acréscimos patrimoniais não correspondentes aos rendimentos declarados (Lei n º 5.172, de 1966, art. 43, incisos I e II, e Lei n º 7.713, de 1988, art.

3º, § 1º). E, a tributação independe da denominação dos rendimentos, títulos ou direitos, da localização, condição jurídica ou nacionalidade da fonte, da origem dos bens produtores da renda e da forma de percepção das rendas ou proventos, bastando, para a incidência do imposto, o benefício do contribuinte por qualquer forma e a qualquer título (Lei n º 7.713, de 1988, art. 3º, § 4º). Ainda mais, são também tributáveis (Lei n.º 4.506, de 1964, art. 26, Lei n º 7.713, de 1988, art. 3º, § 4º, e Lei n.º 9.430, de 1996, arts. 24, § 2º, inciso IV, e 70, § 3º, inciso I) os rendimentos derivados de atividades ou transações ilícitas ou percebidos com infração à lei, independentemente das sanções que couberem. Ora, se até atividades ilícitas são tributáveis, e o mercado Bitcoin, em sentido oposto, é uma atividade plenamente lícita, então os recursos nessa moeda devem ser declarados pelo titular no ajuste anual de Rendimentos.

- Lei n º 5.172/1966 - http://www.planalto.gov.br/ccivil_03/leis/L5172.htm;
- Lei n º 7.713/1988 - http://www.planalto.gov.br/ccivil_03/leis/L7713.htm;
- Lei n.º 4.506/1964 - http://www.planalto.gov.br/ccivil_03/leis/L4506.htm;
- Lei n.º 9.430/1996 - http://www.planalto.gov.br/ccivil_03/leis/L9430.htm.

Saiba mais sobre a regulamentação do Imposto de Renda no Brasil em:

- http://exame.abril.com.br/seu-dinheiro/noticias/ate-bitcoin-deve-ser-declarada-no-imposto-de-renda;
- http://idg.receita.fazenda.gov.br/acesso-rapido/tributos/irpf-imposto-de-renda-pessoa-fisica;
- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/declaracao-de-ajuste-anual-irpf;
- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/ajuste-anual;
- http://idg.receita.fazenda.gov.br/acesso-rapido/legislacao/legislacao-por-assunto/Ganhos-de-capital;
- http://idg.receita.fazenda.gov.br/orientacao/tributaria/pagamentos-e-parcelamentos/pagamento-do-imposto-de-renda-de-pessoa-fisica/ganho-de-capital/ganhos-de-capital.

Assim, ela (bitcoin) é considerada um bem, da mesma forma que uma obra de arte, por exemplo. Quem possui mil reais ou mais em bitcoins, deve incluí-los na seção “outros bens” da declaração de imposto de renda. Por não existir uma cotação oficial (governamental, disciplinada por lei ou acordada entre governos ou entidades internacionais) da bitcoin, estes incluídos em “outros bens” podem ter seu valor calculado considerando-se a cotação de uma bolsa, como o Mercado Bitcoin (https://www.mercadobitcoin.com.br/), no Brasil, ou Bitstamp, na Europa. O valor a declarar por cada unidade, deve ser o valor de 31/12 do ano anterior. Mas isso não quer dizer que inexista cotação de bitcoin.

- PL - Projeto de Lei n.º 2303/2015 coloca Bitcoin sob a supervisão do Banco Central - http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470;
- O texto da proposição encontra-se em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1358969&filename=Tramitacao-PL+2303/2015;
- European Central Bank - virtual currency schemes - october 2012 - https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

O projeto enquadraria a bitcoin nas regras da Lei n.º 12.865, de 09 de outubro de 2013, artigos 6º ao 15 (http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm) e sob as regras do CDC - Código de Defesa do Consumidor (http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm).

O Bacen, em 19/02/2014, emitiu esclarecimento sobre os riscos decorrentes da aquisição das chamadas “moedas virtuais” ou “moedas criptografadas”.

- http://www.bcb.gov.br/pt-br/Paginas/bc-esclarece-sobre-os-riscos-decorrentes-da-aquisicao-das-chamadas-moedas-virtuais-ou-moedas-criptografadas.aspx.

O Bacen emitiu o Comunicado nº 25.306, de 19/02/2014 (https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277), tecendo esclarecimentos “sobre os riscos decorrentes da aquisição das chamadas moedas virtuais ou moedas criptografadas e da realização de transações com elas.”.

Em resumo, o **Comunicado nº 25.306/2014**:

a) Diferenciou as criptomoedas das moedas eletrônicas, esclarecendo que estas últimas "são recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento denominada em moeda nacional" (e reguladas pela lei nº 12.865/13) ou passo que as criptomoedas "possuem forma própria de denominação, ou seja, são denominadas em unidade de conta distinta das moedas emitidas por governos soberanos, e não se caracterizam dispositivo ou sistema eletrônico para armazenamento em reais";

b) Alertou para o fato de que as criptomoedas não são emitidas nem garantidas por uma autoridade monetária, não têm garantia de conversão para a moeda oficial, tampouco são garantidos por ativo real de qualquer espécie;

c) Informou que não há mecanismo governamental que garanta o valor em moeda oficial;

d) Alertou que pode haver grande variação dos preços das criptomoedas, até mesmo a perda total do seu valor;

e) Informou que seu uso em atividades ilícitas pode ensejar investigações pelas autoridades públicas, as quais poderá envolver o usuário destas, ainda que imbuídos de boa-fé;

f) Alertou que o armazenamento das criptomoedas pode representar risco de perda porque as carteiras digitais não estão imunes vulnerabilidades tecnológicas e respectivos ataques;

g) Informou que o uso das criptomoedas no país ainda não se mostra suficientemente perigoso para oferecer riscos ao Sistema Financeiro Nacional, particularmente quanto às transações de pagamentos de varejo (art. 6º, § 4º, da Lei nº 12.685/2013);

h) Esclareceu, ao final, que o Bacen tem acompanhado a evolução da utilização das criptomoedas para fins de adoção de eventuais medidas no âmbito de sua competência legal, se for o caso.

No Brasil, em 18/11/2015 (https://www.youtube.com/watch?v=Je-r7sw5Xkg), Antonio Gustavo Rodrigues, presidente do COAF (Conselho de Controle de Atividades Financeiras), disse ser contra a regulamentação do mercado de meios de pagamentos virtuais, entre eles o Bitcoin. Que ao se dar qualquer ar de regulação a esse produto, começa-se a dar a proteção do Estado para esse produto, o que acaba podendo transmitir a sensação de que ele é um produto seguro, mas não é; pois há o risco de o dinheiro sumir. As moedas virtuais são feitas para não serem controladas pelo Estado, o que atrai criminosos e não tem nenhuma autoridade que garanta que aquela moeda vai estar lá na hora que ela precisar ser usada.

"A despeito de não terem sido especificamente regulados pelas autoridades competentes do mercado financeiro e de capitais, os bitcoins poderão vir a ser alvo de regulamentação específica do Conselho Monetário Nacional e/ou do Banco Central (em especial na medida em que passem a representar risco sistêmico relevante ao Sistema Financeiro Nacional) e/ou da Comissão de Valores Mobiliários (em especial na medida em que atinjam um grande público de poupadores/investidores) e/ou das autoridades criminais (preocupadas, sobretudo, com lavagem de dinheiro) e/ou de outras autoridades que, em sua respectiva esfera de competência, busquem identificar riscos e criar instrumentos legais para mitigá-los. Isto sem prejuízo do interesse das autoridades fiscais (sempre buscando identificar novas fontes de captação)." (Bitcoins podem ser alvo de regulamentação específica de CMN, BC ou CVM; Bruno Balduccini, Rosine Kadamani e Leonardo Baracat Bedicks, 07/02/2015, *in* http://www.conjur.com.br/2015-fev-07/bitcoins-podem-alvo-regulamentacao-especifica-bc-ou-cvm).

NATUREZA JURÍDICA DA BITCOIN NO BRASIL

A bitcoin (moeda) é um bem (confira supra a definição de bem), incorpóreo (imaterial), móvel (passível de movimentação ou transferência de lugar), fungível (pode ser substituído ou restituído por outro igual na mesma medida), inconsumível (não se destrói com o uso, mas continua existindo), singular (individualizado ou unidade independente), divisível (comporta desmembramento), principal (existe por si só, não sendo acessório, dependente ou componente de outro bem), particular (iniciativa privada) e alienável (negociável ou comerciável).

Qualificar a bitcoin como um ativo semelhante às moedas ou aos metais preciosos (comódites) é essencial porque nos permite entender melhor a sua natureza e suas propriedades, além de conduzir a uma correta metodologia de avaliação de valor.

A Convenção de Palermo, internalizada para legislação pátria por meio do Decreto nº. 5.015, de 12 de março de 2004, artigo 2, d, dispõe que bens são: "os ativos de qualquer tipo, corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis, e os documentos ou instrumentos jurídicos que atestem a propriedade ou outros direitos sobre os referidos ativos.".

- Decreto nº. 5.015/2004 - http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5015.htm.

A bitcoin, pela ótica jurídica brasileira, é um bem móvel incorpóreo que é utilizado na troca de bens e serviços. Não deve ser considerado como um título de crédito eletrônico, pois não possui os seus requisitos de criação e circulação (Código Civil, artigos 887 a 926); muito menos como moeda, pois a moeda, em cada jurisdição, é definida por força de lei, sendo de prerrogativa exclusiva da União.

- Código Civil - https://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

Segundo o *Commodity Exchange Act* dos Estados Unidos, *commodity* pode ser basicamente qualquer produto ou artigo. Ou, traduzindo para a nossa própria língua, *commodity* é simplesmente uma mercadoria. Nessa

definição, não haveria problema algum em classificar a bitcoin como uma mercadoria; embora digital, incorpórea.

E, nessa classificação, a bitcoin compartilha muitas das propriedades encontradas em outra *commodity*, o ouro. Este, por sinal, foi moeda durante milênios (em ambos os sentidos do termo, econômico e legal), mas hoje não passa de um ativo de proteção (seu uso como meio de troca é virtualmente inexistente).

Dentre as características comuns às duas comódites (bitcoin e ouro), podemos destacar a escassez relativa; ambos apresentam uma oferta limitada derivada das leis da matemática e da natureza.

Durante grande parte da história mundial, o ouro foi o dinheiro empregado amplamente pelo mercado; uma mercadoria que passou a ser empregada como meio de troca, ganhando cada vez mais liquidez, em um processo que se retroalimenta, até atingir o estágio de moeda, o meio de troca universalmente aceito. Segundo o economista Ludwig Von Mises, quando circulava como meio de troca no mercado, o ouro era classificado como dinheiro *commodity*, ou dinheiro mercadoria. Se o ouro foi dinheiro *commodity*, podemos considerar a bitcoin hoje como um dinheiro *commodity* digital.

Mas a bitcoin não é uma *commodity* da natureza como ouro, prata, minério de ferro, soja, arroz, algodão, milho, etc. Tampouco é uma moeda nacional emitida por alguma jurisdição. Então, que espécie de ativo seria a bitcoin?

Do ponto de vista legal, bitcoins já foram definidas como “unidade de conta” ou “uma forma de dinheiro”, na Alemanha; como moeda, no Reino Unido, para certos fins fiscais; e como propriedade ou mercadoria pelo *Internal Revenue Service* (similar à Receita Federal) dos EUA (Estados Unidos). No Brasil não houve, até a presente data, nenhuma menção específica quanto à classificação da bitcoin. Para o Fisco brasileiro, bitcoin é simplesmente uma mercadoria.

POR QUE A BITCOIN SERIA UMA COMÓDITE?

Muitas pessoas, ou por não entenderem as criptomoedas, ou em razão de legislações locais, ou por motivos escusos, entendem que a bitcoin não seria uma moeda e, portanto, seria uma mercadoria. Por outras palavras, a consideração da bitcoin como mercadoria é o entendimento de que ela não se enquadra no conceito ou definição de moeda.

Comódite (*commoditie* ou *comodity*) é qualquer bem em estado bruto ou primário, geralmente de origem agropecuária ou de extração mineral ou vegetal, produzido em massa (em larga escala mundial) e com características físicas homogêneas, que funciona como matéria-prima e que pode ser estocado sem perda de qualidade, destinado ao comércio externo e cujo preço é determinado pela oferta e procura internacional. A palavra inglesa *commodity* significa mercadoria.

Pode-se argumentar que existem alguns casos de uso "intrínseco" para a bitcoin: resistência contra a "censura" ou prova de existência de pagamentos online, que dão o valor de comódite (*commodity*) digital fora do seu uso como dinheiro. Estas propriedades da bitcoin que lhe assemelham à comódite são o que atrai as pessoas à bitcoin em um primeiro momento, e muitos destes indivíduos decidem comprar algumas poucas moedas como economia ou como reserva de valor; ou seja: comprando e esperando valorizar, para depois revendê-las.

Em 2013, Trendon Shavers, o fundador do Bitcoin Savings & Trust (BTCST), um fundo de investimento on-line, foi acusado de fraudar seus clientes no valor de US $ 4,5 milhões em bitcoins. Shavers prometeu aos investidores um retorno semanal incrível de 7 por cento, de acordo com uma queixa criminal federal, mas fechou seu site após recolher mais de 700.000 bitcoins. Quando a SEC - *Securities and Exchange Commission* (https://www.sec.gov/) acusou o Shavers de esquema ilegal de pirâmide, sua resposta foi que a bitcoin não era moeda real e, portanto, suas ações não estavam abrangidas pela regulamentação da SEC. Mas o juiz Amos Mazzant, do Distrito Leste do Texas, decidiu que a SEC poderia prosseguir com a sua ação judicial contra Shavers porque "Bitcoin é uma moeda ou forma de dinheiro." Mais recentemente, em agosto de 2014, outro juiz federal,

Katherine Forrest, do Tribunal Distrital dos Estados Unidos para o Distrito Sul de Nova York, entendeu que os estatutos federais de crime de lavagem de dinheiro "englobam uso de Bitcoin" e que "qualquer outra leitura" da lei seria "sem sentido".

Entretanto, a CFTC - *Commodity Futures Trading Commission* (http://www.cftc.gov/), órgão que regula o mercado de comódites dos Estados Unidos, definiu que a moeda virtual é oficialmente uma comódite, assim como petróleo, trigo e soja.

- http://www.cftc.gov/PressRoom/PressReleases/pr7231-15.

A moeda virtual é, também, tratada como propriedade pela Receita Federal americana (IRS - *Internal Revenue Services*) para fins tributários (https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance).

Investir em comódites requer uma boa dose de análise do mercado para saber identificar os momentos em que a oferta e a demanda estejam em desequilíbrio e aproveitar excelentes oportunidades de negociação. Assim, por exemplo, no caso de comódites como minério de ferro, soja, petróleo, etc., basta entender como se comportarão os produtores (ofertantes) e os consumidores (os demandantes), para estimar o preço futuro. Entretanto, com o ouro, a tarefa não é tão simples; vez que ao contrário das comódites que são produzidas e consumidas, quem adquire o metal precioso não o consome; na verdade, o entesoura. Embora haja aplicação industrial, a maior parte da demanda do ouro advém de seu uso como bem monetário, como ativo de proteção. Isso significa que o estoque de ouro produzido em um ano não é extinto ao contrário, por exemplo, do minério de ferro, que é consumido e transformado em outros produtos. Na verdade, o ouro circula de investidor para investidor, fazendo parte do encaixe financeiro destes. Desse modo, prever o preço de uma comódite como o ouro exige não somente compreender a evolução da oferta originada pelos grandes mineradores ao redor do globo, mas também imaginar como evoluirá a demanda desse ativo (para fins de proteção e investimento) pelos indivíduos.

A metodologia para precificar as moedas não é muito diferente. Dinheiro é o único bem que não é consumido e tampouco serve para produzir outros bens; não é um bem de consumo, nem um bem de produção. É dinheiro, é um meio de troca. Ninguém adquire moeda para consumi-la. A moeda é adquirida para ser trocada posteriormente por bens, sejam eles de consumo, sejam de produção.

Porém, a lei de oferta e demanda é inexorável, e atua igualmente sobre qualquer mercadoria, até mesmo a moeda, que também é um bem, com a particularidade de ser o bem mais líquido no mercado. Isso significa que, tudo o mais constante, quando aumenta a oferta da quantidade de uma moeda, o seu preço diminui. Dito de outra forma, quanto mais aumenta a quantidade de dinheiro em circulação, menor tende a ser o poder de compra de cada unidade monetária. Desse modo, a moeda perde valor.

Prever o valor de uma moeda em relação à outra (câmbio) é uma das tarefas mais intrincadas do mercado financeiro. É preciso ponderar como será a política monetária dos bancos centrais e é imprescindível considerar como se comportará a demanda por uma moeda pelos agentes de mercado. Para uma moeda ganhar poder de compra (apreciar-se), não basta uma política monetária relativamente mais rígida se sua demanda despencar. Da mesma forma, uma política monetária frouxa e expansionista não necessariamente irá causar a depreciação do dólar, por exemplo, se a demanda pela moeda norte-americana seguir aumentando. Porém, é certo que, no longo prazo, aquelas moedas que foram relativamente mais inflacionadas que as demais acabarão se desvalorizando inevitavelmente. Essa metodologia de avaliação de comódites monetárias e moedas é precisamente a que se deve empregar ao buscar o valor justo (*fair value*) da bitcoin.

POR QUE A BITCOIN É UMA MOEDA?

Uma vez que a bitcoin esteja na mão de bilhões de pessoas, e que uma vasta maioria de comerciantes o aceite como pagamento, então poderia fazer sentido que eventualmente se precificassem bens e serviços em bitcoins, ao invés de moedas FIAT. A taxa de câmbio da bitcoin é simplesmente muito volátil (instável) para que este "ativo digital" seja usado como uma unidade de conta no momento, mas a estabilidade do preço tem melhorando com o passar do tempo. A utilização da bitcoin como uma unidade de conta, seria o seu último passo antes que este pudesse ser considerada moeda.

A bitcoin possui praticamente todas as **características das moedas estatais** que já conhecemos e usamos:

- **Possuível**. Um elemento essencial da moeda é ser suscetível de posse e a bitcoin é baseada justamente na posse.

- **Portabilidade ou transportabilidade**. A bitcoin é portátil através de várias formas: distribuição eletrônica, smartphones, tablets, pendrives, carteiras de papel, etc. Por outras palavras, é possível armazenar as bitcoins em qualquer dispositivo eletrônico capaz de armazenar dados.

- **Fungibilidade**. A bitcoin é completamente intercambiável (fungível) com outra unidade do mesmo dinheiro.

- **Reserva de valor**. O FMI - Fundo Monetário Internacional (parte do Banco Mundial) define o dinheiro em geral como uma "reserva de valor"; o que significa que as pessoas podem guardá-lo e usá-lo depois. Desse modo, bitcoins podem guardadas com intuito de economizar e juntar uma grande quantia para que no futuro, possam ser trocadas por alguma coisa que precise ou simplesmente goste.

- **Divisibilidade**. A bitcoin pode ser divisível em partes muito pequenas. Enquanto que as moedas convencionais possuem

apenas 2 casas decimais (ex. R$ 2,10), a bitcoin possui 8 (oito) casas decimais (exemplo BTC 0,00000001).

- **Durabilidade**. Enquanto que as moedas fiat não são duráveis, a bitcoin por consistir em dados digitais é impossível que sofra desgaste ou deteriorização; vez que é imaterial. Ainda mais, por ser suscetível de *back-ups* (cópias de segurança), ainda que o local original onde esteja guardada sofra algum dano, poderá ser recuperada pelo *back*-up. Inclusive, à medida que as pessoas se familiarizem mais com referida tecnologia, cada vez mais diminui a probabilidade de perda acidental de bitcoins.

- **Indestrutibilidade**. Apesar da grande semelhança, durabilidade e indestrutibilidade não são sinônimos. A bitcoin não pode ser destruída ou excluída da rede. Uma vez criada (minerada). A única forma de inutilizar uma bitcoin, é guardá-la em uma carteira (*wallet*) e jogar sua chave privada fora para sempre.

- **Facilmente identificável**. Em razão de ser totalmente original, é facilmente identificável e praticamente impossível de falsificar. O mesmo não pode ser dito de moedas fiat convencionais.

Saiba mais no capítulo "REQUISITOS DE VIABILIDADE DA MOEDA".

O que faz dinheiro é o que se pode fazer com ele. Se pudermos comprar bens e serviços com ele, é dinheiro; se não pudermos, não é.

Ainda mais, se as partes envolvidas concordam que determinado produto ou serviço será pago por meio de bitcoins e não em moeda corrente, trata-se de um contrato entre elas, com plena validade legal.

> "A moeda é uma convenção social. Tudo aquilo que é geralmente aceito pelo público em pagamento de bens, serviços e ativos de valor, e no reembolso de dívidas, é convencionalmente conhecido por moeda [...] Em sua origem, moeda é apenas mercadoria aceita mais facilmente

> que outras, nas trocas; quando o governo se encarrega da operação de amoedagem, ela perde qualquer caráter de instrumento privado e facultativo, e torna-se "moeda pública" de "curso forçado" (aceitação imposta). Tem "curso legal" (credores e vendedores são obrigados a aceitá-la em pagamento de seus créditos e mercadorias), e "poder liberatório" (o devedor, ao entregá-la ao credor, liberta-se de sua dívida). Se outras sociedades a aceitam, em troca de sua moeda, torna-se conversível. E, se ganha foro de aceitação generalizada, torna-se moeda de reserva." (Mercado de capitais, Luiz Fernando Rudge e Francisco Cavalcante, CNBV - Comissão Nacional de Bolsa de Valores, 1998, 4ª edição, revista e atualizada, página 25).

Mas pelas regras da União Europeia, a bitcoin é uma moeda, não uma mercadoria virtual. Suíça, Espanha, Finlândia, Bélgica e outros países europeus declararam que bitcoin é isenta de valor agregado (IVA), o tributo equivalente ao ICMS (Imposto sobre Circulação de Mercadorias e Serviços) no Brasil.

O Tribunal de Justiça Europeu (ECJ - *European Court of Justice*: http://curia.europa.eu/jcms/jcms/j_6/pt/), no processo C-264/14 do sueco David Hedqvist, decidiu que Bitcoin operações de câmbio devem ser isentos de IVA - Imposto sobre o Valor Acrescentado (tributo similar ao ICMS no Brasil).

- http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=503587;
- http://curia.europa.eu/juris/document/document.jsf?text=&docid=165919&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=503587;
- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62014CN0264:EN:PDF.

O FinCEN - *Financial Crimes Enforcement Network* (https://www.fincen.gov/) também trata bitcoin como moeda; considera que é "um meio de troca, que funciona como uma moeda em alguns ambientes."

DO ASPECTO CRIMINAL NO BRASIL

A **elisão fiscal** (economia legal ou planejamento tributário) tem o objetivo de diminuir ou eliminar a incidência de tributos através de previsão expressa, lacunas e brechas existentes na lei. Por outras palavras, é uma atuação preventiva dentro da lei para evitar e/ou reduzir a tributação. A **evasão fiscal**, por sua vez, utiliza-se de meios ilícitos para evitar o pagamento de tributos; ou seja, não é mera inadimplência e nem simples fuga, mas o emprego de fraudes, simulações, mentiras e/ou omissão na confecção e/ou entrega de livros, registros, informes e demais documentos aos entes públicos. Portanto, **evasão é sonegação**!

Outra diferenciação, a **mera inadimplência fiscal não é delito penal** (crime ou contravenção), ocasionado apenas a aplicação das penalidades administrativas cabíveis e a inscrição do débito em dívida ativa para fins de ser promovida a execução fiscal pela Fazenda Pública. Por outras palavras, se a lei não define como crime, será mera inadimplência.

O Código Penal (http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm) no artigo 334-A define o crime de **contrabando** (importar ou exportar mercadoria proibida). Equipara-se às atividades comerciais, para os efeitos deste crime, qualquer forma de comércio irregular ou clandestino de mercadorias estrangeiras, inclusive o exercido em residências; bem como incorre na mesma pena do crime de contrabando quem:

> "I - pratica fato assimilado, em lei especial, a contrabando;
> II - importa ou exporta clandestinamente mercadoria que dependa de registro, análise ou autorização de órgão público competente;
> III - reinsere no território nacional mercadoria brasileira destinada à exportação;
> IV - vende, expõe à venda, mantém em depósito ou, de qualquer forma, utiliza em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria proibida pela lei brasileira;
> V - adquire, recebe ou oculta, em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria proibida pela lei brasileira."

Já no artigo 334, o Código Penal versa sobre o crime de **descaminho**: iludir, no todo ou em parte, o pagamento de direito ou imposto devido pela entrada, pela saída ou pelo consumo de mercadoria. Equipara-se às atividades comerciais, para os efeitos deste crime, qualquer forma de comércio irregular ou clandestino de mercadorias estrangeiras, inclusive o exercido em residências. Incorre na mesma pena quem:

> "I - pratica navegação de cabotagem, fora dos casos permitidos em lei;
> II - pratica fato assimilado, em lei especial, a descaminho;
> III - vende, expõe à venda, mantém em depósito ou, de qualquer forma, utiliza em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria de procedência estrangeira que introduziu clandestinamente no País ou importou fraudulentamente ou que sabe ser produto de introdução clandestina no território nacional ou de importação fraudulenta por parte de outrem;
> IV - adquire, recebe ou oculta, em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria de procedência estrangeira, desacompanhada de documentação legal ou acompanhada de documentos que sabe serem falsos."

O Código Penal (http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm), no Título X, tece algumas disposições sobre os crimes praticados contra a fé pública, em especial sobre os crimes de moeda falsa (Capítulo I), onde constam os crimes de moeda falsa e assimilados (CP, artigos 289 e 290), petrechos para falsificação de moeda (CP, artigo 291) e, ainda, emissão de título ao portador sem permissão legal (CP, artigo 292).

O **crime de moeda falsa** (CP, artigo 289) versa sobre falsificar (seja fabricando, adulterando ou autorizando a emissão) moeda metálica ou papel-moeda de curso legal no país ou no estrangeiro; bem como, importar, exportar, adquirir, vender, trocar, ceder, emprestar, guardar ou introduzir na circulação moeda falsa. Também se aplica ao caso de desviar e fazer circular moeda, cuja circulação ainda não estava autorizada. Portanto nenhuma das previsões se aplica às moedas criptográficas, vez que não são metálicas, não são em forma de cédulas e nem são de curso legal (moeda oficial e obrigatória) de nenhum país, mas, pelo contrário, constituem

dinheiro totalmente privado ou particular. Do mesmo modo em relação ao **crime de petrechos para falsificação de moeda** (CP, artigo 291), se tratar apenas de geração de criptomoedas, também não haverá crime nenhum; vez que a previsão legal do ato criminoso é fabricar, adquirir, fornecer, a título oneroso ou gratuito, possuir ou guardar maquinismo, aparelho, instrumento ou qualquer objeto especialmente destinado à falsificação de moeda (CP, artigo 289). Por outras palavras, os equipamentos destinados à mineração das moedas digitais não constituem os petrechos para a falsificação de moeda.

Os **crimes assimilados ao de moeda falsa** (CP, artigo 290) consistem no ato de formar cédula, nota ou bilhete representativo de moeda com fragmentos de cédulas, notas ou bilhetes verdadeiros; suprimir, em nota, cédula ou bilhete recolhidos, para o fim de restituí-los à circulação, sinal indicativo de sua inutilização; restituir à circulação cédula, nota ou bilhete em tais condições, ou já recolhidos para o fim de inutilização. Inaplicável, também, às moedas digitais por dedução lógica.

Por fim, o **crime de emissão de título ao portador sem permissão legal** (CP, artigo 292) consiste no ato de emitir, sem permissão legal, nota, bilhete, ficha, vale ou título que contenha promessa de pagamento em dinheiro ao portador ou a que falte indicação do nome da pessoa a quem deva ser pago. Sendo prevista punição também para quem recebe ou utiliza como dinheiro qualquer dos documentos referidos. O objeto jurídico desse crime é a proteção da fé pública. Para a configuração do crime é necessário que o documento ou título tenha a finalidade de circular como dinheiro e o agente tenha conhecimento da inexistência da permissão legal. A consumação do crime ocorre com a introdução do documento na circulação; ou seja, quando o agente entrega, ou tenta entregar, o documento a outrem (tomador ou portador) como forma de pagamento.

O crime de emissão de título ao portador sem permissão legal é semelhante ao crime de falsificação de moeda, mas trata-se de falsificação de título de crédito. Por óbvio o crime acima envolve a premissa de que existem títulos que a lei exigem autorização para sua emissão; mas, também, existem inúmeros títulos, tais como, por exemplo, a confissão de dívida, que pode ser emitida sem nenhuma formalidade ou burocracia por qualquer

pessoa e pode ser colocada em circulação (“passar para frente”, transferir os direitos de créditos para outrem ou utilizar o próprio documento como se fosse dinheiro e, assim, usá-lo como forma de pagamento com terceiro, que fará o mesmo ou cobrará o devedor constante do documento). Por outras palavras, se não existe lei prescrevendo que somente determinadas pessoas podem emitir determinado título de crédito, todos podem emitir referido título de crédito. É direito constitucional que tudo aquilo que não for especificadamente proibido, é permitido. Ainda mais, como referida previsão legal do Código Penal (CP) visa proteger a fé pública, por dedução lógica não pode ser aplicado às moedas criptográficas porque elas não possuem fé pública, vez que não são de curso legal (moeda oficial e obrigatória) e nem constituem nenhum título de crédito previsto em lei.

A título de esclarecimento, o **endosso** (ou título à ordem; CC - Código Civil [http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm], artigos 910 a 920, 923, § 2º do 785 e 890) é uma das formas de transmissão da posse ou dos direitos creditícios de um título de crédito, através da qual o credor (detentor do direito de receber) original assina no próprio documento (seja na frente [dorso ou anverso] ou no verso [atrás]), podendo indicar (endosso em preto ou pleno), ou não (endosso em branco ou incompleto), quem é o novo beneficiário do crédito (valor). Mas o endossante (credor original do título que fez o endosso) é co-responsável (devedor solidário) pelo pagamento ao novo portador ou credor do título (endossatário), tanto com o devedor original como dos endossantes anteriores a ele. O endosso é comumente realizado em títulos de crédito (documentos formais, portanto) onde consta a expressão "à sua ordem", que significa que possui a característica de circulação autorizando ao portador endossá-lo; já os títulos de crédito que usam a expressão "não à sua ordem" não admitem endosso. Portanto, o endosso não é só uma forma de fazer circular um título de crédito; ou seja, não só transfere o benefício do título de crédito, mas também a sua portabilidade e responsabilidade, não pode haver endosso parcial (endosso transfere o crédito, mas impõe a responsabilidade aos endossantes). Caso o credor originário do título não queira ser co-responsável pelo mesmo ou no caso de o título de crédito ser "não à sua ordem", pode-se utilizar-se do instrumento (contrato) da **cessão de crédito** (Código Civil, artigos 221, 286 a 298, 347, 348, 377, 497, 498, 919, 1.451, 1.793 e 1.795), o qual trata-se de uma transferência ordinária (comum ou

simples) de crédito apenas; onde o cedente (credor original a quem pertence a titularidade do título de crédito), transfere o crédito (total ou parcial) ao cessionário (adquirente do crédito), que deverá ser pago pelo cedido (devedor original constante do título de crédito). Portanto, a cessão de crédito é um documento separado do título de crédito que transfere apenas o direito de crédito (parcial ou total), sem qualquer responsabilidade ou garantia pelo cedente; exceto pela existência do crédito, mas não pelo seu pagamento pelo cedido. De modo similar, numa **cessão de contrato** uma das partes contratantes cede (transfere ou vende) a sua posição contratual (todos os direitos e todos os deveres) a um terceiro. Entretanto, dependendo do tipo de contrato e da posição (contratante ou contratado) no mesmo, pode não ser permitido (exemplo, seguro de vida: Código Civil, artigo 785) ou, caso seja, pode ser exigida a aprovação da outra parte para a substituição; por exemplo, em contratos de financiamentos, como é pré-requisito o contratante ser submetido à uma análise de crédito e de até fornecer uma garantia, por óbvio não pode o devedor originário repassar sua dívida para alguém que não condições de pagá-la. E, em outros casos, pode ser exigida por lei determinada formalidade ou burocracia, como, por exemplo, em questão de cotas de empresas (Código Civil, artigos 221, 288, 1.003 e 1.057).

Ainda mais, o CPC - Código de Processo Civil (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm), no artigo 783 prescreve que são **títulos executivos extrajudiciais**:

> "I - a letra de câmbio, a nota promissória, a duplicata, a debênture e o cheque;
> II - a escritura pública ou outro documento público assinado pelo devedor;
> III - o documento particular assinado pelo devedor e por 2 (duas) testemunhas;
> IV - o instrumento de transação referendado pelo Ministério Público, pela Defensoria Pública, pela Advocacia Pública, pelos advogados dos transatores ou por conciliador ou mediador credenciado por tribunal;
> V - o contrato garantido por hipoteca, penhor, anticrese ou outro direito real de garantia e aquele garantido por caução;
> VI - o contrato de seguro de vida em caso de morte;

VII - o crédito decorrente de foro e laudêmio;

VIII - o crédito, documentalmente comprovado, decorrente de aluguel de imóvel, bem como de encargos acessórios, tais como taxas e despesas de condomínio;

IX - a certidão de dívida ativa da Fazenda Pública da União, dos Estados, do Distrito Federal e dos Municípios, correspondente aos créditos inscritos na forma da lei;

X - o crédito referente às contribuições ordinárias ou extraordinárias de condomínio edilício, previstas na respectiva convenção ou aprovadas em assembleia geral, desde que documentalmente comprovadas;

XI - a certidão expedida por serventia notarial ou de registro relativa a valores de emolumentos e demais despesas devidas pelos atos por ela praticados, fixados nas tabelas estabelecidas em lei;

XII - todos os demais títulos aos quais, por disposição expressa, a lei atribuir força executiva."

Constata-se, assim, que não constam as moedas criptográficas como sendo uma das espécies de títulos de crédito; razão pela qual não é possível configurar o crime de emissão de título ao portador sem permissão legal. Poder-se-ia dizer que a moeda digital é um instrumento particular de crédito (CC - Código Civil, artigos 104, 107, 112, 212, 219 e 221; CPC - Código de Processo Civil, artigos 408 e 412), mas conforme consta do CPC, artigo 783, inciso III, exige-se a assinatura de duas testemunhas. E, mesmo que surja uma altcoin que preencha esse requisito de constar a assinatura de duas testemunhas (o qual também é normalmente necessário em contratos), ainda assim não estaria configurado o crime de emissão de título ao portador sem permissão legal.

De modo semelhante, o Código Civil - Lei n.º 10.406/2002 (http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm), no artigo 887 reza que: "O título de crédito, documento necessário ao exercício do direito literal e autônomo nele contido, somente produz efeito quando preencha os requisitos da lei".

Por fim, como inexiste regulamentação legal sobre as moedas criptográficas, é inconcebível se falar em inexistência de autorização legal

para sua emissão; vez que tudo o que não é expressamente proibido, é permitido.

Os bens passíveis de **"lavagem de dinheiro"** (práticas que visam dissimular ou esconder a origem ilícita de determinados ativos financeiros ou bens patrimoniais) são aqueles que decorrem, direta (*producta sceleris*) ou indiretamente (*fructus sceleris*), da infração penal (exemplos, sonegação fiscal ou evasão de divisas). Os bens diretamente provenientes têm ligação imediata com o crime anterior, enquanto os indiretamente são resultado de uma transformação ou substituição dos bens anteriores.

Em razão disso, a bitcoin, por suas características essenciais, as quais se podem citar a utilização de pseudônimo (codinome ou nome fictício ou falso) por seus usuários e a falta de controle por parte do governo sobre sua emissão e circulação, faz com que facilmente se torne objeto material do crime de lavagem de dinheiro.

O processo de lavagem de dinheiro inicia-se com a prática de uma infração penal e a consequente ocultação dos valores auferidos ilicitamente. Logo após, são desenvolvidas diversas operações para dissimulação da origem dos bens, completando-se com a reinserção do capital na economia formal com aparência lícita. Em suma, as fases do crime de lavagem de dinheiro são: ocultação, dissimulação e integração dos bens à economia formal.

A ocultação é o movimento para "distanciar" o valor de sua origem criminosa ou contravencional, alterando qualitativamente os bens e afastando-os do local da prática delitiva anterior. Alguns exemplos de atos de ocultação são: depósito em contas de terceiros ("laranjas"), a transferência de capital sujo para fora do país ou seu envio para práticas lícitas comerciais sem controles rígidos de receitas e despesas, tais como padarias e postos de gasolina.

A seguir, tem-se o mascaramento ou dissimulação do capital, que se caracteriza pelo uso de transações financeiras ou comerciais posteriores à ocultação, contribuindo assim, pelo afastamento dos valores de sua origem ilícita.

Ao final, ocorre a integração é o ato final da lavagem, que é a introdução dos valores na economia com aparência de serem lícitos.

A conceituação do crime de sonegação fiscal encontra-se dispersa em vários dispositivos legais como a **Lei nº. 4.729/1965** (https://www.planalto.gov.br/ccivil_03/leis/1950-1969/L4729.htm). Desta feita, conforme o artigo 1.º da Lei nº. 4.729/1965, constitui crime de sonegação fiscal:

> "I - prestar declaração falsa ou omitir, total ou parcialmente, informação que deva ser produzida a agentes das pessoas jurídicas de direito público interno, com a intenção de eximir-se, total ou parcialmente, do pagamento de tributos, taxas e quaisquer adicionais devidos por lei;
> II - inserir elementos inexatos ou omitir, rendimentos ou operações de qualquer natureza em documentos ou livros exigidos pelas leis fiscais, com a intenção de exonerar-se do pagamento de tributos devidos à Fazenda Pública;
> III - alterar faturas e quaisquer documentos relativos a operações mercantis com o propósito de fraudar a Fazenda Pública;
> IV - fornecer ou emitir documentos graciosos ou alterar despesas, majorando-as, com o objetivo de obter dedução de tributos devidos à Fazenda Pública, sem prejuízo das sanções administrativas cabíveis.
> V - Exigir, pagar ou receber, para si ou para o contribuinte beneficiário da paga, qualquer percentagem sôbre a parcela dedutível ou deduzida do impôsto sôbre a renda como incentivo fiscal."

Em resumo, a **Lei n.º 4.502/1964** (http://www.planalto.gov.br/CCivil_03/Leis/L4502.htm), no artigo 71, reza que sonegação é toda ação ou omissão dolosa tendente a impedir ou retardar, total ou parcialmente, o conhecimento por parte da autoridade fazendária: I - da ocorrência do fato gerador da obrigação tributária principal, sua natureza ou circunstâncias materiais; e, II - das condições pessoais de contribuinte, suscetíveis de afetar a obrigação tributária principal ou o crédito tributário correspondente. Já o artigo 72 prescreve que: "Fraude é tôda ação ou omissão dolosa tendente a impedir ou retardar, total ou parcialmente, a

ocorrência do fato gerador da obrigação tributária principal, ou a excluir ou modificar as suas características essenciais, de modo a reduzir o montante do impôsto devido a evitar ou diferir o seu pagamento.".

Por sua vez, a **Lei n.º 8.137/1990** (https://www.planalto.gov.br/ccivil_03/leis/L8137.htm), denominada de Lei dos Crimes contra a Ordem Tributária, Econômica e Contra as Relações de Consumo, no seu artigo 1º preceitua que constitui crime contra a ordem tributária suprimir ou reduzir tributo, ou contribuição social e qualquer acessório, mediante as seguintes condutas:

> "I - omitir informação, ou prestar declaração falsa às autoridades fazendárias;
> II - fraudar a fiscalização tributária, inserindo elementos inexatos, ou omitindo operação de qualquer natureza, em documento ou livro exigido pela lei fiscal;
> III - falsificar ou alterar nota fiscal, fatura, duplicata, nota de venda, ou qualquer outro documento relativo à operação tributável;
> IV - elaborar, distribuir, fornecer, emitir ou utilizar documento que saiba ou deva saber falso ou inexato;
> V - negar ou deixar de fornecer, quando obrigatório, nota fiscal ou documento equivalente, relativa a venda de mercadoria ou prestação de serviço, efetivamente realizada, ou fornecê-la em desacordo com a legislação."

Em reforço, o artigo 2º diz que constitui crime da mesma natureza:

> "I - fazer declaração falsa ou omitir declaração sobre rendas, bens ou fatos, ou empregar outra fraude, para eximir-se, total ou parcialmente, de pagamento de tributo;
> II - deixar de recolher, no prazo legal, valor de tributo ou de contribuição social, descontado ou cobrado, na qualidade de sujeito passivo de obrigação e que deveria recolher aos cofres públicos;
> III - exigir, pagar ou receber, para si ou para o contribuinte beneficiário, qualquer percentagem sobre a parcela dedutível ou deduzida de imposto ou de contribuição como incentivo fiscal;

IV - deixar de aplicar, ou aplicar em desacordo com o estatuído, incentivo fiscal ou parcelas de imposto liberadas por órgão ou entidade de desenvolvimento;

V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública."

Com o advento da Lei nº. 8.137/1990 ocorreu a revogação tácita da Lei nº. 4.729/1965; ou seja, deve-se aplicar a Lei nº. 8.137/1990 e não mais a Lei nº. 4.729/1965.

A **Lei n.º 7.492/1986** (http://www.planalto.gov.br/ccivil_03/leis/L7492.htm), denominada de Lei do Colarinho Branco, em seus artigos 21 e 22, definiu como crimes as fraudes cambiais e a evasão cambial ou de divisas (reservas monetárias) para lavagem de dinheiro ilegal em paraísos fiscais. E para facilitar as investigações, a Lei 8.021/1990 (http://www.planalto.gov.br/ccivil_03/leis/L8021.htm) e o artigo 19 da Lei 8.088/1990 (https://www.planalto.gov.br/ccivil_03/Leis/L8088consol.htm) extinguiram as operações ao portador e a emissão de títulos sem a identificação de seus beneficiários. Também deixaram de existir os endossos ao portador, inclusive em cheques sacados contra contas correntes bancárias.

Depois veio a **Lei n.º 9.613/1998** (https://www.planalto.gov.br/ccivil_03/leis/L9613.htm), que acabou sendo substancialmente alterada pela Lei n.º 12.683/2012 (http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm).

Deste modo, a Lei n.º 9.613/1998, que dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores, bem como a prevenção da utilização do sistema financeiro para os ilícitos, em seu artigo 1º prescreve como crime o ato de: "Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal".

Urge ressaltar que **a fiscalização tributária possui amplo acesso às informações e documentos**. Senão vejamos.

O artigo 38 da Lei 4.595/1964 que versava sobre sigilo bancário, obstaculizando a atuação da fiscalização tributária, foi revogado pela Lei Complementar 105/2001. Ainda mais, o artigo 1.193, do Código Civil de 2002 (http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm), preceitua expressamente que não existe sigilo para as autoridades fazendárias nas esferas federal, estadual e municipal, entre as quais também estão os agentes fazendários do Distrito Federal.

Ainda mais, o Código Tributário Nacional (Lei n.º 5.172/1966: https://www.planalto.gov.br/ccivil_03/leis/L5172.htm), no artigo 195 estabelece que: "Para os efeitos da legislação tributária, não têm aplicação quaisquer disposições legais excludentes ou limitativas do direito de examinar mercadorias, livros, arquivos, documentos, papéis e efeitos comerciais ou fiscais, dos comerciantes industriais ou produtores, ou da obrigação destes de exibi-los.".

Ressalta-se, ainda, que a Lei Complementar n.º 104/2001 (https://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp104.htm), dentre outras providências de combate à elisão fiscal, realizou uma alteração no artigo 198 do Código Tributário Nacional para evitar óbices ao trabalho da fiscalização tributária.

Por sua vez, o § 1º, do artigo 33, da Lei n.º 8.212/1991 (https://www.planalto.gov.br/ccivil_03/leis/L8212cons.htm), na redação dada pela Lei n.º 11.941, de 2009, prescreve que: "É prerrogativa da Secretaria da Receita Federal do Brasil, por intermédio dos Auditores-Fiscais da Receita Federal do Brasil, o exame da contabilidade das empresas, ficando obrigados a prestar todos os esclarecimentos e informações solicitados o segurado e os terceiros responsáveis pelo recolhimento das contribuições previdenciárias e das contribuições devidas a outras entidades e fundos.".

Através da previsão constante do artigo 28 da Lei 6.385/1976 (http://www.planalto.gov.br/ccivil_03/leis/L6385.htm), da Lei

Complementar n.º 104/2001 (https://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp104.htm) e da Lei Complementar n.º 105/2001 (http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm), existe intercâmbio de informações sigilosas entre os órgãos públicos.

Existe previsões legais para extinguir a punição pelo crime tributário ou de isentar das multas e demais encargos da inadimplência tributária.

O CTN - Código Tributário Nacional (https://www.planalto.gov.br/ccivil_03/leis/L5172.htm), no artigo 156 prescreve que:

> "**Extinguem o crédito tributário**:
> I - o pagamento;
> II - a compensação;
> III - a transação;
> IV - remissão;
> V - a prescrição e a decadência;
> VI - a conversão de depósito em renda;
> VII - o pagamento antecipado e a homologação do lançamento nos termos do disposto no artigo 150 e seus §§ 1º e 4º;
> VIII - a consignação em pagamento, nos termos do disposto no § 2º do artigo 164;
> IX - a decisão administrativa irreformável, assim entendida a definitiva na órbita administrativa, que não mais possa ser objeto de ação anulatória;
> X - a decisão judicial passada em julgado.
> XI – a dação em pagamento em bens imóveis, na forma e condições estabelecidas em lei." (Grifo nosso).

O CTN, ainda, no artigo 138, prevê o instituto da denúncia espontânea, que permite aos contribuintes que tenham cometido algum tipo de infração a legislação tributária, eximir-se do pagamento de multas decorrentes de sua omissão.

A **Lei n.º 9.249/1995** (http://www.planalto.gov.br/ccivil_03/leis/L9249.htm), em seu artigo 34, preceitua que o pagamento do tributo antes do recebimento da denúncia do Ministério Público leva à extinção da punibilidade.

A **Lei nº. 9.964/2000** (http://www.planalto.gov.br/ccivil_03/leis/L9964.htm) instituiu o **Programa de Recuperação Fiscal (REFIS)**, a fim de promover a regularização de créditos da União, decorrentes de débitos de pessoas jurídicas, relativos a tributos e contribuições, (administrados pela SRF - Secretaria da Receita Federal e pelo INSS - Instituto Nacional do Seguro Social), créditos estes que podem ser constituídos ou não, inscritos ou não em dívida ativa, ajuizados ou a ajuizar, com exigibilidade suspensa ou não, inclusive os decorrentes de falta de recolhimento de valores retidos. No artigo 15 reza que: "É suspensa a pretensão punitiva do Estado, referente aos crimes previstos nos arts. 1º e 2º da Lei nº 8.137, de 27 de dezembro de 1990, e no art. 95 da Lei nº 8.212, de 24 de julho de 1991, durante o período em que a pessoa jurídica relacionada com o agente dos aludidos crimes estiver incluída no Refis, desde que a inclusão no referido Programa tenha ocorrido antes do recebimento da denúncia criminal.". E, no respectivo § 3º: "Extingue-se a punibilidade dos crimes referidos neste artigo quando a pessoa jurídica relacionada com o agente efetuar o pagamento integral dos débitos oriundos de tributos e contribuições sociais, inclusive acessórios, que tiverem sido objeto de concessão de parcelamento antes do recebimento da denúncia criminal.".

Já a **Lei nº. 10.684/2003** (http://www.planalto.gov.br/ccivil_03/leis/2003/L10.684.htm), alterou a legislação tributária e dispôs sobre o parcelamento de débitos junto à Secretaria da Receita Federal, à Procuradoria Geral da Fazenda Nacional e ao INSS - Instituto Nacional do Seguro Social. No seu artigo 1º permite o parcelamento em 180 (cento e oitenta) meses dos débitos junto à Secretaria da Receita Federal ou à Procuradoria-Geral da Fazenda Nacional. O artigo 9º, por sua vez, reza que: “É suspensa a pretensão punitiva do Estado, referente aos crimes previstos nos arts. 1º e 2º da Lei no 8.137, de 27 de dezembro de 1990, e nos arts. 168A e 337A do Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal, durante o período em que a pessoa

jurídica relacionada com o agente dos aludidos crimes estiver incluída no regime de parcelamento"; cujo § 2º prescreve que: "Extingue-se a punibilidade dos crimes referidos neste artigo quando a pessoa jurídica relacionada com o agente efetuar o pagamento integral dos débitos oriundos de tributos e contribuições sociais, inclusive acessórios".

Em caso de eventual condenação criminal, a Lei n.º 8.137/1990 (https://www.planalto.gov.br/ccivil_03/leis/L8137.htm) comina pena de reclusão de dois a cinco anos aos crimes contra a ordem tributária, com o que o sonegador condenado terá direito ao regime aberto, e se em regime semiaberto, terá direito ou a suspensão condicional da pena (Sursis), ou a substituição da pena por serviços à comunidade, salvo se a pena for superior a quatro anos o que é muito raro.

GÊNESE E PRIMÓRDIO DO BITCOIN

Vale lembrar, inclusive, que o "sonho" de se criar uma moeda inteiramente digital, baseada em criptografia e que não dependesse da confiança em qualquer intermediário para ser trocada remete a manifestos de criptógrafos de 1985. Além disso, os conceitos do Bitcoin foram em larga medida inspirados por duas propostas interessantíssimas, mas que nunca tinham sido integralmente postas em práticas com sucesso: o b-Money de Wei Dai (1998) e o Bitgold de Nick Szabo (2005). Satoshi foi o primeiro a resolver um problema que perdurava na computação por mais de 20 anos, dando-nos um meio de gerar consenso de forma segura e transparente em redes distribuídas.

Assim o software Bitcoin não "caiu do céu" ou "surgiu do nada", como às vezes se supõe, mas foi construído sobre ideias de várias pessoas ao longo de décadas. E muitas outras moedas eletrônicas acabaram (Liberty Reserve, eGold, etc.).

Embora a moeda bitcoin seja mais conhecida e utilizada, outras criptomoedas foram criadas e podem ser utilizadas no meio virtual. Os valores de mercado das moedas digitais encontram-se disponíveis em sites como http://coinmarketcap.com/.

O **ECash** foi concebido por David Chaum como uma moeda eletrônica ou sistema de dinheiro eletrônico em 1983 (*Blind Signatures for Untraceable Payments*, D. Chaum, *Advances in Cryptology Proceedings of Crypto* 82, D. Chaum, R.L. Rivest, & A.T. Sherman (Eds.), Plenum, pp. 199-203).

- http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.

O ECash foi realizado através de sua corporação Digicash e usado como sistema de micropagamento de um banco (*Mark Twain bank in Saint Louis, MO*) dos Estados Unidos de 1995 a 1998. O sistema foi encerrado em 1998, um ano após o banco ter sido comprado por Mercantile Bank, um grande emissor de cartões de crédito. A DigiCash faliu em 1998 e, então, foi vendida para eCash Technologies, incluindo suas patentes eCash. Em 2002

eCash Technologies foi adquirida pela InfoSpace, atualmente conhecida como Blucora. Em 2016, Due Inc adquiriu a marca "ECash" (https://due.com/ecash).

Os nerds (fanáticos por informática) puseram a mão na massa na década de 1990 e desenvolveram uma série de protótipos (E-cash, Bitgold, RPOW, b-money, etc.), mas todos fracassaram pela mesma razão: sua oferta não podia ser limitada e ninguém conseguia descobrir como tornar impossível que a mesma quantia fosse gasta duas, três ou várias vezes. Pela lógica e programação do Bitcoin, é impossível duas pessoas gastarem a mesma moeda digital (*double-spending*). Isso quer dizer que somente uma pessoa detém o direito de propriedade de uma unidade monetária e somente essa pessoa a controla.

Muitas moedas digitais já "morreram"! É o caso da e-gold, Sambacoin, BRCoin, Floripacoin, etc.

- http://www.viruscore.com/2015/moeda-virtual/.

Moedas digitais (tais como MochiCoin, BG Coins, hoplon, Hazit, myClub, etc.) já existem há anos nos games (jogos) on line; tais como, por exemplo, Perfect World (PW), League of Legends, Habbo, Colheita Feliz, Segredos do Mar, Bola, CrimeCraft, Tíbia, Bottle Game, etc. Mas tais moedas possuem utilização, comercialização e aceitação muito restritas.

- http://www.shoppingcartaopresente.com.br/games/;
- http://www.portaldoscreditos.com.br/;
- https://www.e-prepag.com/;
- https://go4gold.uol.com.br/;
- https://blogpagseguro.com.br/2011/12/pincode-o-servico-de-creditos-para-jogos-online/.

Muitos jogos online podem ir além da diversão e servir como uma fonte de renda. Os ciberatletas ganham dinheiro em jogos que envolvem apostas, como pôquer, ou jogos em que há campeonatos organizados pelas empresas desenvolvedoras; alguns chegando a prêmios milionários. Em jogos onde se

acumula pontos e pode trocá-los por melhoras no avatar (como roupas, armas e habilidades) o comércio mesmo quando é proibido, sempre existe um mercado negro ou paralelo.

Goldentowns é um jogo combinado com simulador econômico online, contendo uma economia bastante complexa e interessante. Para tornar esse simulador econômico ainda mais interessante, os resultados nele obtidos podem ser convertidos em dinheiro real e isso dá um dinamismo excepcional ao jogo. GoldenTowns é um jogo online gratuito que pode ser jogado por um browser como o Internet Explorer. É o primeiro jogo do mundo com lastro em ouro. Em GoldenTowns há uma quantidade limitada de ouro virtual (100.000 GoldenTowns Coins ou GTC) que são distribuídos gradualmente com a mineração dos jogadores. Toda essa quantia é lastreada por uma quantidade crescente de ouro real. Ou seja, o sistema da moeda virtual e sua conversão em moeda real é muito similar ao sistema Bitcoin. É claro que o jogo muito dificilmente dará rendimentos comparáveis com o seu salário na vida real. Ele precisa ser visto como um jogo. No entanto, ao contrário da maioria dos jogos que prometem dinheiro real, mas uma rápida análise demonstra que são *scams*, os fundamentos econômicos do GoldenTowns são muito sérios e você pode, com certeza, obter alguma renda enquanto se diverte nele!

- http://www.goldentowns.com/?i=macfly;
- http://www.goldentowns.com/terms.php;
- http://www.goldentowns.com/pages/articles/article.php?ID=61;
- http://www.goldentowns.com/forum/faq.php?sid=7d25b59e819c429eb324569994d16740;
- http://www.goldentowns.com/forum/viewtopic.php?f=24&t=6887&sid=19407b9e7b2184a9c7c4a8c32a46aeac;
- http://www.annowallet.com/.

PipsTycoon (http://www.pipstycoon.com/) é o primeiro jogo de negociação social. PipsTycoon é um dinheiro real num simulador econômico e financeiro em torno da negociação social. Simulador de dinheiro real

significa que se pode transformar os dólares virtuais para a moeda corrente ou oficial.

O **E-Gold** foi desenvolvido em 1996 para facilitar transações comerciais entre empresas. No início de 1999 foi disponibilizado para todo o público em geral. O site (http://www.e-gold.com) operava apenas com metais preciosos (tinha lastro), que circulam eletronicamente: e-Gold (ouro), e-Silver (prata), e-Platinum (platina) e e-Paladium (paládio). O e-gold foi encerrado em 2014.

- https://pt.wikipedia.org/wiki/E-gold;
- https://en.wikipedia.org/wiki/E-gold;
- https://en.bitcoin.it/wiki/E-gold;
- http://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/Bitcoins/e-gold.html;
- http://blog.e-gold.com/;
- http://www.abelard.org/value-transfer/egold-info.htm.

Semelhantemente, a *Liberty Reserve* (http://www.libertyreserve.com/), fundado em 2001, era um sistema de pagamento online e provedor de uma moeda eletrônica baseadas no valor do ouro (*digital gold currency*). A moeda *Liberty Reserve* foi utilizada com frequência em HYIP´s ("High-Yield Investment Program" ou "Programa de Investimento de Alto Rendimento", que virou sinônimo de fraude - https://pt.wikipedia.org/wiki/HYIP), PTC´s (*Pay To Click* ou “pago para clicar”) e Forex (acrônimo da expressão inglesa “foreign exchange”, significa “Mercado de Câmbio”). O governo dos Estados Unidos a acusou de ter “lavado” dinheiro. Com o fim da *Liberty Reserve* em maio de 2013, os *crackers* (*hackers* que usam o conhecimento para a prática de crimes) migraram para o sistema de pagamentos *Perfect Money* (https://www.perfectmoney.is/).

- http://investindoonline.com.br/blog/liberty-reserve-milhoes-de-dolares-no-limbo/;
- http://br.ccm.net/news/20410-liberty-reserve-fechada-pela-justica-americana-por-lavagem-macica-de-dinheiro;

- http://www.rtp.pt/noticias/mundo/justica-dos-eua-desmantela-plataforma-liberty-reserve_v655016;
- http://g1.globo.com/tecnologia/noticia/2013/08/hackers-adotam-nova-moeda-digital-depois-da-liberty-reserve.html;
- http://exame.abril.com.br/tecnologia/noticias/hackers-adotam-nova-moeda-digital-depois-da-liberty-reserve;
- http://www.cmjornal.xl.pt/mundo/detalhe/eua-acusam-banco-online-de-apoiar-o-crime.html;
- http://idgnow.com.br/ti-corporativa/2013/05/29/liberty-reserve-e-indiciado-pela-lavagem-de-6-bilhoes-de-dolares/;
- http://www.tvi24.iol.pt/economia/crimes-economicos/liberty-reserve-e-o-banco-de-referencia-do-mundo-criminal;
- http://www.rtp.pt/noticias/mundo/liberty-reserve-apontado-pelos-estados-unidos-como-banco-de-referencia-do-mundo-criminal_a655043;
- https://nakedsecurity.sophos.com/pt/2014/09/15/liberty-reserve-cto-pleads-guilty-to-involvement-in-massive-money-laundering/.

Desde que a Internet começou, várias moedas foram criadas e encerradas pelos mais diversos motivos. O mais comum é a suspeita de estar sendo usada por criminosos, então a Justiça encerra o serviço. O grande problema do encerramento da e-gold, e de todas as moedas subsequentes, é que muitas pessoas estavam usando para comprar produtos ilegais (incluindo drogas e armas); o que fez o FBI - *Federal Bureau of Investigation* (Polícia Federal dos Estados Unidos) investigar e acabar detectando a transferência de fundos de grupos terroristas.

O segundo motivo é a criação de valores artificiais. O dono da moeda virtual (centralizada) não pode criar moedas ou valores sem ter um lastro, garantia e/ou fé pública (credibilidade geral, aceitação coletiva, convenção social, etc.), porque se parte considerável dos usuários (detentores da moeda) desejarem ter seus valores virtuais convertidos em moeda real (física, oficial ou convencional), isso será impossível se o dono criou valores irreais (abstratos, aleatórios, surreais) e/ou não tiver uma garantia (depósito, reserva, recursos, etc.) para honrar com o pagamento prometido. Em não sendo possível fazer a conversão da moeda virtual para uma convencional, será a morte da moeda e o fim do serviço; bem como todos os

titulares dessa moeda perderão tudo. Isso já aconteceu com a moeda virtual StormPay (https://en.wikipedia.org/wiki/StormPay) porque seu dono criava valores falsos sem lastro até que não poder pagar todos os requisitantes.

Nenhuma moeda ou valor pode ser aleatório ou simplesmente imposto (arbitrário, ordenado, forçado ou obrigado). Todo valor precisa de um fundamento ou suporte; ou seja, precisa estar associado a algo que valha (lastro, garantia, confiança, justificativa, razão, etc.) e lhe atribua valor e aceitação.

O Bitcoin foi uma ideia incrível, pois evita todos estes problemas nas moedas virtuais anteriores. Não tem um controlador central (é totalmente decentralizada); ou seja, não tem um dono. Todo valor é associado a um nome. Não é possível inflacionar o Bitcoin, pois cada valor é criado através de cálculos (mineração eletrônica); ou seja, teoricamente qualquer computador pode "fabricar" Bitcoins. Assim, não tendo um dono e nem podendo se fabricar valores de forma arbitrária e aleatória, o Bitcoin é tão seguro que até o FBI é dono de uma boa parte deles e alguns países permitiram a circulação com caixas eletrônicos e até saque com cartão de débito.

QUEM CRIOU O BITCOIN?

O criador do Bitcoin utilizou o pseudônimo (ou *ghostwriter* [escritor fantasma]) **Satoshi Nakamoto**(□ □ □ □) e, possivelmente, os e-mails satoshin@gmx.com e satoshi@vistomail.com.

Em 31 de outubro de 2008 ele publicou o manifesto: "Bitcoin: A Peer-to-Peer Electronic Cash System" (http://nakamotoinstitute.org/bitcoin/ e https://bitcoin.org/bitcoin.pdf).

> "O Bitcoin foi inventado em 2008 com a publicação de um documento intitulado "Bitcoin: Um Sistema de Dinheiro Eletrônico Ponto-a-Ponto" ("Bitcoin: A Peer-to-Peer Electronic Cash System" em inglês), escrito por um autor sob o pseudônimo de Satoshi Nakamoto. Nakamoto combinou várias das invenções anteriores tais como *b-money* e *HashCash* para criar um sistema de dinheiro eletrônico completamente descentralizado que não dependesse de uma autoridade central para a emissão de moeda ou para a liquidação e validação de transações. A principal inovação foi usar um sistema de computação distribuído (chamado algoritmo de "prova de trabalho" ou "proof of work") para conduzir uma "eleição" global a cada 10 minutos, permitindo à rede descentralizada chegar em um consenso sobre o estado das transações. Isto resolve de forma elegante o problema de gasto duplicado, onde uma única unidade de moeda poderia ser gasta duas vezes. Antes do Bitcoin, o problema de gasto duplicado era uma fraqueza do dinheiro digital, e sua solução envolvia a transmissão e verificação de todas as transações através de uma entidade central.
>
> A rede bitcoin surgiu em 2009, baseada em uma implementação de referência publicada por Nakamoto e desde então revisada por muitos outros programadores. A computação distribuída que proporciona segurança e robustez ao bitcoin cresceu exponencialmente, e agora excede a capacidade combinada de processamento dos principais supercomputadores do mundo." (Mastering Bitcoin por Andreas M. Antonopoulos LLC *in* https://bitcoinbook.info).

Cópia do e-mail, intitulado "Bitcoin P2P e-cash paper", que Satoshi Nakamoto enviou para a lista / fórum de discussão “Cryptography na

metzdowd.com" (crypto.discuss@bloom-picayune.mit.edu), divulgando seu manifesto, encontra-se disponível em:

- http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html;
- http://satoshi.nakamotoinstitute.org/emails/cryptography/1/;
- https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.

Em 03 de janeiro de 2009 o primeiro bloco de Bitcoin foi extraído (bloco 0 [*block 0*] ou bloco gênesis [*genesis block*] e contém o texto: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", talvez como prova de que o bloco foi extraído a partir dessa data e, talvez, também como relevante o comentário político. Depois, em 08/01/2009, a primeira versão do *software* Bitcoin foi anunciada no grupo "Cryptography Mailing". E, em 09/01/2009, o Bloco 1 foi extraído.

Satoshi Nakamoto é um nome muito comum no Japão como João da Silva no Brasil. Satoshi é uma palavra japonesa que significa "pensamento claro" ou "sábio". O nome também se refere ao programa código aberto que ele projetou para o uso da moeda e a respectiva rede *peer-to-peer* que é formada.

No final de 2010, como o projeto estava acertando seu passo, Satoshi Nakamoto, que era bastante participativo no fórum, gradativamente diminuiu suas postagens até o total silêncio. E, assim, em 2011 desapareceu.

Surgiram vários caçadores do fantasma fazendo diversas especulações e, assim, várias teorias / teses surgiram apontando vários suspeitos de serem Satoshi Nakamoto.

- http://www.bitkoins.com.br/wordpress/2015/08/22/quem-e-satoshi-nakamoto-veja-lista-de-10-suspeitos/.

Uma tese foi de que Satoshi não seria uma pessoa real, mas sim um pseudônimo usado por um grupo de desenvolvedores para ser a persona criadora da Bitcoin.

Outras teorias propuseram que Satoshi seria um economista da Finlândia, um especulador financeiro norte-americano, um estudante de Dublin ou até mesmo um pseudônimo criado com o acrônimo de quatro grandes corporações mundiais (Samsung, Toshiba, Nakamichi e Motorola).

Mas programadores e empreendedores mais profundamente envolvidos com o Bitcoin (como Skye Grey), alegam que boa parte das evidências apontam para um americano recluso de ascendência húngara, chamado Nick Szabo, pesquisador da Universidade de Washington. A contribuição mais notável de Szabo foi um antecessor do Bitcoin conhecido como “bit gold” que alcançou muitos dos mesmos objetivos usando ferramentas similares de matemática avançada e criptografia. Apesar de estar envolvido desde o começo dos anos 90 em uma comunidade online chamada *Cypherpunks*, pioneira na discussão de ideias que ajudaram a formatar o Bitcoin, são suas atividades em 2008 que mais contribuíram para levantar suspeitas com relação ao papel de Szabo. Foi naquele ano, um pouco antes da chegada do Bitcoin, que ele escreveu em seu blog sobre o bit gold. Pesquisadores ingleses notaram semelhanças fora do comum entre seu linguajar e maneirismos com aqueles atribuídos a Satoshi. Como Satoshi parou de contribuir para o projeto em 2011, a maior parte do código aberto foi reescrita por um grupo de programadores cujas identidades são conhecidas.

No seu perfil da P2P Foundation, Nakamoto alegou ser um homem de 37 anos que vive no Japão, enquanto outros especulam ser improvável ele ser japonês devido ao seu inglês perfeito e seu *software* Bitcoin não ter sido documentado ou rotulado no Japão. Ocasionalmente, também, ele utiliza ortografia e terminologia de inglês britânico (como a frase "bloody hard"), tanto em códigos-fonte e postagens no fórum, com o que se levou a especulação de que Nakamoto, ou pelo menos um indivíduo no consórcio afirmando ser ele, é de origem *Commonwealth* (nações que faziam parte do Império Britânico - https://pt.wikipedia.org/wiki/Commonwealth). Stefan Thomas, um programador suíço e membro ativo da comunidade Bitcoin, estudou os horários das postagens de Nakamoto no fórum bitcoin e observou a inexistência de postagens dele entre 5:00 e 11:00 da manhã, pelo fuso horário de Greenwich (GMT ou TMG - *Greenwich Mean Time*); com isso sugeriu-se que Satoshi Nakamoto residiria em uma região usando o UTC-05:00 ou UTC-06:00 de diferença horária. Isso inclui as partes da América

do Norte que cai dentro da Zona de Tempo Oriental, bem como partes da América Central, Caribe e América do Sul.

Em um artigo de 2011, no *The New Yorker*, Joshua Davis alegou ter reduzida a identidade de Nakamoto para uma série de possíveis indivíduos, incluindo o sociologista econômico Dr. Vili Lehdonvirta e o estudante irlandês, Michael Clear, que em seguida se tornou um estudante de pós-graduação em criptografia no *Trinity College Dublin*.

Em outubro de 2011, escrevendo para *Fast Company*, o jornalista investigativo, Adam Penenberg, citou uma circunstancial evidência sugerindo que Neal King, Vladimir Oksman e Bry poderiam ser Nakamoto. Eles apresentaram, conjuntamente um pedido de patente que continha a frase "computacionalmente impraticável para reverter" em 2008, que também foi utilizado no *Bitcoin White Paper* por Nakamoto. O domínio bitcoin.org na Internet foi registrado três dias após a patente ser arquivada.

Em maio de 2013, Ted Nelson especulou que Nakamoto era o matemático Japonês Shinichi Mochizuki.

Em 2013, dois matemáticos israelitas, Dorit Ron e Adi Shamir, publicaram um artigo reivindicando uma ligação entre Nakamoto e Ross William Ulbricht.

Em dezembro de 2013, um blogger chamado Skye Grey vinculou Nick Szabo com o *whitepaper* do Bitcoin usando a análise de conteúdo estilométrica. Nick Szabo é um jurista e criptógrafo conhecido por sua pesquisa em contratos digitais e moeda digital. A frase e conceito de "contratos inteligentes" foi desenvolvido por Szabo com o objetivo de trazer o que ele chama de práticas evoluídas da lei e da prática de contrato para o projeto de comércio eletrônico na Internet. Por volta de 1998 a 2005, Szabo desenvolveu um mecanismo para uma moeda digital descentralizada que ele chamou de "bit gold", que alguns têm chamado de 'precursor direto para a arquitetura Bitcoin'. Szabo é entusiasta da moeda descentralizada e é conhecido por ter usados pseudônimos na década de 1990. Em um artigo de maio de 2011, Szabo afirmou sobre o criador Bitcoin: "Eu mesmo, Wei Dai, e Hal Finney foram as únicas pessoas que eu conheço quem gostaram da

idéia (ou no caso de Dai sua idéia relacionada) o suficiente para persegui-la de forma significativa até Nakamoto (assumindo Nakamoto não é realmente Finney ou Dai)". Em seu livro, “Bitcoin: The Future of Money?”, e em “RT's The Keiser Report”, o escritor e repórter investigativo, *Dominic Frisby*, também afirma que é bastante certo de que Nick Szabo seja Satoshi Nakamoto. Citado no “Relatório Keiser” (*Keiser Report*), foi dito que: "eu já concluiu há apenas uma pessoa no mundo todo, que tem a grande amplitude, mas também a especificidade do conhecimento e é esse cara".

Hal Finney foi um dos pioneiros de criptografia pré-Bitcoin e a primeira pessoa (que não seja o próprio Satoshi) para usar o *software*. Ele também morava a poucos quarteirões da casa da família de Dorian Nakamoto, de acordo com a jornalista da Forbes, Andy Greenberg. Ela pediu a consultoria Juola & Associates para comparar uma amostra de escrita de Finney com a de Satoshi Nakamoto e eles descobriram uma grande semelhança; muito maior do que os candidatos ou suspeitos sugeridos pela Newsweek, Fast Company, The New Yorker, Ted Nelson e Skye Grey.

Em 06/03/2014, a jornalista Leah McGrath Goodman, do *Newsweek* (http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html) encontrou um Satoshi Nakamoto que poderia ser o tal. Tratava-se de um imigrante japonês, de 64 anos, que mora na Califórnia, em *Temple City*. Logo depois de se formar em Física, mudou de nome para Dorian Prentice Satoshi Nakamoto, assinando Dorian S. Nakamoto. Na Wikipédia ele é descrito como se fosse realmente o criador do Bitcoin (https://pt.wikipedia.org/wiki/Satoshi_Nakamoto).

- http://olhardigital.uol.com.br/pro/noticia/conheca-a-historia-de-satoshi-nakamoto-o-inventor-da-bitcoin/40681;
- http://saopaulotimes.r7.com/sp/o-homem-por-tras-da-bitcoin-materia-na-integra/;
- http://g1.globo.com/tecnologia/noticia/2014/03/reportagem-identifica-satoshi-nakamoto-criador-do-bitcoin.html;
- http://www1.folha.uol.com.br/tec/2014/03/1422033-engenheiro-de-64-anos-nega-ser-criador-da-moeda-virtual-bitcoin.shtml;
- https://tecnoblog.net/153170/dorian-satoshi-nakamoto-carta-advogado/.

Entretanto, através da conta do pseudônimo na Fundação de Nakamoto P2P (http://p2pfoundation.ning.com/profile/SatoshiNakamoto), o fantasma lançou sua primeira mensagem em cinco anos, afirmando: "Eu não sou Dorian Nakamoto" ("I am not Dorian Nakamoto").

- http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186&xg_source=activity.

Em maio de 2016, um empresário australiano, Craig Wright, se identificou como sendo o mentor ("Satoshi Nakamoto") que desenvolveu a moeda virtual. Apesar de ter apresentado provas e ter sido reconhecido como o fundador da moeda virtual pelo cientista-chefe da *Bitcoin Foundation* (Gavin Andresen), muitos ainda duvidam. Entre as provas estaria a chave criptográfica por traz do primeiro bloco de bitcoins minerado. Essa chave funciona como uma identidade por traz de cada transação. Em 2015, *hackers* vazaram informações do computador de Craig Wright à Imprensa, sugerindo que ele poderia ser o homem por traz de Satoshi. Logo em seguida, a casa de Wright foi vasculhada por conta de problemas com a fiscalização financeira da Austrália. Em dezembro de 2015, Wired escreveu que Craig Steven Wright, um australiano ex-acadêmico, "ou é o inventor do bitcoin ou é um farsante brilhante que deseja muito que nós acreditemos nisso".

Craig Wright desistiu de realizar uma transferência que provaria que ele é mesmo o criador da moeda criptográfica Bitcoin. No dia 05/05/2016, ele apagou todo o conteúdo do seu site (http://www.drcraigwright.net/), substituindo por uma mensagem com um pedido de "desculpas". O australiano não nega que é Satoshi Nakamoto, apenas diz que não vai mais fornecer provas. O jornalista Rory Cellan-Jones da "BBC" informou que ele, Jon Matonis (diretor da Fundação Bitcoin) e Gavin Andresen (cientista-chefe na Fundação Bitcoin e já foi líder de desenvolvimento do Bitcoin) enviaram pagamentos para um endereço de Bitcoin que deve pertencer a Satoshi Nakamoto. Wright deveria devolver esse dinheiro para eles, assim provando que é o criador do Bitcoin. O retorno do dinheiro, porém, nunca aconteceu. Jon Matonis e Gavin Andresen endossaram a declaração de Wright é uma fraude.

- http://www.bbc.com/news/technology-36213580;
- http://www.bbc.com/news/technology-36575524.

Conforme veremos infra, nos capítulos "BITCOIN" e "INTRODUÇÃO ÀS ALTCOINS", a bitcoin não foi a primeira moeda digital; muito menos foi uma ideia totalmente original, mas sim a junção e aperfeiçoamento de ideias e experiências anteriores. Entretanto, a bitcoin foi a primeira criptomoeda descentralizada.

SOFTWARES LIVRE E *OPEN SOURCE*

Softwares (programas de computador) de código aberto (OSI - *Open Source Initiative*) e livres ("Free Software") possuem muitas diferenças.

O termo “código aberto” significa que qualquer pessoa pode ter acesso ao código fonte do programa (é como se fosse a receita do programa); mas é seu desenvolvedor quem determina a distribuição, modificação, comercialização e as condições de uso.

Em 1983, Richard Stallman fundou o GNU (*GNU is not Unix*) com o objetivo de construir um sistema operacional totalmente livre, que tivesse seu código fonte aberto para leitura, modificação e redistribuição sem restrições. Cerca de dois anos depois, fundou a FSF - *Free Software Foundation* (entidade sem fins lucrativos que serve de base para o movimento do software livre). Depois, Linus Torvalds criou o Linux, resultando no GNU/Linux.

Em 1989, foi lançada a GPL (*General Public License*), que regulamentava o uso do **Software Livre** de maneira formal, com a premissa de respeitar a liberdade de qualquer um executar o programa para qualquer propósito e ter acesso ao código-fonte para estudá-lo e adaptá-lo para as suas necessidades; inclusive aperfeiçoá-lo e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie deles. Portanto, nota-se a colaboração voluntária entre desenvolvedores.

- http://www.gnu.org/licenses/gpl.html.

Os programas mundiais mais utilizados que possuem o código aberto são Mozilla Firefox, Perf, Apache HTTP Server, Linux, OpenOffice, Gimp, Amule, etc.

- http://meiobit.com/9735/lista-de-30-programas-codigo-aberto-para-o-windows/.

Hackathon (hackatona, hackathão, hack day, hackfest ou codefest), derivada da junção das palavras inglesas Hack e Marathon, é uma maratona de programação em que vários *hackers* se reúnem para passar horas a fio desvendando dados, sistemas lógicos e desenvolvendo algo com isso.

Em resumo, o Software Livre costuma ser aquele desenvolvido colaborativamente (operação comunitária) e que pode ser usado e compartilhado livremente.

Um programa não necessita obrigatoriamente de uma licença GPL para ser um software livre. É possível o uso de outras licenças, desde que compatíveis com as liberdades em questão. É possível conhecer as opções em www.gnu.org/licenses/license-list.html.

Um software meramente gratuito (*freeware*) é aquele que se pode utilizar licitamente sem pagar.

Para um software ser considerado Software Livre ele precisa apenas ter o código fonte disponível, mas isso não quer dizer que não se possa cobrar pelo código fonte do programa ou pelo programa em si. A palavra "livre" ("free" no original) está relacionada com liberdade, ao invés de preço.

Embora os programas livres sejam livres de contratos comerciais, permitindo sua livre distribuição e propagação, pode ser cobrado serviços necessários como instalação, customização, personalização, podendo ser até vendidos por terceiros em instalações customizadas abrangendo um pacote de serviços.

Qualquer licença de software livre é também uma licença de código aberto (*Open Source*), mas o contrário nem sempre é verdade.

O ***Open Source*** é um movimento que surgiu em 1998 por iniciativa principal de Bruce Perens, definindo dez quesitos para que um software possa ser considerado *Open Source*:

1) Distribuição livre;
2) Acesso ao código-fonte;
3) Permissão para criação de trabalhos derivados;
4) Integridade do autor do código-fonte;
5) Não discriminação contra pessoas ou grupos;
6) Não discriminação contra áreas de atuação;

7) Distribuição da licença;
8) Licença não específica a um produto;
9) Licença não restritiva a outros programas;
10) Licença neutra em relação à tecnologia.

Basicamente, um desenvolvedor (ou a equipe de desenvolvedores) adota um modelo de código aberto porque acha melhor para desenvolver, e não necessariamente porque crê nele como um modelo de liberdade. A grande diferença entre software livre e *Open Source*, é que o primeiro prega a liberdade no software não só do ponto de vista técnico, mas também sob a ótica da moral e ética. Em resumo, o pessoal do "open source" é mais pragmático, enfatiza o código aberto, mas aceita que existam softwares distribuídos sob outros modelos de desenvolvimento, como o proprietário.

Por não possuir um custo de licença, um software *open source* oferece a oportunidade de um maior investimento em serviços e formação, garantindo um retorno dos investimentos em TI maior e melhor. Na grande maioria dos casos, essas ferramentas são compartilhadas online pelos desenvolvedores, podendo ter acesso a elas qualquer pessoa, sem restrições.

- http://softwarelivre.org/open-source-codigo-aberto;
- https://opensource.org/docs/definition.php.

Quando um software é criado, o desenvolvedor o associa a um documento que determina quais ações o utilizador pode ou não executar. Esta é a licença de software.

Enquanto o *copyright* (direito autoral protegido) dá mais foco nas restrições, o *copyleft* (liberdade de copiar, modificar e redistribuir, exigindo que esse direito seja mantido em todas as versões modificadas) se baseia nas permissões.

QUEM CONTROLA OU ESTÁ POR TRÁS DO BITCOIN?

Bitcoin usa a tecnologia ponto-a-ponto (P2P) para operar sem a necessidade de uma autoridade central ou banco; as transações com bitcoins são gerenciadas coletivamente pelos usuários da rede. O Bitcoin é código aberto, seu *design* é público, ninguém é proprietário ou controla o Bitcoin e qualquer um pode participar. Através das suas várias e únicas características, a rede Bitcoin permite usos interessantes indisponíveis nos sistemas de pagamento anteriores.

A topologia *peer-to-peer* da rede Bitcoin, e a ausência de uma entidade administradora central torna inviável que qualquer autoridade financeira ou governamental manipule a emissão e o valor de bitcoins ou induza inflação fabricando mais dinheiro. No entanto, em tese, grandes movimentos especulativos de oferta e demanda poderiam fazer com que o seu valor sofresse oscilação no mercado de câmbio.

> "A demanda chinesa é o principal vetor de crescimento do bitcoin, influenciando diretamente não só a cotação da moeda digital, mas também o mecanismo essencial para o funcionamento do blockchain: a mineração. Atualmente, fabricantes chineses são responsáveis pela grande maioria das máquinas mineradoras e grupos de mineradores chineses controlam mais de 70% da capacidade de processamento dedicada ao blockchain. O predomínio chinês na mineração coloca um grau de complexidade adicional em relação aos mecanismos de governança do protocolo e resulta em conflito no que diz respeito à natureza descentralizada do blockchain." (Publicado em 15/08/2016 - https://www.coinbr.net/blog/afinal-de-contas-os-chineses-controlam-o-bitcoin/).

O domínio Bitcoin.org foi originalmente registrado aos dois primeiros desenvolvedores do Bitcoin, Satoshi Nakamoto e Martti Malmi. De acordo com a pesquisa de DNS ou Whois, o endereço (site) Bitcoin.org foi criado em 18/08/2008 e sofreu várias atualizações de informações. Atualmente este domínio da Internet é "WhoisGuard Protected"; ou seja, a identidade da pessoa que registou não é informação pública. Outro detalhe, é que o

endereço https://bitcoin.org/en/ seria apenas mais um outro nome para vhost.sourceforge.net (criado em 08/08/1999).

- http://whois.domaintools.com/bitcoin.org;
- http://www.whois.com/whois/bitcoin.org;
- http://www.mydnstools.info/whois/bitcoin.org;
- http://www.cuwhois.com/info/www.jtrac.info.

Pelo http://www.whatmyip.co/info/whois/208.64.123.130/k/2768844247/website/bitcoin.org é informado que Saivann Carignan (https://github.com/saivann) seria o proprietário do domínio Bitcoin.org.

- https://bitcoinfoundation.org/author/saivann/;
- https://wiki.edubuntu.org/Saïvann;
- https://github.com/saivann;
- https://libraries.io/github/saivann;
- https://plus.google.com/115025166606177994067;
- https://www.transifex.com/user/profile/saivann/.

A *Fast Company* providenciou uma investigação mais profunda sobre a origem desta moeda virtual e conseguiu descobrir que em agosto de 2008 Neal King, Vladimir Oksman e Charles Bry registraram uma patente relacionada a dados encriptados. O registro dessa patente foi feito exatamente 72 horas antes do registro do domínio bitcoin.org ser registrado. Para tornar a história ainda mais interessante, existem trechos semelhante na descrição da patente e da documentação do bitcoin, incluindo a frase “computationally impractical to reverse”, encontrada em ambos os documentos.

Martti Malmi (aka Sirius), um estudante da Universidade Aalto, na Finlândia, foi um dos desenvolvedores do núcleo no início do projeto. Tanto bitcoin.org e bitcointalk.org é propriedade de Martti. Ele é o administrador do fórum bitcointalk.org.

Quando Nakamoto deixou o projeto, ele deu a propriedade do domínio para pessoas adicionais, separadas dos desenvolvedores Bitcoin, para espalhar a responsabilidade e evitar que qualquer pessoa ou grupo de facilmente ganhar o controle sobre o projeto Bitcoin. De 2011 a 2013, o local foi usado principalmente para liberar novas versões do *software* agora chamado Bitcoin Core. Atualmente o site é um projeto *open source* independente com colaboradores de todo o mundo. A autoridade de publicação final é realizada pelos co-proprietários, mas toda a atividade é organizada através do processo público de solicitação de recebimento e gerido pelo site através dos co-mantenedores. Bitcoin.org não é o site oficial do Bitcoin. Assim como ninguém possui a tecnologia de e-mail, ninguém é dono da rede de Bitcoin. Como tal, ninguém pode falar com autoridade em nome de Bitcoin. O Bitcoin é controlado por todos os usuários Bitcoins em todo o mundo. O Bitcoin só pode funcionar decentemente com um consenso total entre todos os usuários.

A Fundação Bitcoin (https://bitcoinfoundation.org/) é uma organização que promove o desenvolvimento da referida moeda virtual. De modo semelhante, há a Fundação Bitcoin Brasil (http://institutobitcoin.org/).

- https://bitcoin.org/pt_BR/comunidade.

O Estatuto Social (*Bylaws*) da Bitcoin Foundation (http://bitcoinfoundation.org/transparency/) pode ser visto em https://github.com/pmlaw/The-Bitcoin-Foundation-Legal-Repo/blob/master/Bylaws/Bylaws_of_The_Bitcoin_Foundation.md.

Outros dados da Bitcoin Foundation podem ser conferidos em http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=237471762.

A rede e o software bitcoin estão constantemente evoluindo através do trabalho da comunidade bitcoin (https://bitcoin.org/pt_BR/desenvolvimento). O desenvolvimento do Bitcoin é código-livre ou aberto (*open source*) e, assim, qualquer desenvolvedor pode contribuir para o projeto através da língua inglesa (https://bitcoin.org/en/developer-documentation). As Propostas de Melhorias ao Bitcoin (**BIPs** - *Bitcoin Improvement Proposals*) são documentos de *design* que fornecem informações para a comunidade bitcoin, ou descreve uma nova função para o Bitcoin, seus processos ou ambiente. As versões das BIPs são gravadas em um repositório no GitHub (https://github.com/bitcoin/bips).

- https://bitcoinmagazine.com/articles/open-letter-bitcoin-community-developers-1441146317;
- http://www.bitkoins.com.br/wordpress/2015/09/02/carta-aberta-dos-desenvolvedores-para-a-comunidade-bitcoin/.

O fato das moedas digitais dispensarem uma autoridade controladora, um banco central, a regulamentação pelo governo ou a intervenção estatal (ser descentralizada) lhe rendem o apelido de "crypto-anarchy" (cripto-anarquia). Não confunda "cripto", abreviatura de criptografia (conjunto de princípios e técnicas empregadas para cifrar [codificar] a escrita, tornando-a ininteligível [incompreensível] para os que não tenham acesso às convenções combinadas), com cripta, palavra derivada do grego "kryptein" (esconder-se), que se refere à construção ou caverna subterrânea, geralmente uma galeria sob uma igreja.

Crypto-anarchy deriva de outra palavra, "cypherpunk" (inventada por Jude Milhon); um trocadilho da expressão "Cypher Block Chaining" (Criptografia de Blocos Encadeados) com junção à palavra "punk", na conotação de antigoverno, revolução contra o sistema ou anarquismo (e não de estilo musical, movimento cultural ou grupo social). A palavra anarquia ("anarchy"), no caso, se refere à ideia de independência, liberdade, desvencilhamento do Estado ou governo; ou seja, moeda descentralizada e livre das garras dos sistemas financeiro e político. Desse modo, "cypherpunk", apesar do nome sugestivo não se trata de um movimento de

punks da Internet; mas sim de um grupo informal de pessoas interessadas em criptografia, em especial sobre moeda de criptográfica.

A palavra **anarquismo** tem origem no termo grego *ánarkhos*, cujo significado é, aproximadamente, "sem governo".

> "O termo anarquismo tem origem na palavra grega *anarkhia*, que significa "ausência de governo". Representa o estado da sociedade ideal em que o bem comum resultaria da coerente conjugação dos interesses de cada um. A anarquia é contra a divisão em classes e por consequência é contra toda a espécie de opressão de uns sobre os outros. Vulgarmente é entendida como a situação política em que a constituição, o direito e as leis deixam de ter razão de existir. O anarquismo é uma teoria política que rejeita o poder estatal e acredita que a convivência entre os seres humanos é simplesmente determinada pela vontade e pela razão de cada um." (http://www.significados.com.br/anarquismo/).

Anarquismo é uma ideologia política que se opõe a todo tipo de hierarquia e dominação política, econômica, social e cultural, incluindo o Estado, o capitalismo, as instituições religiosas, o racismo e o patriarcado. Através de uma análise crítica da dominação, o anarquismo pretende superar a ordem social na qual esta se faz presente através de um projeto construtivo baseado na defesa da autogestão, tendo em vista a constituição de uma sociedade libertária baseada na cooperação e na ajuda mútua entre os indivíduos e onde estes possam associar-se livremente. Os meios para se alcançar os objetivos anarquistas são motivos de debates e divergências internas no anarquismo. Já o **anarcocapitalismo**, anarquismo de propriedade privada, anarquismo de livre mercado, dentre outras designações, é uma versão radical do liberalismo clássico e anarquismo individualista que tem como postulado que quaisquer formas de governo estatais são desnecessárias e prejudiciais à liberdade e ao bem-estar humano. Defende a eliminação completa do Estado em favor da soberania individual em um livre mercado.

O **liberalismo clássico**, também referido como liberalismo tradicional, liberalismo laissez-faire ou liberalismo de mercado, é uma filosofia política

e uma doutrina econômica cuja principal característica é a defesa da liberdade individual, com limitação do poder do Estado pelo império da lei (ou pela *rule of law* anglo-saxã), a igualdade de todos perante a lei, o direito de propriedade, e, em política econômica, prega o *laissez-faire*.

Laissez-faire é hoje expressão-símbolo do liberalismo econômico, na versão mais pura de capitalismo de que o mercado deve funcionar livremente, sem interferência, apenas com regulamentos suficientes para proteger os direitos de propriedade.

O **anarquismo individualista** (ou anarcoindividualismo) é uma tradição filosófica do anarquismo com ênfase no indivíduo, e sua vontade, argumentando que cada um é seu próprio mestre, interagindo com os outros através de uma associação voluntária. O anarquismo individualista refere-se a algumas tradições de pensamento dentro do movimento anarquista que priorizam o indivíduo sobre todo tipo de determinação externa, que ele é um fim em si mesmo e não um meio para uma causa, incluindo grupos, bem-comum, sociedade, tradições e sistemas ideológicos.

> "Quando falamos em “anarquia”, muitos acreditam que a expressão tem a ver com qualquer evento ou lugar carente de organização. Contudo, essa apropriação contemporânea está bem distante das teorias que integram o chamado pensamento anarquista, estabelecido logo depois que as contradições e injustiças do sistema capitalista já se mostravam visíveis no século XVIII. [...]. Em uma sociedade desprovida de Estado, a produção e o gerenciamento das riquezas seriam estipulados por meio de ações cooperativistas. Nesse contexto, todos alcançariam condições de possuírem uma vida minimamente confortável e ninguém teria sua força de trabalho explorada em benefício de um terceiro. Logo, a violência e a miséria dariam lugar para um novo mundo regido pela felicidade da ampla maioria. Assim como os socialistas, os anarquistas acreditavam na expressa necessidade de se realizar um movimento revolucionário que combatesse as autoridades vigentes. Apesar de tal concordância, os anarquistas não acreditavam que uma ditadura do proletariado fosse realmente necessária para que a sociedade comunista fosse alcançada. Em sua visão, a substituição de um governo por outro

somente fortaleceria novas formas de repressão e desigualdade." (http://brasilescola.uol.com.br/sociologia/anarquismo.htm).

"Em primeiro lugar, deve-se desprezar concepções errôneas segundo as quais "anarquia" seria sinônimo de "bagunça". Anarquia é ausência de governo e mesmo de atividade parlamentar; que os agentes políticos devem atuar diretamente em busca de manter e ampliar todas as formas de participação nos aspectos decisórios da sociedade em que vivem. Ação Direta, aliás, é o nome que adotam várias organizações anarquistas pelo mundo afora." (http://www.culturabrasil.pro.br/anarquia.htm).

"Anarquia, ao contrário do que imagina a cultura popular, nada tem a ver com a ausência de ordem. Mas sim com a ausência de coerção. Ou seja, anarquistas são basicamente contra qualquer ordem hierárquica que não seja livremente aceita." (http://www.infoescola.com/politica/anarquia/).

"Anarquismo pode ser definido como uma doutrina (conjunto de princípios políticos, sociais e culturais) que defende o fim de qualquer forma de autoridade e dominação (política, econômica, social e religiosa). Em resumo, os anarquistas defendem uma sociedade baseada na liberdade total, porém responsável." (http://www.suapesquisa.com/o_que_e/anarquismo.htm).

"O Anarquismo permite que as próprias pessoas decidam os rumos de suas vidas e construam a organização de sua vida social. Só quem sabe o que é melhor para uma pessoa é a própria pessoa. Nele, as pessoas se reúnem em grupos (se quiserem) e decidem entre si o que é melhor para todas. Essa forma de organização Anarquista chama-se AUTOGESTÃO. Autogestão, significa AUTONOMIA, ou seja, governo das pessoas por elas mesmas, sem ninguém para liderá-las ou dize-las o que podem ou não fazer. Essa forma de organização faz com que as riquezas produzidas pela sociedade fiquem diretamente nas mãos de quem pertencem, ou seja, seus produtores." (http://www.ebooksbrasil.org/eLibris/tudosobreanarquia.html).

A ideia de uma moeda descentralizada começou a ser discutida por membros de uma lista de e-mails de interessados em criptografia e foi concretizada por um programador com o pseudônimo de “Satoshi Nakamoto”; o criador do Bitcoin e co-criador do respectivo *software*.

> “A mensagem é clara: Em vez de confiar em governos, bancos centrais ou instituições de terceiros para manter o valor da moeda e garantir transações, a confiança do Bitcoin seria na matemática (‘Vires in Numeris’, como diz seu moto em Latim que significa ‘força nos números’).” (http://gizmodo.uol.com.br/tudo-sobre-o-bitcoin/).

A ideia por trás das criptomoedas é de que qualquer pessoa pode criar o dinheiro eletrônico, através da descoberta e transmissão de uma solução para um problema computacional previamente sem solução. Obviamente existem regras para essa competição pelas soluções desses problemas matemáticos e, assim, a solução efetuada outra forma não têm nenhum valor, mesmo sendo mais prática, fácil, rápida, barata, criativa ou intelectual.

> "O Bitcoin tem o potencial de mudar radicalmente o poder do governo:
> 1. De imprimir moeda como fez Juscelino Kubitschek para construir Brasília, gerando 30 anos de inflação crescente no Brasil.
> 2. De imprimir moeda para salvar seus Bancos e Banco Central, como fizeram Obama e Bernanke.
> 3. De confiscar nosso dinheiro, como fizeram em Collor, Zelia, Kirchner, Chipre e Grécia.
> 4. De financiar furos de caixa do governo com emissão de dívida pública, como fazem TODOS os governos.
> 5. De acabar com mudanças na política monetária, um dos preços mais manipulados da nossa economia, os juros.
> 6. De acabar com fraudes com cartão de crédito.
> [...]
> Mas lembre-se: O Bitcoin 2.0, 3.0 e 4.0 têm o potencial de:
> 1. Acabar com Bancos e Banco Central.
> 2. Acabar com estes Bancos Centrais torrando bilhões para salvar seus futuros colegas banqueiros, cargos que todos almejam e que quase todos no Brasil conseguiram.
> 3. Acabar com sequestros, tipo Collor e Delfim Netto.

4. Acabar com financiamento do Governo e Títulos do Tesouro Nacional como reserva de valor.

5. Acabar com políticas monetárias que não têm funcionado.

6. Acabar com especulação financeira, *hedge funds*, e todas as consultorias econômicas que assessoram Bancos e *Hedge Funds* alertando futuras mudanças na política monetária." (http://blog.kanitz.com.br/revolucao-bitcoin/).

Portanto, quem diz que a comunidade bitcoin está procurando, desejando ou esperando a regulamentação, está totalmente equivocado. Na sua essência, o bitcoin é para ser totalmente livre do controle estatal. Entretanto, recém-chegados, novatos e pessoas que "caíram de paraquedas" ou "pegaram carona" na "moda" Bitcoin, acabam por querer a regulamentação por idealizarem outros propósitos lucrativos totalmente diferentes dos ideais que inspiraram seus criadores.

- https://cointelegraph.com/news/once-libertarian-dream-bitcoin-is-now-chinese-currency.

A bitcoin tem atraído grandes investimentos do Vale do Silício (https://pt.wikipedia.org/wiki/wiki/Vale_do_Silício) e de um significativo número de seguidores em *Wall Street* (https://pt.wikipedia.org/wiki/Wall_Street). É a corrida ou batalha pelo domínio, primazia, liderança ou poderio sobre as moedas virtuais. Em razão desses novos adeptos e aportes de recursos, o bitcoin está sofrendo uma crise de identidade através do cabo de força de forças antagônicas: capitalismo selvagem x pureza de suas ambições originais. Diferentemente da maioria dos usuários ocidentais do bitcoin, os chineses são pouco ou nada apegados aos ideais libertários tão presentes na proposta de Satoshi Nakamoto (o personagem anônimo que criou o bitcoin). Nenhum chinês aderiu ao Bitcoin porque ele é libertário ou porque possui potencial para causar a queda de governos; os chineses veem o bitcoin apenas como um investimento.

A influência da China sobre a rede Bitcoin levanta preocupações sobre a independência e descentralização do Bitcoin. Na sua concepção inicial, o Bitcoin deveria existir fora do controle de qualquer governo, país, instituição, organização, entidade ou pessoa. Deveria estar baseado em todos

os lugares e, ao mesmo tempo, em nenhum lugar. Deveria ser totalmente imune às manipulações e práticas especulativas. Contudo, apesar da teoria ou utopia de uma moeda desestatizada e sem fronteiras, as empresas chinesas têm efetivamente assumido o controle majoritário da rede Bitcoin. Elas têm feito isso por meio de investimentos pesados, estratégicos e astutos em vastas fazendas de servidores (*server farms*) que estão dispersas por todo o país.

- http://www.esquerda.net/artigo/bitcoin-e-perigosa-fantasia-do-dinheiro-apolitico-por-yanis-varoufakis/42956.

Conforme análise realizada por Chainalysis (https://www.chainalysis.com/) para o *New York Times* (http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?_r=0), mais de 70% (setenta por cento) das transações na rede Bitcoin estavam (ou ainda estão) passando por apenas quatro empresas chinesas (piscinas de mineração) e a maioria desses bitcoins fluiu através de apenas duas dessas empresas. *Exchanges* (casas de câmbio) chinesas foram responsáveis por 42% (quarenta e dois por cento) de todas as transações Bitcoin no primeiro semestre de 2016. Isso lhes dá o poder de vetarem quaisquer alterações ao software e à tecnologia Bitcoin e, detalhe, os chineses divergem dos norte-americanos. O voto é de maior peso atualmente é o dos chineses.

- https://www.cryptocoinsnews.com/china-now-controls-bitcoin-thats-just-beginning/;
- https://www.cryptocoinsnews.com/chinese-miners-influence-on-the-future-of-bitcoin/;
- http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin/s/db-chinabit-slide-PQCQ.html;
- http://www.smh.com.au/business/banking-and-finance/after-4400-surge-bitcoins-fate-hinges-on-huge-chinese-miners-20160708-gq19jo.html.

Ao concentrar a maior parte do poder de mineração, menos de 5 grupos chineses têm o poder de impor restrições que podem impedir qualquer proposta de mudança pelos desenvolvedores.

- http://www.infomoney.com.br/mercados/bitcoin/noticia/4018497/conheca-maior-mineradora-bitcoin-china-que-faz-milhao-por-mes;
- http://www.tecmundo.com.br/bitcoin/73755-conheca-mina-bitcoins-chinesa-funciona-24-horas-dia.htm;
- http://motherboard.vice.com/pt_br/read/por-dentro-de-uma-mineradora-chinesa-de-bitcoins;
- http://www.bbc.com/future/story/20160504-we-looked-inside-a-secret-chinese-bitcoin-mine.

Confira a lista das 10 maiores e melhores piscinas de mineração em https://www.hobbymining.com/bitcoin-mining-pools/.

Executar piscinas de mineração (*mining pools*) confere o direito de voto sobre as alterações ao software do Bitcoin e, quanto maior a piscina, mais poder de voto. Se os membros de uma piscina discordarem das decisões, eles podem mudar para outra piscina. Entretanto, a maioria dos mineiros escolhem uma piscina com base na sua estrutura de pagamento e não pela sua política Bitcoin.

BTCC (https://www.btcc.com/), anteriormente denominada BTC China, é a *exchange* bitcoin mais antiga da China, e é agora uma das maiores do mundo em volume de negociação.

Duas bolsas chinesas, Huobi (https://www.huobi.com/) e OKCoin (https://www.okcoin.com/), em conjunto, respondem por 92% (noventa e dois por cento) do comércio global de bitcoin.

A piscina de mineração mais poderosa da China, ou de qualquer lugar no mundo, é a F2Pool (https://www.f2pool.com/); que tinha 27% (vinte e sete por cento) do poder computacional da rede em maio de 2016.

A chinesa Bitmain (https://www.bitmain.com/), que vende computadores de mineração Bitcoin, é descrita como sendo a mais valiosa empresa Bitcoin do mundo. Do mesmo proprietário (Jihan Wu), é a piscina Antpool (https://www.antpool.com/).

Baidu, o gigante da Internet chinesa, se juntou com três bancos chineses em investimentos no Bitcoin.

Não só as empresas chinesas, mas também a população (usuários) chinesa é possui um grande percentual na rede bitcoin e isso afeta a cotação da moeda.

- http://www.scmp.com/news/china/economy/article/1968733/why-bitcoin-has-become-chinas-new-darling;
- http://www.cityam.com/243166/all-roads-lead-to-china-surging-demand-pushes-bitcoin-above-700.

Senão vejamos.

Em dezembro de 2013, em razão do governo (banco central) chinês ter impedido as empresas financeiras de trabalharem com bitcoin, ocorreu a queda de 50% (cinquenta por cento) do valor do bitcoin.

- http://super.abril.com.br/blogs/rebit/2013/12/;
- http://g1.globo.com/tecnologia/noticia/2013/12/valor-do-bitcoin-cai-para-us-500-apos-china-interromper-cambio.html;
- http://br.wsj.com/articles/SB10001424052702304866904579266710645195076;
- http://canaltech.com.br/noticia/mercado/Cotacao-da-Bitcoin-despenca-apos-problemas-com-moeda-chinesa/.

Já no final de maio de 2016, em razão do banco central chinês ter intervido na taxa de câmbio de sua moeda (yuan), desvalorizando-a em relação ao dólar americano ao nível mais baixo dos últimos cinco anos, ocorreu uma, repentina e maciça, compra de bitcoins pelos chineses, com o que a cotação subiu consideravelmente pela demanda do mercado.

- http://www.segs.com.br/info-ti/18542-coinbr-explica-a-alta-historica-do-bitcoin.html;
- http://noticias.r7.com/economia/valor-da-bitcoin-toca-maxima-em-2-anos-com-demanda-chinesa-preocupada-sobre-iuan-01062016;
- http://noticias.uol.com.br/ultimas-noticias/reuters/2016/06/01/valor-da-bitcoin-toca-maxima-em-2-anos-com-demanda-chinesa-preocupada-sobre-iuan.htm;

- https://www.coinbr.net/blog/bitcoin-dispara-com-aumento-da-demanda-na-china/.

BITCOIN

A criptomoeda ("cryptocurrency") ou moeda de criptográfica ("crypto currency") é um meio de troca ("medium of exchange") usando criptografia ("cryptography") para proteger as transações e para controlar a criação de unidades adicionais da moeda ("coin" ou "currency"). Portanto, bitcoin é uma das criptomoedas ("cryptocurrencies") existentes. A palavra "altcoins", a princípio, é uma abreviação da expressão "coin alternative" (moeda alternativa); mas, na verdade, é muito mais do que isso; tratasse de uma sigla de trocadilho abreviado da expressão "bitcoin alternative" (alternativa à bitcoin). Portanto se refere às outras moedas digitais com exceção da bitcoin.

Bitcoin (símbolo/sigla: ฿ [com duas barras verticais]; abrev.: BTC ou XBT), criada em 2009, por alguém que utilizou o pseudônimo Satoshi Nakamoto (□□□□), é uma criptomoeda (c*ryptocoin*) ou moeda digital, virtual ou eletrônica (*e-cash*), baseada no conceito de moeda encriptada de Wei Dai (□ □), um engenheiro de computação, criador do b-money (http://www.weidai.com/bmoney.txt) e o desenvolvedor da biblioteca Crypto ++, CryptoPP, libcrypto ++ ou libcryptopp).

- https://en.wikipedia.org/wiki/History_of_bitcoin#Pre-history;
- https://en.bitcoin.it/wiki/Wei_Dai;
- http://www.weidai.com/;
- http://pt.bitcoinwiki.org/História_de_Bitcoin.

Coincidentemente utiliza um símbolo muito semelhante ao (฿) das moedas Baht da Tailândia e da Balboa do Panamá. De tão semelhantes, muitas pessoas se confundem. Pior, os entusiastas do Bitcoin usam o símbolo errado por falta de opção no teclado do computador. Ambos símbolos são a letra B na fonte (tipo) Cambria Math, mas a diferença básica está na quantidade de linhas verticais (colunas) que cortam a referida letra B; na bitcoin são dois traços enquanto que nas moedas de ditos países é apenas um traço. Em razão dessa confusão existe uma sugestão de Ken Shirriff (http://bitcoinsymbol.org/) para mudar o símbolo do Bitcoin para Ƀ (símbolo fonético da letra grega Beta).

- http://www.unicode.org/L2/L2015/15229-bitcoin-sign.pdf.

Além de ser uma moeda, Bitcoin também é um sistema de pagamento online baseado em protocolo de código aberto, que é independente de qualquer autoridade central. Desse modo, a bitcoin (moeda) pode ser transferida por um computador ou *smartphone* sem recurso, intervenção, intermédio ou intermediação de uma instituição bancária ou financeira e, também, independente da confiança, autorização ou regulamentação de um emissor centralizado, banco central ou governo.

O nome Bitcoin, portanto, também se refere ao software de código aberto para o uso da moeda e a respectiva rede *peer-to-peer* (P2P), pela qual os usuários podem transacionar diretamente uns com os outros sem a necessidade de um intermediário.

O nome bit não faz referência a byte, como muitos podem pensar, mas sim a uma rede de compartilhamento ponto a ponto (P2P), chamada de BitTorrent, em que cada usuário é anônimo e possui o mesmo valor. E "coin" é moeda em inglês.

Bitcoin (“B” maiúsculo) descreve o conceito da moeda criptografada ou a rede de computadores que torna possível a efetivação de transações com essa moeda; já **bitcoin** (“b” minúsculo) é a unidade monetária da moeda criptografada.

- Bitcoin: Um sistema de dinheiro eletrônico ponto a ponto - http://www.outros.net/blog/wp-content/uploads/2013/11/Bitcoin-Portugues-Brasileiro.pdf;
- Bitcoin: A Peer-to-Peer Electronic Cash System - https://bitcoin.org/bitcoin.pdf;
- http://www.infomoney.com.br/blogs/moeda-na-era-digital/post/3160782/dez-formas-explicar-que-bitcoin.

Na prática não é comum esse rigor na forma da escrita da palavra bitcoin (letra maiúscula ou minúscula e quando usar cada uma) e, pior, até há certa liberdade, ou confusão mesmo, sobre a forma de escrever. Desse modo, a diferenciação possui a intenção de sermos mais didáticos nas explanações.

Mas podemos ter cometido algum deslize por descuido ou ante o vício de linguagem na literatura existente no meio.

Uma bitcoin é um bem digital que não pode ser reproduzido ou falsificado; sua titularidade de propriedade está devidamente registrada na *Blockchain* (cadeia de blocos ou livro contábil). Tal como a eletricidade que é invisível, imaterial e impalpável, o Bitcoin por ser um programa de computador e respectivos dados computacionais, não pode ser pego nas mãos, apalpado e visto diretamente; mas tão somente de forma indireta através de dispositivos computacionais e pelas coisas que se pode fazer com ela ou através dela. Não precisamos ver os dados trafegados pelo ar para sabermos que o Wi-Fi existe e funciona. Do mesmo modo, não é preciso vermos as ondas de rádios, de tv e de celulares viajando pelo ar para sabermos que elas existem e funcionam.

Por outras palavras, as pessoas podem falar que não conseguem ver a bitcoin, mas elas também não veem as ondas de rádio em torno delas, os dados de wifi e celular trafegando próximos delas, etc. Apesar de não verem tais coisas, sabem que elas existem e estão ali. E, de modo semelhante à bitcoin, através de aparelhos específicos conseguem ouvir as ondas de rádio, assistir os dados receptados por um aparelho de TV, receber um fax, conversarem no celular, acessar a Internet sem fio, etc.

Diferente da maioria das moedas, a bitcoin não depende da confiança em nenhum emissor centralizado. Ela é totalmente independente de qualquer país. Por outras palavras, a bitcoin, portanto, é diferente das moedas (dinheiro) com as quais estamos acostumados; pois sua emissão se dá de forma descentralizada. Ela não depende de nenhum banco central e não possui lastro físico (seja ouro, seja cédulas).

- http://www.bitcoinnews.com.br/bitcoinbrasil/o-bitcoin-e-verdadeiramente-descentralizado-sim-entenda-porque-isso-e-importante/.

Bitcoins não são regulamentadas e ninguém é obrigado a aceitá-las; é uma decisão voluntária.

Na sua essência, contudo, ele nada mais é do que um protocolo, um conjunto de regras pelas quais se comunicam computadores conectados à

rede *peer-to-peer* do sistema. Não há um servidor central monitorando o cumprimento das normas. Primeiro, porque elas incentivam o comportamento honesto; segundo, porque todos são monitorados por todos. A confiança e a segurança são alcançadas de forma descentralizada, graças ao uso engenhoso da criptografia moderna, e sem que seja necessário conhecer a identidade dos participantes.

Por outras palavras, o Bitcoin é um protocolo P2P (*peer-to-peer*, ponto a ponto ou de igual para igual) que não pode ser desligado pelas autoridades. Não existe um servidor central responsável pelo Bitcoin: todos os participantes do protocolo Bitcoin são ao mesmo tempo clientes e servidores desse sistema. O Bitcoin é um sistema de comunicação que funciona com base na Internet. Da mesma forma que não existe uma empresa responsável pelo e-mail, não existe uma empresa responsável pelo Bitcoin. Ele é apenas um protocolo de comunicação.

Peer-to-peer (de igual para igual ou de par a par) é um formato de rede de computadores em que a principal característica é descentralização das funções convencionais de rede, onde o computador de cada usuário conectado acaba por realizar funções de servidor e de cliente ao mesmo tempo. Seu principal objetivo é a transmissão de arquivos e seu surgimento possibilitou o compartilhamento em massa de músicas e filmes. Com a crescente utilização da rede P2P para este fim, cada vez mais surgem programas para este fim, porém nem sempre eles atendem às expectativas do usuário. Diversas redes operam hoje em dia nestes moldes de compartilhamento, entre elas Kademlia, Gnutela, Kad Network e SoulSeek. Alguns exemplos de compartilhamento P2P são Napster, eMule, LimeWire, Kazaa, Ares Galaxy, Shareaza, DreaMule, iMesh e Morpheus.

- http://super.abril.com.br/tecnologia/compartilhamento-de-arquivos-troca-troca/;
- https://pt.wikipedia.org/wiki/Peer-to-peer.

Os protocolos para acessar as páginas da Internet e para enviar e-mails funcionam em modo cliente – servidor; ou seja, existe um cliente (usuário) que se comunica com um servidor (por exemplo, um servidor web que atende a requisição do usuário de visualizar uma página da Internet). Diante disso, é fácil para as autoridades tirarem um site específico do ar através do

servidor responsável (bloquear o site no servidor ou desativar o servidor). Entretanto, existem protocolos que não fazem essa distinção; ou seja, todo cliente é também um servidor. Esses protocolos são chamados de *peer-to-peer* ou P2P. Um exemplo é o protocolo Bittorrent, que é usado para compartilhamento de arquivos.Ao contrário do protocolo cliente – servidor, é muito mais complicado e difícil de interferir no funcionamento de um protocolo P2P em razão de inexistir servidor central. Por essa razão é que o protocolo Bittorrent é usado para compartilhamento de músicas, filmes e séries (leia-se pirataria).

O bitcoin, portanto, forma uma rede P2P conectando cada carteira com uma quantidade razoável de outras carteiras, de forma que as mensagens entre uma e outra consigam percorrer toda a rede. De uma forma simplificada, as transações criadas por uma carteira são enviadas a todas as outras conectadas a ela. Cada uma dessas carteiras, por sua vez, retransmite as transações recebidas de uma carteira conectada para todas as outras e assim sucessivamente, até que toda a rede tenha recebido uma cópia daquela transação. Os blocos minerados passam pelo mesmo processo. A diferença é que as transações ficam armazenadas em uma memória temporária e os blocos são armazenados na *Blockchain* (contabilidade pública descentralizada), de forma permanente.

Desse modo, o Bitcoin usa um banco de dados distribuídos espalhados pelos nós da rede *peer-to-peer* para registrar as transações e usa criptografia para prover funções básicas de segurança, como certificar que as bitcoins só podem ser gastas pelo dono e, inclusive, evitar os gastos duplos ("double spends").

O Bitcoin, portanto, compreende um sistema que opera ligado à Internet de modo a propiciar a emissão e a circulação de unidades da moeda digital de mesmo nome (as bitcoins), tendo embutido na tecnologia um meio de pagamento para que sejam livremente enviadas e recebidas. Com o Bitcoin, é possível enviar valores (bitcoins) para qualquer parte do mundo ligado à Internet sem esforço, burocracia ou custos elevados.

Os diferenciais da bitcoin estão no fato de ser uma moeda inteiramente digital, tanto em sua emissão quanto em sua circulação, e que não depende

de intermediários para garantir que tudo funcione como o planejado. Ou seja, com a criação do Bitcoin, pela primeira vez se tornou possível transmitir valores de maneira segura entre quaisquer dois pontos do mundo ligados à Internet sem que um banco tenha que estar por trás, diminuindo substancialmente os custos operacionais, a burocracia e o risco sistêmico do processo.

Além disso, pode-se dizer que a bitcoin é uma moeda politicamente neutra, já que é um sistema global gerido exclusivamente por seus usuários, quando fazem uso dos aplicativos que se conectam à rede P2P. Isto é, ela não está ligada a qualquer país, não é controlada por uma empresa em particular e existirá sempre em quantidade limitada e conhecida, eliminando a existência de um banco central para cuidar dessas variáveis.

Em sua essência, a bitcoin é uma moeda com implementos de criptografia com especificações de código aberto (*open code*) e software que depende totalmente de uma rede *peer-to-peer* para a validação e processamento das transações (transferências de créditos).

Uma bitcoin é simplesmente um hash SHA-256 (uma sequência alfanumérica bem grande) em formato hexadecimal. As bitcoins de uma pessoa são armazenadas em um arquivo especial chamado de carteira (*wallet*). Esta contém endereçamento onde o usuário envia e recebe bitcoins com uma senha ou chave privada (*private key*) de conhecimento apenas dele, necessários para que as bitcoins possam ser transferidas para outra pessoa. Isso significa que uma pessoa que tem bitcoins não armazena a bitcoin em si, mas uma chave digital, que todo mundo está em consenso (de acordo ou unânime) que tem autoridade sobre um determinado valor em bitcoins.

O protocolo Bitcoin define uma unidade digital, chamada de bitcoin (em minúsculo), e o protocolo faz três coisas com essas bitcoins:

1) Lembrar que determinadas chave digitais tem um valor em bitcoin associados a elas;

2) Permitir a transferência de valores em bitcoin de uma chave digital para outra;

3) Gerar valores em bitcoin e distribui-los entre as chaves digitais dos seus usuários.

Todo usuário do protocolo Bitcoin se conecta a vários outros usuários do protocolo P2P através da Internet. Na primeira vez que o usuário entra no serviço, ele baixa dos outros usuários uma cópia completa do banco de dados (Blockchain) contendo absolutamente todos as chaves digitais que possuem propriedade sobre algum valor em Bitcoin. Desse modo, as informações sobre as transações (transferências de créditos entre os usuários) passam de um usuário para outro de forma descentralizada.

Pelo fato de inexistir fronteiras (físicas, virtuais ou políticas) e nem qualquer tipo de barreira ou bloqueio para as transações, os usuários podem efetuarem transações com qualquer pessoa de qualquer parte do mundo. Além de inexistir burocracias (comparecer numa agência bancária para assinar papéis), tornar desnecessário o uso de um ATM - *Automated Teller Machine* [caixa multibanco]) com um cartão (bancário ou de crédito) e dispensar o uso de PayPal ou similares, esse procedimento é muito mais simples, rápido e barato (sem impostos, taxas de conversões e tarifas bancárias, etc.); tal como, por exemplo, enviar um e-mail.

Evidentemente esse sistema possui muitas vantagens como a liberdade de pagamento (já que pode ser realizado instantaneamente, em qualquer lugar, a qualquer momento, sem feriados e nem fronteiras), taxas baixas (pagamentos com bitcoins são processados sem taxas ou com taxas pequenas quando se requer prioridade na confirmação da transação), menos riscos para os comerciantes (as transações são seguras, irreversíveis e não contêm informações confidenciais ou pessoais dos clientes), segurança e controle (os usuários tem controle total de suas transações, sendo impossível forçar cobranças indesejadas), transparência e neutralidade (toda informação em relação a própria moeda está facilmente disponível na *Blockchain* para qualquer um verificar e usar em tempo real. Nenhum indivíduo ou organização pode controlar ou manipular o protocolo Bitcoin, porque este é criptograficamente seguro. Entretanto, por outro lado, também há desvantagens, como o grau de aceitação (muitos ainda desconhecem), a volatilidade (seu valor pode ser significantemente alterado em razão de

eventos relativamente pequenos), seu desenvolvimento incompleto (estando em processo de aprimoramento), etc.

Uma ressalva. Como as altcoins costumam ser baseadas no Bitcoin e na sua *Blockchain*, muitos dos conceitos, protocolos, terminologias (por exemplos: mineração, blocos, carteira, exchange, consenso, prova, P2P, *fork*, hash, etc.) e equipamentos são os mesmos ou muito semelhantes. Desse modo, aprender sobre o Bitcoin e a sua *Blockchain* é a base para poder compreender as altcoins e todo o ecossistema surgido a partir do Bitcoin e sua *Blockchain*.

Para entender melhor, ou se profundar, sobre o que são as bitcoins e como elas são feitas, confira os capítulos: "*HASH*", "CERTIFICADOS DIGITAIS", "*PEER-TO-PEER* (P2P)", "COMO A BITCOIN É FEITA?", "*BLOCKCHAIN*" e "COMO MINERAR BITCOINS E ALTCOINS".

PEER-TO-PEER (P2P)

Para fazer um ***download*** (receber ou "baixar" dados e arquivos da Internet) convencional é necessário que o dispositivo (computador, notebook, tablet, smartphone, etc.) esteja conectado a um servidor (computador hospedeiro) para poder transferir ou salvar uma cópia do arquivo pretendido (o arquivo original permanece no servidor). A título de esclarecimento, ***upload*** é o caminho inverso do download; ou seja, é o envio de dados e arquivos.

Servidor é o serviço de hospedagem e disponibilidade de conteúdo na Internet. O servidor, portanto, é o intermediário entre o *download* e o *upload*. Por outras palavras, o servidor faz a ligação do computador do usuário a algum site, portal, sistema, rede, dados ou arquivos. Explica-se. Os sites, portais, sistemas, redes, dados e arquivos disponibilizados na Internet (*on line*) costumam estar armazenados (arquivados, salvos, disponibilizados) em algum servidor (serviço de hospedagem). Portanto, ao navegar na Internet se está acessando diferentes servidores que contém os respectivos dados; ou seja, os sites estão em um servidor e o computador do usuário está fazendo o *download* de referidos sites. Entretanto, o servidor também pode se referir ao computador que controla o acesso de uma determinada rede (terminais ligados ao servidor) à Internet; ou seja, o computador que concede o acesso à Internet aos equipamentos interligados a ele. Procedimento comum em empresas onde os computadores dos funcionários não se conectam diretamente à Internet e nem salvam arquivos em seus próprios discos rígidos (HDs - *Hard Disks*), mas tudo é feito no servidor e através dele. Esse tipo de servidor é semelhante à uma central PABX para os terminais (ramais) telefônicos. Frisa-se que **provedor** é tão somente quem presta o serviço de acesso (conexão) à Internet.

Para que essa comunicação entre computadores seja possível, é necessário que todos eles “falem um mesmo idioma” ou utilizem o mesmo procedimento padrão, a isso se dá o nome de **protocolo**. Portanto, protocolo é uma convenção (acordo) que define como os sistemas computacionais realizam uma conexão, comunicação e/ou transferência de dados.

"Os protocolos funcionam como línguas universais, que permitem que os vários computadores diferentes da Internet consigam se comunicar para realizar diferentes tarefas específicas.

Outro exemplo de protocolo famoso é o email: não importa o cliente de email que você use, se você usa o Gmail, Hotmail, ou o e-mail da sua empresa, seu email chega em qualquer caixa postal do mundo. Isso só é possível porque os servidores de email espalhados pela internet todos "falam" o mesmo protocolo de email.

Os protocolos para você acessar páginas da internet e para você enviar email funcionam em modo cliente-servidor: existe um cliente (você) que se comunica com um servidor (por exemplo, o servidor web que te entregou essa página que você está lendo agora, ou os servidores do Gmail). Existem protocolos que não fazem essa distinção: todo cliente é também um servidor. Esses protocolos são chamados de peer-to-peer, ou p2p. Um exemplo é o protocolo Bittorrent, que é usado para compartilhamento de arquivos. Para as autoridades é fácil tirar um site específico do ar (basta mandar desligar o servidor responsável pelo site), mas é muito difícil interferir no funcionamento de um protocolo p2p, pois não há nenhum servidor central que eles podem mandar desligar. É justamente por esse motivo que o protocolo Bittorrent é usado para compartilhamento de músicas, filmes e séries: os detentores de direitos autorais podem chorar e espernear junto às autoridades, mas elas não têm como impedir o funcionamento de um protocolo p2p.

O Bitcoin é um protocolo também, e um protocolo p2p, desses que não pode ser desligado pelas autoridades. Não existe um servidor central responsável pelo Bitcoin: todos os participantes do protocolo Bitcoin são ao mesmo tempo clientes e servidores desse sistema. O Bitcoin é um sistema de comunicação que funciona em cima da Internet, e nada mais que isso. Da mesma forma que não existe uma empresa responsável pelo e-mail, não existe uma empresa responsável pelo Bitcoin. Ele é apenas um protocolo de comunicação." (http://blog.bussoladoinvestidor.com.br/o-que-e-bitcoin/#o-que-e-bitcoin).

HTTP (*Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto) **e FTP** (*File Transfer Protocol* ou Protocolo de Transferência de Arquivos) são formas muito semelhantes de comunicação entre

computadores para troca de arquivos. Para que a transferência de dados na Internet seja realizada, os protocolos (linguagens utilizadas para que os computadores consigam se comunicar e se entenderem) HTTP e FTP necessitam de outros dois protocolos de rede: TCP (*Transmission Control Protocol* ou Protocolo de Controle de Transmissão) e IP (*Internet Protocol* ou Protocolo de Internet). **IP** é um número exclusivo (único) que identifica um dispositivo em uma rede (um computador, impressora, roteador, etc.) e é composto por 4 números (até 3 dígitos) e separados por "." (ponto). Os valores que podem assumir estes números variam entre 0 e 255. Já **porta** é a identificação de um determinado *software* em um computador dentro da rede.

O HTTP é um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, principalmente na *World Wide Web* (Internet). Ele é mais adequado para receber muitos dados e arquivos e enviar apenas uma pequena quantidade deles. Já o FTP é uma via de duplo sentido, podendo copiar ou mover arquivos de um servidor para um computador cliente, bem como carregar ou transferir arquivos de um cliente para um servidor; é semelhante ao compartilhamento de pastas numa rede local e, até mesmo, ao aplicativo Windows Explorer ou Explorador de Arquivos do sistema Windows, pelo qual se navega pelas pastas existentes no computador e manuseia-se os arquivos existentes nessas pastas. Recorda-se que pasta compartilhada é aquela que pode ser acessada por outros usuários ou computadores dentro de uma rede. Desse modo o FTP é mais usado por quem tem site ou envia muitos arquivos para um servidor, vez que por essa via a transferência de dados é mais rápida. Todo endereço (URL - *Uniform Resource Locator* ou Localizador Uniforme de Recursos) na Internet que possui o prefixo "www" ou a terminação "HTML" utiliza o HTTP. Enquanto que a enorme maioria dos dados e arquivos transferidos via HTTP são de uso provisório ou temporário (ou seja, são considerados como inúteis [lixo] e até podem ser deletados automaticamente após fechar o navegador (*browser*) ou desligar o computador), exceto se o usuário decidir salvar, no FTP todos os dados e arquivos são salvos automaticamente. Diferentemente de transferências via HTTP, um cliente torrent faz diversos pedidos em diferentes sockets (pontos finais de uma rede, ou seja, a localização de um arquivo). Isso significa mais de uma fonte para se “baixar” os arquivos. Outra diferença é que o protocolo torrent baixa de uma maneira não sequencial e vai “montando” o arquivo

como se fosse um quebra-cabeça, juntando as diferentes partes dos arquivos baixados.

Ressalta-se que o protocolo **HTTPS** (*Hyper Text Transfer - Secure*) é uma implementação do protocolo HTTP sobre uma camada SSL (*Secure Sockets Layer*) ou do TLS (*Transport Layer Security*), que permite que os dados sejam transmitidos através de uma conexão criptografada e se verifique a autenticidade do servidor e do cliente através de certificados digitais; sendo, portanto, em regra utilizado para evitar que a informação trocada entre o cliente e o servidor seja usada por terceiros. Os certificados para servidores Web ou simplesmente Certificados SSL/TLS, são os que identificam os web sites e garantem a autenticidade, privacidade e a integridade dos dados de um portal na rede, proporcionando aos visitantes a garantia de que estão realmente acessando um site original e seguro, e não a uma cópia (site *fake* ou falso) operada por fraudadores (golpistas). Pelo protocolo SSL/TLS o servidor do site que está sendo acessado envia uma chave pública ao *browser* (navegador), usada por este para enviar uma chamada secreta, criada aleatoriamente. Uma chave criptográfica é um valor secreto que modifica um algoritmo de encriptação. Exemplificando, a fechadura mecânica (exemplo, da porta de uma casa) tem uma série de pinos (engrenagens). Cada um desses pinos possui múltiplas posições possíveis. Quando alguém põe a chave certa na fechadura, cada um dos pinos é movido para uma posição específica, tal como o segredo giratório de um cofre. Se as posições ditadas pela chave são as que a fechadura precisa para ser aberta, ela abre, caso contrário, não. Por outras palavras, geralmente, os sites iniciam suas URLs (endereços) com "http" sem o "s". Desse modo, nas páginas de pagamentos, onde é necessário ter segurança, o "s" (de segurança) aparece ao lado do "http" da URL. Assim na página da Internet onde o consumidor digita os dados do cartão de crédito ou outras informações pessoais, aparece um "s" após o "http" no endereço da Web dessa página. Isso indica que a página possui criptografia (medida de segurança que codifica [senha, linguagem secreta] os dados trafegados na Internet). Para mostrar que a página é segura, a maioria dos navegadores (*browsers*), exibe o desenho de um “cadeadinho” fechado (ou um escudo) ao lado do endereço ou no canto inferior direito da janela. Esse é o Certificado (Digital) SSL/TLS. Mesmo se o navegador não mostrar esse desenho (cadeado), mas constar "https", presume-se que o site é seguro. Quando a

barra do navegador (Internet Explorer, Firefox, Google Chrome, Opera, KDE, etc.) muda para a cor verde quer dizer que o site visitado tem um Certificado Digital de Validação Avançada (SSL-EV - *Secure Socket Layer - Extended Validation* = Protocolo de Camada de Sockets Segura com Validação Estendida) e passou por uma validação de dados muito mais exigente e criteriosa (definidas pelo CA/Browser Fórum) através de autoridades certificadoras como a Certisign, Geotrust, VeriSign, Comodo, etc. Já se ficar vermelho, alerta a existência de algum problema de identidade ou risco de segurança.

Peer-to-peer (P2P, par-a-par ou ponto-a-ponto) é uma arquitetura (estrutura) de rede (computadores interligados) ou de sistemas distribuídos caracterizada pela descentralização das funções na rede, onde cada nó realiza tanto funções de servidor quanto de cliente (infraestrutura associada de arquivos em rede). Daí o nome “ponto a ponto”.

Nó, nodo ou *node* é cada um dos dispositivos que formam a rede. Se refere, portanto, a cada ponto de conexões múltiplas e simultâneas. Os nós são semelhantes aos terminais rodoviários ou aos aeroportos, só que em vez de envolver transporte de pessoas, animais e coisas, estão relacionados à transmissão, recepção e compartilhamento de dados. Frisa-se que tais transferências de dados não são unilaterais (via de mão única ou monólogo) e, nem mesmo bilaterais (via de mão dupla ou diálogo), mas múltiplas ou multifacetárias; tal qual um trevo rodoviário difere de um cruzamento (intersecção ou entroncamento) simples (comum ou padrão) por consistir no cruzamento de várias vias (e não apenas de duas). Desse modo, não se restringe (limita) à uma única direção, linha reta ou um (único) computador se comunicar com outro (único) computador; mas de vários computadores se comunicando entre si, por todos os lados, tudo em tempo real (instantâneo), todos ao mesmo tempo e onde cada participante serve de ponte (intermediário, ponto de ligação, central telefônica, local de baldeação ou trevo rodoviário) de contato para os demais usuários. Dessa forma, diferentemente dos elos de uma corrente, que quando um elo se rompe a corrente se quebra, no caso dos nós da rede, quando um (e até mesmo quando vários) dos nós se desconecta, a rede continua funcionando (operante); tal como quando se interdita uma rua e existem diversos outros caminhos alternativos.

De forma semelhante é a condução (transmissão) da energia elétrica pela fiação; quando um elétron começa a oscilar, ele repassa (retransmite, propaga) seu movimento ao vizinho e, assim, sucessivamente até que a corrente elétrica chegue ao seu destino.

O nome "**rede**" não é por acaso, mas faz referência à antiga arte de tecelagem, onde ocorre o entrelaçamento (cruzamento) de fios formando uma malha. Cada fio ou linha representa o caminho (rota, estrada, rodovia) por onde os dados trafegam (transitam), tal como se fosse a fiação de uma linha telefônica fixa. Assim, cada cruzamento (encruzilhada, intersecção, trevo, etc.) dessas linhas é um nó e o conjunto (união) dos nós forma a malha (rede) viária do tráfego de dados. Portanto os dados transitam de computador a computador, de nó a nó ou de ponto-a-ponto. É semelhante ao passatempo de ligar os pontos através do ato de ir traçando uma linha conectando, um a um, até chegar onde se quer; mas cada um tem seu próprio destino e escolhe seu próprio trajeto (percurso). Pense, ainda, num rio cheio de pedras grandes, firmes e acima d'água, onde as pessoas pulam de pedra em pedra para atravessarem de uma margem à outra sem se molharem.

> Existem programas de *tracert* (*traceroute* ou rota do traço), como o NeoTrace (http://neotrace-pro.softonic.com.br/), que mostram o caminho percorrido pelos dados; ou seja, os intermediários entre o computador do usuário até o computador de destino.

Exemplificando melhor, faça de conta que ainda não existisse nenhuma estrada, rua ou rodovia e, assim, cada proprietário ou usuário de imóvel (residência, comércio, propriedade rural, etc.) fizesse uma estrada para ter contato com seus vizinhos e demais locais de seu interesse. Desse modo, referidas estradas não são utilizadas somente por quem as fez e não somente para contatar aqueles pontos próximos, mas são utilizadas por todos para se locomoverem para qualquer lugar.

Apesar do nome ("rede"), ditos cruzamentos não são "bonitinhos" ou "quadradinhos" como uma rede (ou tela) literal, onde várias linhas (ou fios), horizontais e verticais, se cruzam de forma harmônica, alinhada e com espaçamento idêntico. Por outras palavras, não possui um formato

geométrico organizado como, por exemplo, do favo de uma colmeia, que é formado por vários hexágonos (polígonos com seis lados) idênticos. O formato (desenho) da rede é aleatório e totalmente irregular.

O formato real da rede se assemelha ao das vias de trânsito de automóveis, principalmente das não urbanas; vez que se trata somente dos computadores que integram a mesma e estão espalhados pelo mundo. Em razão disso o termo teia de aranha (ao invés da palavra rede) é muito menos impreciso por dar uma visualização mais próxima do formato real. Entretanto, o formato comparativo mais idêntico da rede é o cérebro; ou seja, as várias conexões múltiplas entre os neurônios. Deste modo, como o cérebro é a união de bilhões de neurônios, a rede é a união de inúmeros nós. Cada neurônio, além da bainha de mielina, possui vários dendritos (terminais de recepção) e axônios (terminais de transmissão), ambos os dois últimos no formato semelhante de raízes de árvores, e através de todos esses conectores os neurônios trocam e transitam informações entre si de qualquer região do cérebro (lóbulo [ou lobo] frontal, lóbulo parietal, lóbulo occipital, gânglio da base, córtex motor, cerebelo, etc.) e de qualquer sensor (olfato, audição, visão, paladar, tato, etc.) do corpo. Detalhe, do neurônio inicial até o de destino, existem vários outros neurônios intermediando a comunicação. Assim, de modo similar cada neurônio do cérebro é como se fosse cada nó da rede. Apesar disso, a palavra rede é mais comumente usada.

Em suma, portanto, **P2P** trata-se uma rede de computadores que compartilham informações e arquivos pela internet sem um servidor geral que os armazene; ou seja, todos os usuários (clientes) servem de servidores uns para os outros para manterem a rede funcionando. Desse modo, cada estação possui capacidades e responsabilidades equivalentes; ou seja, são dedicados a servirem dados uns aos outros. Exemplos de P2P são os softwares como Napster, Kazaa, eMule, Gnutella, LimeWire, Shareaza, Bittorrent, iMesh, Ares Galaxy, DreaMule, Soulseek, etc.

O primeiro uso da expressão *Peer-to-Peer* foi em 1984, com o desenvolvimento do projeto *Advanced Peer-to-Peer Networking Architecture* na IBM.

"*Peer-to-Peer* existiu sempre, mas na altura não era reconhecido como tal; servidores com endereços IP fixos ou determináveis podia sempre comunicar com outros servidores para usufruir dos serviços disponibilizados. Um número de aplicações pre-P2P, como o correio electrónico e o serviço de resolução de nomes (DNS), assentavam nestas capacidades para oferecer um serviço numa rede distribuída, mas uma aplicação, a USENET, destaca-se das outras.

A USENET foi criada em 1979 por estudantes universitários dos Estados Unidos da América para permitir que dois computadores trocassem informação nos primórdios antes da conectividade oferecida pela Internet. A primeira iteração consistia na capacidade de um computador ligar via modem a outro, pesquisar documentos novos e transferir estes documentos para armazenamento local. Este processo era efectuado de noite para poupar nas chamadas telefónicas. Este sistema evoluiu para o sistema de massivo de newsgroups que conhecemos hoje em dia. Por muito grande que seja, a USENET tem algumas propriedades que ajudam a distinguir-la como sendo provavelmente o primeiro sistema P2P. Na USENET não existe nenhuma autoridade central, a distribuição dos documentos é gerida por cada nó e o conteúdo da rede é replicada (totalmente ou em parte) por todos os nós.

Uma das coisas mais interessantes sobre a USENET é que não é nada de especial. A USENET não é nenhuma aplicação ou um conjunto de servidores de rede. Embora necessite de servidores para funcionar, estes não a definem. Na alma deste sistema está a possibilidade das máquinas comunicarem para permitir aos utilizadores afixar mensagens que são distribuídas pela rede. A definição do *Network News Transport Protocol* (IETF RFC 977), o maior número possível de máquinas são capazes de participar independentemente e fornecer serviços. Esta distribuição de responsabilidade é o que faz a USENET sobressair como a primeira aplicação em que se reconhecem traços da tecnologia P2P.

Desde a USENET, as aplicações mais populares que usam tecnologia P2P podem ser agrupadas em três categorias: *Instance Messaging*, partilha de ficheiros e computação distribuída." (https://sites.google.com/site/sitesrecord/o-que-e-peer-to-peer-computing).

O termo é utilizado em diferentes tecnologias que adotam um modelo conceitual "par-a-par", tal como o protocolo NNTP (para Usenet News), SMTP (para envio de e-mail), e sistemas de troca de mensagens instantâneas (ICQ, MSN, WhatsApp, Telegram, Skype, Hangouts, Viber, Line, WeChat, ChatOn, KakaoTalk, Kik Messenger, GroupMe, SnapChat, BBM - BlackBerry Messenger, etc.). Porém, o termo tornou-se popular com o surgimento de aplicações de compartilhamento de arquivo, em outras palavras, programas que possibilitam a distribuição de arquivos em rede, permitindo o acesso de qualquer usuário dessa rede a este recurso.

Saiba mais em https://pt.wikipedia.org/wiki/Peer-to-peer.

A rede **Torrent** se diferencia da rede P2P (*peer-to-peer*) comum pela forma como encontra e "baixa" os arquivos. Enquanto que no protocolo BitTorrent (ou simplesmente Torrent) é utilizado um servidor de mediação entre os usuários chamado de *tracker* (ou rastreador), para encontrar os arquivos (completos e fragmentos dele) armazenados nos computadores dos outros usuários; na rede P2P as transmissões são diretas, sem um servidor centralizado, onde todos os usuários buscam e fazem *download* de arquivos nas pastas compartilhadas entre si nos computadores integrantes da rede. E na rede P2P os arquivos são transmitidos por inteiro numa fila de cronológica sequencial de espera. Desse modo, o computador do usuário é direcionado por um computador central (*tracker*) para outros computadores no mundo inteiro que tenham partes do arquivo desejado (*peers*) ou ele completo (*seeds*). Todos que fazem ou já terminaram o *download* (*leecher*) também fazem *upload* (*seeder*) ao mesmo tempo. Os arquivos transferidos são divididos em partes e cada pessoa que tem tal arquivo ajuda a fazer o *upload* a outros usuários. A primeira pessoa a disponibilizar um arquivo para *download* é conhecida como o primeiro *seed*. Alguém faz o *download* desse arquivo e também passa a disponibilizá-lo, tornando-se mais um *seed*. Basicamente, todas as pessoas que baixaram o torrent enviam pedaços dele para outras. No final do *download*, o cliente unifica os pedaços. Isso reduz significantemente o consumo de banda do distribuidor original do arquivo, não sendo necessário que o mesmo fique armazenado em um servidor. Quanto mais *seeds* houver de um mesmo arquivo, mais rápidos e eficientes serão os *downloads*, pois mais pessoas estarão disponibilizando o mesmo.

Para baixar arquivos usando o protocolo BitTorrent, é preciso ter um *software* cliente (uTorrent, BitComet, Vuze, BitTorrent, Azureus, etc.), que é responsável por abrir arquivos no formato "torrent" e por se conectar a *trackers*, *seeds* e *peers* na rede. Entretanto, o navegador Opera (http://www.opera.com/pt-br) "baixa" automaticamente torrents como se fossem *downloads* comuns e, também, existem diversos sites onde os usuários disponibilizam seus arquivos torrent através de Magnet Links (Links Magnéticos). Porém, como o número desses serviços é crescente, foi criado outro tipo de serviço: o de pesquisar arquivos nesses sites sem a necessidade de vasculhar um por um. Entre alguns dos mais populares estão: The Pirate Bay, YouTorrent, Torrents.to, isoHunt e Mininova.

Seed (ou *seeding*): é a denominação dada ao computador que possui um arquivo completo compartilhado, como o computador que primeiramente disponibilizou o arquivo e os outros que o baixaram por inteiro.

Peer é cada computador que compartilha arquivos na rede Torrent; ou seja, um ponto ou um nó da rede.

Leech (ou *leeching*) é a denominação dada ao momento em que um computador faz *download*.

Tracker é o servidor que é responsável por organizar os arquivos disponíveis e direcionar os downloads. É um dos principais responsáveis pelo funcionamento da rede do BitTorrent, pois ele praticamente gerencia a distribuição de arquivos porque possui informações sobre onde estão os computadores com os arquivos compartilhados num determinado momento.

Swarm é o conjunto de computadores que estão compartilhando o mesmo arquivo. Assim, por exemplo, se arquivo.pdf está sendo compartilhado por 3 *seeds* (sementes) e por 7 *peers* (pares), o *swarm* do arquivo contém 10 computadores (3 *seeds* + 7 *peers*).

As transações do Bitcoin são verificadas pelos nós da rede *peer-to-peer* e, depois, registradas em um banco de dados distribuídos, um verdadeiro

livro razão de contabilidade, com acesso público, conhecido como *Blockchain*.

Para entender melhor, ou se profundar, sobre o que são as bitcoins e como elas são feitas, confira os capítulos: “*HASH*", "CERTIFICADOS DIGITAIS", "BITCOIN", "COMO A BITCOIN É FEITA?", "*BLOCKCHAIN*" e "COMO MINERAR BITCOINS E ALTCOINS".

COMO A BITCOIN É FEITA?

Da mesma forma que numa moeda convencional onde existem instituições responsáveis pela emissão do dinheiro, no caso das moedas criptográficas a emissão é feita pelos mineradores (*miners*); que necessitam investir em *hardware* com alta capacidade de processamento, conexão à Internet com boa velocidade, eletricidade e tempo de processamento para gerar novas unidades da moeda.

O mecanismo utilizado pelo Bitcoin para geração de novos blocos chama-se PoW - *Proof of Work* (prova de trabalho); ou seja, usar o trabalho de computação para a geração de novos blocos. O conceito de prova de trabalho está inserido em vários algoritmos de mineração; tais como, por exxmplos: o SHA-256 utilizado na mineração do Bitcoin; o Script utilizado no Litecoin e no Dogecoin; e, o Crypto-Night utilizado nas Criptocoins 2.0: Bytecoin, Monero, MonetaVerde, etc. Em 2012, foi lançada a criptomoeda PeerCoin, que propôs o sistema de PoS – *Proof of Stake* (prova de propriedade). Algumas criptomoedas adotam sistemas mistos (PoW e PoS), como é o caso da Ethereum (segunda criptomoeda mais valiosa do mercado). Já outras criaram provas de consenso.

A geração de bitcoins é feita através da participação no protocolo de segurança da rede, mediante a validação das transações para evitar os gastos duplos (*double spends*). Quem assim faz são denominados mineradores. Esses usuários especiais trabalham com um arquivo que contém as últimas (recentes) transações realizadas, mas que ainda não foram validadas. Desse modo, o trabalho dos mineradores é encontrar a chave de validação criptográfica para esse arquivo, que só pode ser encontrada através de bilhões de tentativas e erros (*brutal force* ou força bruta). Para conseguir isso (encontrar a chave), o minerador gasta muito em energia elétrica e poder computacional.

Na verdade, portanto, o trabalho do minerador é descobrir a solução de um problema (operação ou fórmula) matemático, similar àquelas equações onde se tem que descobrir o valor do x. Desse modo, o minerador não descobre ou encontra um novo bloco, mas descobre ou encontra a solução da fórmula matemática daquela rodada (partida) de 10 (dez) minutos.

- https://bitcoinpt.blogspot.com/2013/06/que-problema-e-resolvido-pela-mineracao.html;
- https://www.tecmundo.com.br/bitcoin/63804-engenheiro-mostra-minerar-bitcoin-lapis-papel.htm;
- http://exame.abril.com.br/tecnologia/e-possivel-minerar-bitcoin-usando-lapis-e-papel/.

E, quando não se emitirem mais unidades de bitcoin (quando atingir o limite arbitrário de 21 milhões de unidades), os mineradores serão remunerados somente através das taxas de transação. Desse modo, também é impreciso dizer que foi minerado um bloco, já que quando não forem mais emitidas unidades de bitcoins, os blocos continuarão a serem alocados na *Blockchain* como forma de registro das transações e os mineradores não receberão pelo bloco em si minado, mas somente pelas transações nele registradas.

- https://blockchain.info/pt/charts/total-bitcoins.

Miner (mineiro) é o dispositivo de mineração física. Trabalhador (*worker*) é um nome individual dado para cada dispositivo de mineração como um login no software de mineração.

Em resumo, a mineração objetiva usar a capacidade de processamento de um dispositivo para processar as transações (pagamentos e recebimentos ou créditos e débitos), garantir a segurança da rede e manter todos participantes do sistema sincronizados.

A mineração de criptomoedas é o mecanismo utilizado por elas para gerar novos blocos, que consistem em problemas matemáticos resolvidos. Cada moeda tem o seu, mas de modo geral derivam do Bitcoin. O minerador que consegue resolver o problema (bloco ou *hash*) antes de todos, divulga seu trabalho (sucesso, vitória, triunfo, êxito) na rede Bitcoin, para que os outros nós validem seus cálculos (confirmação) e, assim, ele receba seus bitcoins de recompensa.

Como a geração de bitcoin exige muito trabalho, isso torna a bitcoin impossível de falsificar; portanto muito mais segura do que as moedas governamentais da atualidade. A verificação é propositadamente dificultada para que o acesso às bitcoins seja limitado e para que o sistema seja mais seguro. A informação está encriptada e a operação de verificação só poderá ser feita através da resolução de problemas matemáticos muito complicados, com a ajuda de software informático próprio. Devido à natureza complexa do sistema, as transações vão sendo agrupadas em blocos, de dez (10) em dez (10) minutos.

Para que isso tudo seja possível, em intervalos (cerca de 6 vezes por hora) controlados pelo software que administra o sistema (rede Bitcoin), é emitido um hash (sequência de 160 bits gerada pelo algoritmo de criptografia) contendo um determinado valor criptografado, a ser "quebrado" (decifrado ou decodificado); ou seja, a partir do hash deve-se encontrar o valor criptografado. Desse modo, assim que é lançado na rede Bitcoin um novo hash, todos os nós dedicados à mineração se põem imediatamente a tentar decifrá-lo.

Em resumo, minerar Bitcoin envolve executar um *software* que processa equações matemáticas complexas. Se o usuário conseguir resolver uma das equações primeiro, receberá o pagamento em bitcoins. O grande problema é a enorme competição que é semelhante à uma loteria. Isso significa que os equipamentos de vários usuários trabalham muito sem receber nada.

O Bitcoin é um *software* (programa de computador), de código aberto (vide o capítulo "Softwares livre e *open source*"), que forma uma rede (vide o capítulo: "*PEER-TO-PEER* (P2P)") descentralizada de dados compartilhados em tempo real, onde todos os usuários (clientes ou nós) são, ao mesmo tempo, servidores (estações) uns dos outros formando vários nós (dispositivos que compõem a rede), onde são processadas, concretizadas e registradas todas as transações realizadas num registro público chamado "*Blockchain*" ("Cadeia de blocos") e apresentando reiteradamente aos usuários problemas (desafios ou enigmas) matemáticos complexos (quebrar chaves criptográficas ou encontrar sequências de dados chamado "block" ou bloco), com dificuldade constante e que necessita de grande poder computacional para ser resolvido, cujo primeiro a decifrar será

recompensado. Através do processo de resolução do enigma criptográfico, as veracidades (autenticidades) das últimas transações realizadas são confirmadas e propagada essa informação pela rede Bitcoin; pois o vencedor do desafio criptográfico adiciona ao *Blockchain* todas as transações que foram propagadas a seu nó durante alguns minutos antecedentes (cerca de 10), que serão retransmitidas aos demais nós.

> **P2P ou *peer-to-peer*** (par-a-par ou ponto-a-ponto) é uma arquitetura de rede de computadores, onde cada um dos pontos (ou nós) funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços, dados e arquivos sem a necessidade de um servidor central.

Todos os nós mineradores da rede Bitcoin, através de seu próprio bloco candidato, competem entre si para ser o primeiro a achar a solução (resposta certa) do problema criptográfico. Problema este que requer repetidas tentativas e erros para ser resolvido. Quando um nó encontra tal solução, ele anuncia aos demais nós da rede e reivindica seu prêmio. Mas antes de receber sua recompensa, os demais nós da rede, conferem o bloco recém resolvido e, se estiver correto, o validam (aceitam-no e o incluem no banco de dados) e disseminam a informação pela rede Bitcoin. Depois de confirmada, efetua-se a transferência e os dados da transação são adicionados ao livro contábil (*Blockchain*). Entretanto, um novo processo de verificação terá que ser iniciado se as mesmas bitcoin forem novamente utilizadas em outra transferência.

Desse modo, o *software* que gerencia o sistema frequentemente emite e divulga na rede Bitcoin um “hash” (sequência de bits gerada pelo algoritmo de criptografia) contendo um valor encriptografado para que os membros (*nodes* ou nós), caso queiram, disputem para ver quem consegue ser o primeiro a decifrá-lo (“quebrar” a criptografia) e, assim, receber a recompensa. É similar ao que ocorre no desenho animado (anime ou mangá) Dragon Ball ("Esferas do Dragão"), onde várias pessoas disputam para conseguir encontrar e juntar as sete esferas do dragão (que foram previamente espalhadas e escondidas pelo mundo), pois quem conseguir ter as sete esferas terá uma recompensa (no caso, invocar o deus Dragão Shenlong que pode realizar um desejo) e, assim, que o vencedor recebe seu prêmio, as esferas são novamente espalhadas e escondidas iniciando-se uma

nova rodada ou partida da competição. Por várias similitudes com uma corrida pelo ouro, o processo de criação ou geração de bitcoin se denomina mineração (*mining*). É como se pepitas de ouro tivessem sido escondidas em diferentes lugares e com crescente dificuldade de extração para que quem encontrar passe a ser o dono. Em razão de cada vez mais os "mineradores" (*miners*) empregarem equipamentos mais potentes e mais rápidos nessa "disputa pelo ouro", os requisitos mínimos de configuração de *hardware* para poder ter alguma chance de êxito na "mineração" (*mining*) são constantemente elevados, exigindo cada vez mais equipamentos mais potentes e mais rápidos, tornando impossível a detentores de dispositivos simples terem alguma chance real de ganho.

> ***Nonce*** é um número arbitrário, geralmente aleatório ou pseudoaleatório, usado somente uma vez (*number used once* ou *number once*) em um protocolo de autenticação para garantir que comunicações ou dados anteriores não possam ser reutilizados. É muito utilizado em sistemas de autenticação e na prevenção dos ataques do tipo CSRF (*Cross-site request forgery*); ou seja, ataque de repetições de requisições ou de mensagens. Assim, por exemplo, cada usuário ou visitante de um site possui a sua sessão exclusiva e, para diferenciar uma sessão das outras, o servidor do site atribui a ela um identificador único que, geralmente, é devolvido para o usuário em um ***cookie*** (arquivos de internet que armazenam temporariamente o que o internauta está visitando na rede) que será armazenado no navegador do usuário e será enviado automaticamente nas próximas requisições. O *nonce*, portanto, é usado para dar originalidade à uma determinada mensagem de modo que se o destinatário recebe quaisquer outras ordens do mesmo emissor com o mesmo *nonce*, ele irá descartar automaticamente essas ordens como inválidas. É como se fosse um número serial exclusivo para cada mensagem, informação, evento, requisição ou arquivo. O *nonce*, também, é usado em chaves ou assinaturas criptográficas e em sistemas de prova-de-obra. Em complemento, ao *nonce* costuma-se utilizar o recurso de ***timestamp***, que é uma marca temporal ou estampa de tempo consistente numa cadeia de caracteres denotando a hora e/ou data que certo evento ocorreu. **Hash/s** representa a quantidade hashes que são calculadas em um segundo. Saiba mais sobre *nonce* no capítulo

"O QUE É MINERAÇÃO DE BITCOIN?" através desse link. Veja também o verbete *nonce* do glossário (dicionário).

O Bitcoin, portanto, utiliza um banco de dados distribuídos espalhado pelos nós da rede *peer-to-peer* para registrar as transações, utilizando a criptografia para prover funções básicas de segurança, como certificar que bitcoins só podem ser gastos pelo dono e evitar gastos duplos (um mesmo bitcoin ser usado mais de uma vez pela mesma pessoa).

Cada nó na rede Bitcoin recolhe todas as transações não confirmadas de que ele conhece em um arquivo chamado bloco (*block*), que também contém uma referência para o bloco anterior válido conhecida por esse nó. Em seguida, ele acrescenta um *nonce* a este bloco anterior e calcula o *hash* SHA-256 (consistindo em dígitos de 160 bits) de criptografia do bloco e do *nonce* anexado. Como os computadores não podem praticamente inverter a função hash, descobrir o dado original ou inicial da operação é extremamente difícil, pois requer inúmeras tentativas ("chutes", apostas ou palpites) até conseguir acertar; ou seja, a prática reiterada de tentativa e erro. Cada tentativa que um computador faz tentando solucionar a equação é chamada de hash e, quanto mais rápido o equipamento que minera, maior a quantidade de hashs por segundo (h/s). Quando um nó, enfim, encontra a solução, ele anuncia para o resto da rede (os demais nós ou *peers*), que recebem o novo bloco resolvido e vão validá-lo através do cálculo do hash para verificar se o bloco realmente começa com o número determinado de bits zero (ou seja, se o hash está correto). Se estiver de acordo, eles o aceitam e o adicionam à cadeia (relação de blocos anteriores válidos); ou seja, à *Blockchain*.

SHA significa *secure hash algorithm* (algoritmo de hash seguro). Funções hash criptográficas são operações matemáticas complexas executadas em dados digitais. Através dessa operação, compara-se o hash computado (a saída de execução do algoritmo) a um valor de hash conhecido e esperado, para verificar a integridade ou adulteração de dados. Tal procedimento é similar ao do digito verificador. O processo é unidirecional (de mão única, de sentido único, só de ida e sem volta) e impossibilita descobrir o conteúdo original a partir do hash; ou seja, é praticamente impossível utilizar de engenharia reversa (através do

procedimento inverso descobrir o dado original desconhecido). A única maneira de recriar os dados de entrada de saída de uma função hash criptográfica seria usar o ataque de força bruta (*brute-force attack*, ataque de preimagem ou técnica de tentativa e erro) para testar todas as possíveis entradas. Outra característica denominada de resistência à colisão é a impossibilidade de dois valores de entrada diferentes resultarem na mesma saída de hash. Uma colisão é quando duas partes de dados produzem o mesmo resumo. Os dados de entrada (*input*) costumam ser denominado de mensagem (*message*) e os de saída (*output*) são chamados de valor de hash (*hash value*), soma de verificação (*checksum*), hash, resumo da mensagem (*message-digest*) ou simplesmente digest. A síntese da mensagem, portanto, é uma função hash criptográfica que contém uma sequência de dígitos criada por uma fórmula de hash unidirecional com a finalidade de comparação de dados (coincidência ou divergência, integridade ou adulteração, validação ou rejeição, confirmação ou reprovação). Funções hash com uma chave secreta são MAC - *Message Authentication Code* (código de autenticação de mensagem); já sem uma chave são MDC - *Manipulation Detection Code* (código de detecção de sabotagem ou de modificação). Em sistemas criptográficos, MDC é uma cadeia de bits anexa aos dados com a finalidade de detecção de manipulação. O MAC (tag, *keyed cryptographic* ou chave criptográfica) é um pequeno pedaço de informações usadas para autenticar uma mensagem em outras palavras, para confirmar que a mensagem veio do remetente indicado (a sua autenticidade) e não foi alterada em trânsito (a sua integridade). O valor MAC, portanto, protege numa mensagem, tanto a integridade dos dados, como a sua autenticidade, ao permitir que os verificadores (que também possuem a chave secreta) possam detectar qualquer alteração no conteúdo da mensagem. Frisa-se, assim, que a autenticidade das comunicações é tão importante quanto a sua proteção ou sigilo. Em síntese, MAC é uma soma de verificação criptográfica em dados que usa uma chave de sessão para detectar modificações tanto acidentais como intencionais de dados. Não se confunde com endereço MAC (*Media Access Control* ou Controle de Acesso de Mídia), que é um endereço físico único, com 12 dígitos hexadecimais constituído pela combinação de letras e números, gravado em hardware (na memória ROM [*Read-Only Memory*, memória somente de leitura ou memória permanente] da

> placa de rede) e é associado à interface de comunicação, que identifica e conecta um dispositivo (desktops, notebooks, roteadores, smartphones, tablets, impressoras, consoles de games, Smart TVs, etc.) à rede de computadores. Portanto, MAC em criptografia é uma coisa e, em se tratando de Wi-Fi (ou wireless), é outra totalmente diferente.

Quando algum minerador encontra essa chave de validação, ele publica esse arquivo com a chave, que é chamado de bloco, para todos os participantes do protocolo conectados a ele. Quando um participante do Bitcoin recebe um bloco válido, com a assinatura certa e com transações válidas, ele é passado adiante, de forma que em apenas alguns segundos depois de um bloco válido ser produzido por um minerador, todos os participantes do Bitcoin já ficam sabendo desse bloco.

> "Uma boa maneira de descrever a mineração é como um jogo de sudoku, gigantesco e competitivo, que reinicia cada vez que alguém encontra uma solução e cuja dificuldade se ajusta automaticamente, de maneira que leve cerca de 10 minutos para que uma solução seja encontrada. Imagine um sudoku gigantesco, com milhares de colunas e linhas de tamanho. Se eu mostrar para você um sudoku completo, você pode verificar rapidamente que ele está corretamente preenchido. No entanto, se o sudoku tiver apenas alguns quadrados preenchidos e o resto estiver vazio, levará muito trabalho para resolvê-lo! A dificuldade do sudoku pode ser ajustada ao mudar o seu tamanho (mais ou menos linhas ou colunas), mas o sudoku ainda pode ser verificado de maneira rápida, mesmo que ele seja muito grande. O "quebra-cabeças" usado no bitcoin é baseado em um hash criptográfico, que exibe características semelhantes: ele é assimetricamente difícil de resolver, mas fácil de verificar, e sua dificuldade pode ser ajustada." (Mastering Bitcoin por Andreas M. Antonopoulos LLC *in* https://bitcoinbook.info). Nota: Sudoku é um quebra-cabeça baseado na colocação lógica de números. Seu objetivo é colocar um número, de 1 a 9, em cada quadrinho vazio do jogo, de maneira que não se repita nenhum algarismo nas colunas ou linhas.

O Bitcoin usa criptografia de chave pública (*public key*) para permitir a validação da autoria de uma transação na rede por meio de uma assinatura

digital (*digital signature*) e o endereço é produzido a partir da chave pública pertencente a um usuário que, por sua vez, é produzida a partir da chave privada (*private key*) deste mesmo usuário.

A **transação de bitcoin** nada mais é do que uma estrutura de dados que representa a transferência de um certo valor proveniente de uma ou mais fontes de fundos, chamado *input* (entrada), para um ou mais destinos, chamado *output* (saída). O processo de confirmação da transação consiste, essencialmente, em verificar se quem quer transferir tem realmente na sua posse a quantidade de bitcoin necessária. Para isso, é preciso verificar nos registros públicos de contabilidade do sistema. Depois de confirmada, efetua-se a transferência e os dados da transação são adicionados ao livro contábil (*Blockchain*). Um novo processo de verificação terá que ser iniciado se as mesmas bitcoin forem novamente utilizadas noutra transferência. Portanto, nenhuma transação é efetuada sem essa confirmação. Assim, não há falsificação e a mesma pessoa não pode gastar o que não tem ou o que já enviou para outra pessoa.

> ***Double spend* (gasto duplo)** é um tipo de transação fraudulenta onde uma pessoa gasta o mesmo montante de bitcoins duas vezes em transações diferentes. Para convencer a rede de que houve somente um gasto, esta pessoa insere um *hash* da transação em um bloco da *Blockchain* (cadeia de blocos ou livro razão). É muito difícil realizar um gasto duplo; porém há o risco assumido por pessoas que fazem transações sem confirmação. Saiba mais em *Double Spend* (gasto duplo) e Ataque de 51% no glossário.

Assim que a transação é enviada para qualquer nó conectado à rede Bitcoin, ela será verificada por este nó. No caso de a transação ser válida (não estar cometendo um duplo gasto de fundos, estar corretamente formatada, possuir assinatura válida, etc.), este nó que recebeu a transação a propagará para todos os outros nós com os quais ele está conectado e uma mensagem de sucesso retornará de cada nó que validar a transação. Neste processo de propagação, cada novo nó da rede que receber a transação verificará a transação por si próprio e, em caso de validação, continuará transmitindo para todos os nós com os quais estiver conectado sucessivamente. Em caso de a transação ser inválida, o nó apenas rejeitará a

transação e retornará uma mensagem informando a rejeição. Qualquer problema encontrado na transação fará com que ela seja rejeitada pelo nó e não transmitida aos outros nós conectados a ele. Portanto, uma transação inválida não passará do primeiro nó para o qual ela for transmitida. Este processo de verificação independente da transação por cada nó da rede também serve como uma prevenção a *spams*, ataques de *denial-of-service* (DoS) e outros ataques do tipo ou erros provenientes de clientes mal programados.

Em resumo, assim que o primeiro minerador com esta transação em seu bloco alcançar o resultado *hash* esperado pela rede, ele transmitirá o resultado de seu trabalho para que cada nó da rede possa validar por si próprio o seu trabalho de minerador, adicionar este novo bloco à sua própria cópia da *Blockchain* e continuar propagando esta nova escrita na *Blockchain* (cadeia de blocos ou livro razão).

Portanto, quando alguém efetua uma transação bitcoin, ela é propagada por toda a rede Bitcoin rapidamente e fica à espera de ser incluída em um bloco por um minerador, junto com as demais transações pendentes. Quando a inclusão em um bloco acontece, a transação passa a ser considerada confirmada. As transações não confirmadas são aquelas que aguardam a sua inclusão num bloco. Blocos órfãos ou desconectados são os blocos válidos que não fazem parte da *Blockchain* principal do Bitcoin; ocorrerem de forma natural quando dois mineiros produzem um bloco ao mesmo tempo ou são sido criados por um ataque, com poder de hashing suficiente, ao tentar estornar alguma transação. Quando uma transação é incluída em um bloco, diz-se que ela tem uma confirmação. Quando um bloco é gerado após a transação, diz-se que a ela tem duas confirmações e assim por diante. Quanto mais confirmações, mais custoso e improvável se torna reverter aquela transação. São necessárias 6 (seis) confirmações para que uma transação de Bitcoin seja considerada válida e cada confirmação de uma determinada transação é um novo bloco que foi encontrado. E cada bloco novo pega as transações de todo mundo (incluindo a sua) naquele período de 10 (dez) minutos entre o último bloco e ele mesmo, valida todas essas transações com as chaves criptográficas produzidas pelos mineradores (que já vem anexadas aos novos blocos).

A dificuldade de encontrar novos blocos válidos é, automática e constantemente, reajustada pelo sistema para garantir que a média de tempo para encontrar um bloco permaneça igual a 10 (dez) minutos.

Pelo fato de a transação ter que ser verificada pelos mineradores, os usuários (transacionistas) são obrigados a esperar até que eles terminem de minerar. O protocolo Bitcoin é definido de modo que cada bloco leva certa de 10 (dez) minutos para ser minerado. Alguns comerciantes esperam até que o bloco seja confirmado, por receio da pessoa querer tentar usar o mesmo bitcoin em outro lugar antes da transação ser confirmada.

As transações com bitcoins ficam registradas no bloco Bitcoin. Portanto, um bloco Bitcoin é um arquivo que contém um cabeçalho que o identifica e mais algumas informações genéricas sobre o ele (como, por exemplos, o "timestamp", data e hora em que foi emitido referente ao UTC - *Universal Time Coordinated* ou Tempo Universal Coordenado), seguidas do registro das transações mais recentes efetuadas com as bitcoins e que, ainda, não foram registradas em outros blocos. É análogo à uma página individual de um grande livro contábil (*Blockchain*), que registra todas as transações efetuadas em uma bolsa de valores. Pode-se imaginar um bloco como se fosse uma folha de caderno vazia, apenas com a primeira linha em cima com uma transação de bitcoins (o pagamento do próprio bloco para o mineiro que o encontrou), mas que o restante das linhas do caderno já tem uma chave criptográfica pronta por linha para cada nova transação que está sendo processada no momento e será adicionada. Desse modo, cada transação de bitcoin ocupará uma linha da folha (bloco). Quando o bloco adiciona todas as linhas restantes à folha do caderno, as verificações do bloco ficam prontas e são, então, transmitidas pela rede na forma de confirmações, terminando então o trabalho daquele bloco. Dez minutos depois o processo se repete de novo. Uma vez criado o bloco, ele é anexado no final de uma estrutura de dados denominada cadeia de blocos (o livro contábil do sistema; ou seja, a *Blockchain*). Há apenas uma cadeia (com muitas cópias, continuamente atualizadas), que vai se tornando mais longa à medida que novos blocos são anexados. Como cada bloco contém o registro das transações realizadas imediatamente antes de sua criação e, tão logo criado, é anexado no final da cadeia, esta cadeia contém o registro de todas as transações efetuadas com todos os bitcoins emitidos até então.

Os sucessivos blocos da cadeia são necessariamente únicos; ou seja, é impossível repetir um bloco (o que corresponderia a gastar duas vezes [*double spend*] a mesma bitcoin). Esta unicidade é garantida não apenas pelo "timestamp" (senão dois blocos poderiam ser gerados no mesmo intervalo de um segundo), mas, também, porque quando o bloco é criado, é gerado seu "hash" (sequência de um número fixo [160] de bytes gerada por um algoritmo conhecido que funciona como "assinatura digital" garantindo que o conjunto de dados ao qual foi aplicada não foi alterado). Não somente este "hash" é incluído no cabeçalho do bloco como também o "hash" do bloco anterior, identificando sem possibilidade de erro não somente seu conteúdo como também sua posição sequencial na cadeia. Por outras palavras, através de propriedades criptográficas, cada bloco bitcoin faz referência ao bloco anterior de maneira que qualquer adulteração mínima em um bloco anterior invalida não somente aquele bloco, mas todos os blocos subsequentes.

Todas as transações de bitcoins são feitas com uma tecnologia chamada *Blockchain* (corrente de blocos). A *Blockchain* é uma contabilidade pública de todas as operações Bitcoins que já foram executadas (desde o início até o presente). Ele está em constante crescimento através da adição dos blocos concluídos. Os blocos são adicionados à *Blockchain* numa ordem linear e cronológica. Cada nó completo (*full node*) da rede Bitcoin recebe uma cópia completa da *Blockchain*, que é baixada automaticamente após a adesão à rede Bitcoin.

- https://blockchain.info/.

Diante do supra exposto, podemos, enfim, dizer a verdade. Não existem bitcoins, mas tão somente registros de transações com bitcoins. Por outras palavras, as bitcoins não existem em nenhum lugar e, desse modo, ninguém possui de fato (tem a posse) bitcoins; pois elas não estão em nenhum disco rígido ou pen drive. Nem mesmo numa carteira (*wallet*) ou endereço Bitcoin elas existem. As bitcoins somente "existem" na contabilidade da *Blockchain* e em nenhum lugar mais. As carteiras armazenam apenas as credenciais digitais (as chaves privadas que são como simples dados de *login* ou identificação) que permitem o acesso e uso dos fundos bitcoins. Desse

modo, quando um usuário perde sua carteira (ou o acesso a ela), as respectivas bitcoins "perdidas" ainda permanecem na cadeia de blocos (*Blockchain*), como quaisquer outras bitcoins, com a única diferença que ficarão paradas (ociosas) para sempre; pois não há nenhuma maneira de conseguir a respectiva chave privada que lhes permitiriam ser usadas. Portanto, as bitcoins não existem e, muito menos estão, em qualquer objeto físico ou em qualquer arquivo digital. Ninguém pode pegar algo visível ou palpável e dizer: “isso é uma bitcoin”. Em vez disso, somente existem registros de transações entre diferentes endereços, com saldos que aumentam e diminuem. As bitcoins, portanto, não passam de meros bytes (*binary terms*, termos binários, dígitos de computador ou caracteres virtuais). Em síntese, similarmente à moeda bancária ou escritural, a bitcoin não possui existência física ou real, correspondendo apenas aos caracteres eletrônicos, de lançamentos contábeis de débitos e créditos (valores) no sistema digital.

Para entender melhor, ou se profundar, sobre o que são as bitcoins e como elas são feitas, confira os capítulos: "*HASH*", "CERTIFICADOS DIGITAIS", "*PEER-TO-PEER* (P2P)", "BITCOIN", "*BLOCKCHAIN*" e "COMO MINERAR BITCOINS E ALTCOINS".

MÉTODOS DE CONSENSO

Algoritmo de consenso (*consensus algorithm*), ferramenta de consenso (*consensus tool*), mecanismo de consenso (*consensus mechanism*), método de consenso (*consensus method*) ou prova de sistema (*system proof*), é o método usado em mineração de criptomoedas para confirmar e registrar as operações no *datacenter* (bancos de dados ou *blockchain*). É chamado de consenso, porque todos os usuários devem concordar que a informação está correta e que a transação procede.

Preferimos evitar de usar a expressão algoritmo de consenso para não criar confusão com o algoritmo de hash. Portanto, consenso e prova versam sobre a mesma coisa, com a única diferença do primeiro ser a teoria, plano, roteiro ou projeto enquanto o segundo é a prática, realização ou concretização do primeiro.

PoW - ***Proof of Work*** (prova de obra ou de trabalho) é o primeiro, e mais popular, tipo de algoritmo de consenso; onde os usuários fornecem poder computacional para confirmar e registrar as operações e assegurar a integridade da *Blockchain*; tais como, por exemplos, nos sistemas Bitcoin, Ethereum e Dogecoin. Alguns outros algoritmos de *hashing*, que são utilizados para a POW incluem Scrypt, Blake-256, CryptoNight, HEFTY1, Quark, SHA-3, Scrypt-Jane, Scrypt-N, etc.

Confira uma listagem exemplificativa de criptomoedas PoW em https://minkiz.co/coin/cmcap-pow e no capítulo "LISTA DE ALTCOINS: CONSENSO E *HASH*".

Myriadcoin (http://myriadcoin.org/en/home) é uma altcoin que combina cinco diferentes algoritmos PoW: Scrypt, SHA256D, Qubit, Skein e Groestl.

O Blake-256 é utilizado pela BLC - Blakecoin (https://blakecoin.org/).

O Scrypt-N é utilizado por: 10-5 - TenFive Coin, AIR - AIRcoin, CATc - Cataloniacoin, GIARCOC - Giarcoin, GNS - Genesiscoin, H2O - H2O Coin, ONC - Onecoin, RT2 - Rotocoin, XSV - SiliconValleyCoin e YAC - YaCoin.

PoS - ***Proof of Stake*** (prova de participação ou de propriedade) foi desenvolvido como uma alternativa à PoW, que exigem um grande número de cálculos a serem realizados e, portanto, são considerados por alguns como sendo desnecessariamente caro e ineficiente. A palavra *stake* (estaca) faz referência à corrida para o oeste americano, onde os colonos utilizavam-se de estacas como prova de propriedade de seus lotes. Era o ato de fincar a estaca que identificava o proprietário. Ficar a bandeira, além de marcar território, também significa estabelecer-se ou firmar-se. No PoS, em vez de mineração convencional, pede-se aos participantes para comprovarem a propriedade ou a quantidade de referidas moedas digitais. É apelidado de "prova do seu jogo" (numa referência ao ato de mostrar as cartas numa partida de baralho), “prova de participação” ou provar que está apostando (investindo) na moeda. É como um lastro necessário para poder participar. Desse modo, na PoS pede-se aos usuários para comprovar a participação na moeda estancada num cofre ou em compartilhar. O PoS surgiu da necessidade de poupar energia, pois ele gera blocos (emite novas unidades da moeda) ao manter-se as moedas "estaqueadas" (paradas). Em resumo, quanto mais criptomoedas o usuário possuir, mais poder de mineração ele poderá terá. Entretanto, o simples fato de ter moedas "estaqueadas" (paradas) não significa que se irá poder gerar blocos e mais blocos. As moedas "estaqueadas" são similares aos bilhetes de loteria e quanto mais bilhetes, mais chances se tem de gerar blocos (emitir novas unidades da moeda). Esse sorteio é feito por um consenso entre os nós (membros da rede P2P) que também possuam moedas em modo *stake*. Esse método de mineração normalmente possui um mecanismo inicial de fase PoW e depois de um tempo passa para a fase PoS. Essa etapa inicial PoW serve para que uma quantidade inicial da moeda possa existir e ser distribuída; vez que para a geração da moeda através da PoS é necessário que já existam unidades da moeda.

O PoS (*proof of stake*) foi introduzido pela primeira vez pelo criptomoeda Peercoin (https://www.peercoin.net/) e, em seguida, usado por Nxt (https://nxt.org/). Outros exemplos são BitShares, NXT, BlackCoin, NuShares / NuBits, Qora, Blackcoin e a Guarany.

Não confundir com POS (*Point Of Sale* [ponto de venda] ou *Point of Service* [ponto de serviço]), que é a leitora ("maquininha") de cartões bancários. Este é um dos motivos por termos potado por grafarmos PoS (*proof of stake*) para diferenciar de POS (*Point Of Sale* ou *Point of Service*).

Na mineração em nuvem com a BitClub (http://bitclub.network/BitCoinRep), se "apostar" com ClubCoin (http://clubcoin.co/), tem-se o valor da aposta aumentado como recompensa por incentivar a inflação (valorização) dessa moeda.

O princípio do algoritmo da moeda E-Dinar (https://edinarcoin.com/pt/) é o seguinte: é necessário a execução ser confirmada dez vezes; cada um dos computadores, confirmando a operação, recebe uma remuneração que é calculada da seguinte maneira: leva em conta a idade das moedas que são armazenadas na conta do utilizador e sobre o alcance da idade adulta que aumenta dentro de um número de dias (período), dependendo da quantidade que foi realizada na conta da carteira e multiplicado pela taxa de juros (até 0,65% por dia).

O Latium (http://latium.cc/index.html e http://www.latiumcoinbrasil.com.br/) é a primeira criptomoeda a utilizar uma rede de distribuição não-técnica. Não há mineração para manter a rede. Latium não pode ser minerado, mas pode ser adquirido simplesmente por se inscrever; ou seja, ao se inscrever ganha-se moedas. Ainda mais, o participante ganha pelos seus inscritos diretos e pelos inscritos dos seus inscritos, sem gastar nada, em momento nenhum, a não ser um pouco de tempo. Latium é baseada em prova da participação ou de estaca (PoS - *Proof-of-Stake*) em vez de prova de trabalho (PoW). Cada pessoa que detém Latium é capaz de colocar moedas em jogo e é pago com juros por isso.

Confira uma listagem exemplificativa de criptomoedas PoS em https://minkiz.co/coin/cmcap-pos e no capítulo "LISTA DE ALTCOINS: CONSENSO E *HASH*".

Ainda mais, na PoW, quanto mais moedas uma carteira tem, mais votos (peso ou quantidade) ela tem para opinar sobre o que entender ser correto,

ou não, na respectiva rede P2P. Por outras palavras, enquanto que na PoW cada computador é um voto, na PoS, cada moeda é um voto. O raciocínio lógico por trás disso é que, para poder assumir o controle da rede e influenciar o consenso, tem que possuir literalmente mais de metade da rede, o que implica na pessoa não fazer nada contra si mesma; vez que sendo o maior interessado no sucesso e valorização, não vai querer ver a rede fraudada, roubada ou fracassada. Na PoS, portanto, não há nenhuma competição no estilo "rainha vermelha" (*red queen*); ou seja, comprar *hardware* especializado de mineração (corrida armamentista). Além do que o ataque de dominação (*51% attack* ou ataque de 51%) é muito mais caro. Explica-se. Para atacar um sistema baseado na prova de trabalho (PoW), basta comprar poder de mineração suficiente para render a maioria nos trabalhos. Já na prova de jogo, é necessário comprar a maioria da moeda, o que é muito mais caro e estas irão instantaneamente perder o valor após a realização do ataque. Desse modo, a principal vítima seria o próprio atacante.

PoS é, também, um método para tentar evitar o ataque de 51%, incentivando as pessoas a manter as moedas na carteira. E em razão disso, os detentores de moeda são pagos com dividendos (juros).

Snowballs (https://bitcointalk.org/index.php?topic=843495.0) e a SuperTurboStake (https://bitcointalk.org/index.php?topic=1301615.msg13339476#msg13339476), supostamente, pagariam 5000% (cinco mil por cento) de juros ao ano. Já a com a moeda Hyperstake (https://bitcointalk.org/index.php?topic=678849.0) seriam 750% (setecentos por cento) anual. Com a Tubecoin (http://tubecoin.co.uk/ e https://bitcointalk.org/index.php?topic=1503813.0) seriam 125% ao ano. Não temos nenhuma prova disso e não conhecemos ninguém que confirme isso.

A prova da participação é, portanto, uma forma de acumular juros sobre as criptomoedas depositadas na carteira. A desvantagem na prova de jogo é que os ricos ficam ainda mais ricos. Isso somente é evitado se a moeda é incialmente distribuída de forma ampla e democrática entre várias pessoas de várias localidades e diferentes grupos sociais. Enquanto a PeerCoin usa uma abordagem híbrida de prova de jogo (PoS) e prova de obra (PoW), a

Nxt (https://nxt.org/) utiliza a prova de jogo pura, com o inconveniente de ter sido 100% *premined* (pré-minada ou pré-minerada) e, assim, todas as moedas estão, praticamente, nas mãos de cerca de apenas 70 participantes iniciais. A NXT, MSC e BC são 100% *premined*. A QRK é também uma moeda secretamente *premined*.

Este método é muito raramente utilizado sozinho, pois não prevê que qualquer mineração real ocorra. As moedas digitais que usam o método de prova de jogo quase sempre o usam em combinação com a mineração de prova de obra (PoW). Caso contrário, a tentação de investir fortemente, mas não ter um papel ativo em blocos de dados de mineração, pode resultar em mineração extremamente lenta. Isto por sua vez pode resultar em transações mais lentas, longas e menos seguras.

Algumas moedas que usam a **PoS** - ***proof of stake***:

- LSK - Lisk (https://lisk.io/);
- NXT (https://nxt.org/);
- Waves (https://wavesplatform.com/);
- SDC - ShadowCash (https://bitcointalk.org/index.php?topic=745352.0);
- BLK - BlackCoin (http://blackcoin.co/);
- CLAM - Clams (http://www.clamcoin.org/);
- XVC - Vcash (https://v.cash/);
- NSR - NuShares (https://www.nubits.com/nushares/introduction);
- MINT - Mintcoin (http://www.mintcoinofficial.com/);
- IOC - IOCoin (http://iocoin.io/);
- FAIR - Faircoin (https://fair-coin.org/);
- Qora (http://www.qora.org/);
- Hyper (http://hypercrypto.com/ e https://bitcointalk.org/index.php?topic=624651.0);
- RBY - Rubycoin (https://www.rubycoin.org/);
- ZEIT - Zeitcoin (http://www.zeit-coin.net/);
- BLOCK - Blocknet (http://blocknet.co/);
- NEU - NeuCoin (http://www.neucoin.org/en/);

- XWC - Whitecoin (https://bitcointalk.org/index.php?topic=804288.0);
- RADS - Radium (http://www.projectradium.org/);
- XC - XCurrency (https://bitcointalk.org/index.php?topic=630547.0);
- HZ - Horizon (https://horizonplatform.io/);
- YBC - Ybcoin (http://www.ybcoin.com/);
- BITS - Bitstar (http://bitstarcoin.com/);
- TX - Transfercoin (http://transfercoin.io/);
- VPN - VPNCoin (https://bitcointalk.org/index.php?topic=705446.0);
- BAY - BitBay (https://bitcointalk.org/index.php?topic=850267.0);
- RBT - Rimbit (https://bitcointalk.org/index.php?topic=677373.0);
- CLUB - Clubcoin (http://clubcoin.co/);
- GCR - Global Currency Reserve (http://gcrcoin.com/);
- TES - Teslacoin (https://bitcointalk.org/index.php?topic=419494.0).

Burst (https://www.burst-team.us/) é um clone da Nxt (https://nxt.org/), mas não usa a prova de jogo. Seu algoritmo de prova de capacidade permite que as pessoas minerem em casa, vez que se concentra no espaço em disco rígido ao invés de em processadores rápidos.

NEM (https://www.nem.io/) usa um algoritmo de prova de importância, que premia o número de transações realizadas, bem como o número de moedas que o participante possui. Parece ser semelhante à prova de velocidade no jogo usada pela Reddcoin (https://www.reddcoin.com/). Já a Waves (https://wavesplatform.com/ e https://ico.wavesplatform.com/) é uma moeda que permite aos usuários alugar suas moedas para outro usuário que executa um nó completo, de modo que eles são capazes de lucrar apostando sem ter que baixar todo a *Blockchain*.

BitShares (https://bitshares.org/), CLAMs (http://www.clamcoin.org/), Lisk (https://lisk.io/ico), Mintcoin (http://www.mintcoinofficial.com/), ShadowCash (https://shadowproject.io/en), BlackCoin

(http://blackcoin.co/), Nav Coin (http://navcoin.org/), Novacoin (https://novaco.in/), Qora (http://www.qora.org/), Rubycoin (https://www.rubycoin.org/) e NuShares / NuBits 9 https://www.nubits.com/), utilizam a PoW. Já o Ethereum (https://www.ethereum.org/) tem planejado uma transição, via *hard fork*, de PoW para PoS.

Blackcoin é um desdobramento mais *user-friendly* (amigo do usuário), porque não requer uma grande quantidade de dinheiro para "entrar no jogo" (poder participar).

Peercoin e Decred (https://www.decred.org/) hibridizam PoW com PoS, combinando elementos de ambas as abordagens de consenso em uma tentativa de angariar os benefícios dos dois sistemas e criar uma noção mais robusta de consenso.

PoB - *Proof of Burn* (prova de queimadura) é um método de consenso distribuído e alternativo às provas de trabalho (PoW) e participação (PoS); que também pode ser usado para inicialização de uma criptomoeda fora da outra. A ideia é que os mineiros devem provar que queimaram (destruíram) algumas moedas; ou seja, que as enviou a um endereço *unspendable* (impossível de ser gasto). O objetivo da prova de queimadura não é gerar moedas, mas sim verificar a destruição delas, objetivando a transferência da cripto-riqueza de uma criptomoeda para outra. As antigas moedas, então, são transferidas para um endereço de inexistente ou de ninguém onde nenhuma pessoa poderá usá-las; algo como, por exemplo, 1ChancecoinXXXXXXXXXXXXXXXXXZELUFD. A Chancecoin (http://chancecoin.github.io/) utilizou esse procedimento. A BurntCoin (https://www.facebook.com/burntcoin/) é uma nova prova de queimadura de criptomoeda que planeja converter o espaço altcoin atual. Slimcoin (http://www.slimcoin.club/) e CannabisCoin (http://cannabiscoin.net/) também estariam usando a *Proof of Burn*. Deste modo, através da prova de que o usuário jogou fora suas antigas criptomoedas, será recompensado com um tempo de mineração da nova criptomoeda; apelidado de tempo de vida. Naturalmente, quanto mais moedas queimar, mais oportunidade de mineração terá.

- https://bitcoinfactswiki.github.io/Proof_of_burn/.

PoA - ***Proof of Activity*** (prova de atividade) faz uma combinação das provas de trabalho (PoW) e de participação (PoS) para a confecção de cada bloco. Desse modo, mesmo que alguns proprietários detenham 50% de todas as moedas existentes, eles não podem controlar a criação de novos blocos; porque os mineiros PoW podem simplesmente ignorá-los. Por outras palavras, o PoS só atua depois que o PoW foi realizado.

PoU - ***Proof of Use*** (prova de uso) é quando a geração de novos blocos é baseada na quantidade de transações que a pessoa fez e/ou recebeu durante certo tempo ou determinado número de blocos. Isso encoraja as pessoas a colocar a moeda em circulação. Isso pode, no entanto, ser injusto para aqueles que não podem se dar ao luxo de fazer muitas transações. De qualquer forma, deve-se impedir a fraude de transferir as moedas entre contas da mesma pessoa.

PoST - ***Proof of Stake-Time*** (prova de tempo no jogo). Vericoin (http://www.vericoin.info/) é a pioneira nessa denominação. É muito semelhante a uma variante de PoS utilizada em Peercoin que multiplica a PoS pela idade, mas que Peercoin insiste em chamar de PoS. A mineração é baseada fora de uma conta lastreada (*stake*) e o tempo (*time*) relativo à essa conta. A maior diferença é que a Vericoin adiciona um multiplicador fracionário à idade da transação; onde o resultado dessa operação começa a cair à medida que aumenta a probabilidade de um novo bloco ser gerado. Se não estiver ativo, a chance de cada um de mineração de um bloco acabará por começar a cair em vez de crescer. Para os ricos isso acontece mais cedo e para os pobres isso acontece mais tarde, mas isso vai acontecer com todos se eles não estão ativos.

PoST é uma nova abordagem para a formação de um consenso através da introdução de uma componente de tempo no “jogo”, onde a probabilidade de participação diminui ao longo do tempo.

XEM é a moeda da plataforma NEM (https://www.nem.io/) e utiliza o algoritmo de ***PoI – Proof of Importance*** (prova de importância). A fim de incentivar a atividade econômica, NEM introduziu uma expansão de PoS

chamada prova de importância. Este sistema calcula recompensas baseadas cumulativamente no saldo do usuário e no número de transações em que estão envolvidos. Portanto, a PoI não só recompensa aqueles com um grande saldo da conta, mas também leva em conta o quanto eles transacionam com os outros. Ele também leva em consideração com quem essas transações são, para o fim de impedir que os usuários enviem interminavelmente moedas para si mesmos de forma a ganhar recompensas PoL.

PoMAS - ***Proof of Minimum Aged Stake*** (prova de aposta mínima) é quando o direito de fazer o próximo bloco está baseado apenas no fato de que uma conta tem algum saldo mínimo. Enquanto uma conta tem tido algum equilíbrio mínimo durante um período de tempo, um multiplicador (imprevisível, mas verificável) para o valor "alvo" ("target") pode ser escolhido. O problema é que as pessoas com grandes participações podem dividir o montante entre várias contas para melhorar as suas chances; assim é necessário que haja uma forma de desencorajar este comportamento. E um segundo signatário do bloco pode assiná-lo, mas sem poder fazer qualquer alteração ou com acréscimos limitados (valor alvo, por exemplo). E um terceiro assinante do bloco é necessário para fornecer o outro valor (*hit* ou bônus).

DPoS - ***Delegated Proof of Stake*** (prova de jogo delegada). Primeiro visto no Bitshares (https://bitshares.org/), este sistema pede aos usuários para votarem para delegados. O poder de voto de cada usuário depende do seu interesse (aposta) na rede, medido pelo número de moedas que eles possuem. Delegados são eleitos pela *Blockchain* e lhes é dado o direito exclusivo de gerar receita PoS. Por exemplo, no Bitshares (https://bitshares.org/) os delegados ou "trabalhadores" eleitos devem tomar parte de sua renda como o pagamento e, em seguida, usar o resto para ajudar a construir e promover o Bitshares e o ecossistema de serviços que utilizam.

Em Bitshares (https://bitshares.org/) DPoS os delegados podem definir uma taxa de remuneração. A taxa de pagamento de 90%, por exemplo, significaria que o delegado iria manter 90% das taxas de operações que processam e queimar (destruir) o restante (10%). Queimar as moedas diminui a oferta aumenta o valor de todas as moedas restantes; é, portanto,

equivalente ao pagamento das taxas de mineração, mas paga por todos na proporção do número de moedas que possuem.

PoSA - ***Proof of Stake Anonymous*** (prova de jogo anônimo). Cloakcoin (http://cloakcoin.com/) introduziu uma versão de PoS em que os usuários participam na anonimização das transações para outros usuários. Qualquer pessoa que queira enviar uma transação anônima paga uma taxa extra, que é então distribuída como ganhos PoSA.

PoSV - ***Proof of Stake Velocity*** (prova de velocidade no jogo). Introduzido pela Reddcoin (https://www.reddcoin.com/), este sistema recompensa usuários de acordo com o número de moedas que eles têm, mas também como eles são ativos (quantidades de transações envolvendo seu endereço). O objetivo é incentivar o uso da moeda, em vez de acumular. Saiba mais nos sites https://wiki.reddcoin.com/index.php/Proof_of_Stake_Velocity_(PoSV) e https://agroff.github.io/posv/.

PoH - ***Proof of Hodl*** (prova de Hodl) é a utilizada pela Hodlcoin (http://hodlcoin.com/). A referência é a quantidade de blocos numa conta e o tempo que ficaram sem nenhuma transação. Entretanto parece contraditório, porque, ao final, o motivo do investimento é poder usar a moeda (comprar). Por outras palavras, a punição (redefinir a contagem a zero) para quem gastar a moeda, parece ser contrária ao estímulo da moeda (fazer a moeda circular e, assim, a economia prosperar); pois sem gastos, uma economia não pode melhorar. Portanto, uma poupança forçada pode desagradar muitas pessoas.

O projeto de criptomoeda GiveCoin (*cryptocurrency GiveCoin project*) através da atualização (*update*) 2GIVE (http://2givecoin.info/) introduziu a **"Proof of Giving"** (prova de dar), que permite indiretamente doar para instituições de caridade. A rede é assegurada através de um sistema de recompensa compartilhada que permite aos interessados a possibilidade de ganharem 5% de juros (PoS) nas suas explorações por ano e uma taxa de transmissão de 1% (TXFEE) que pode ser obtida pelo processo de mineração (PoW). A 2GIVE utiliza o algoritmo Scrypt.

DDoSCoin (https://github.com/ewust/DDoSCoin) é a criptomoeda que paga por **p0wn** (participação em ataque DDoS [distribuído de negação de serviço] contra servidores alvos específicos; ou seja, fazer um grande número de ligações TLS para um servidor de destino). Foi denominada de ***malicious proof-of-work*** (prova de trabalho maliciosa).

- https://bitcointalk.org/index.php?topic=1583985.0;
- https://www.usenix.org/conference/woot16/workshop-program/presentation/wustrow;
- https://benjaminvandersloot.com/papers/woot16-paper-wustrow.pdf;
- https://www.cryptocoinsnews.com/researchers-reveal-altcoin-to-reward-participating-in-ddos-attacks/.

Como se pode ter percebido, muitos algoritmos são a mistura, mera adaptação ou a utilização de vários (denominado de *proof-of-x*) dos algoritmos principais.

Recapitulando, prova de atividade é uma combinação de prova de trabalho com prova de participação. Já a prova de espaço valoriza a capacidade de armazenamento do computador ao invés de dar importância à velocidade computacional. A prova de capacidade, por sua vez, é baseada no espaço de memória; ou seja, que guardou um certo espaço de data chamado de "plots". Outras moedas, por outro lado, utiliza a prova de largura de banda. Já a prova de pesquisa, um hibrido de PoW e PoS, utiliza os cálculos para resolver funções do tipo BOINC (*Berkeley Open Infrastructure For Network Computing*) ao invés de gerar hashes. Por fim, a *proof of publication* (prova de publicação) visa autenticar que uma determinada informação foi publicada em uma determinada data ou que era conhecida em uma determinada data.

A Gridcoin (https://www.gridcoin.us/), por exemplo, é a primeira e única criptomoeda que premia indivíduos por contribuições científicas. Desse modo, recompensa os mineiros (chamados de *researchers* ou investigadores) por participarem de projetos do BOINC - *Berkeley Open Infrastructure for Network Computing* (http://boinc.berkeley.edu/); que podem levar a avanços nas áreas de medicina, biologia, matemática, ciência, climatologia,

partículas e astrofísica, proporcionando, assim, benefícios reais para a humanidade. Entretanto, só os projetos da lista rendem recompensa: http://wiki.gridcoin.us/Current_BOINC_Whitelist. Gridcoin, portanto, recompensa os pesquisadores por contribuírem com poder computacional para a investigação BOINC e, para isso, usa o algoritmo de prova de investigação (*proof of research*): https://cryptocointalk.com/topic/16940-proof-of-research-and-economic-variables/ e http://wiki.gridcoin.us/Proof-of-Research. Trata-se, na verdade, de um processo de prova de participação (*proof of stake*) de energia ao invés de gerar calor usando o poder computacional numa prova de trabalho (*proof of work*). Houve uma mudança do protocolo original. O Gridcoin Classic usava um sistema híbrido de prova de trabalho (cada computador gastava metade do tempo com *hashing*) e prova de participação (na outra metade do tempo, contribuía para a ciência). Na mudança do Gridcoin Classic para Gridcoin Research (o real Gridcoin), quase toda a energia vai para a ciência; pois o poder de computação de proteger a cadeia de bloco é mínimo. Apesar de que o Gridcoin pode ser "minerado" em qualquer tipo de processo de computação distribuída (ASIC, GPU, CPU, Sensor, etc.): http://wiki.gridcoin.us/Current_BOINC_Whitelist. Com o aumento de usuários ou de poder computacional na rede, torna-se mais difícil obter a mesma quantidade de recompensa. Desse modo, para poder continuar a receber a mesma quantidade de recompensa, é preciso adicionar mais poder de computação. Do mesmo modo, em subindo o valor, mais poder de computação é exigido, tornando-se cada vez mais difícil para obter a mesma recompensa. Trata-se da mesma corrida armamentista da prova de trabalho (*proof of work*) empregada no Bitcoin.

Já a FairCoin (https://fair-coin.org/), descendente da Peercoin, gera os blocos de forma híbrida: Grøstl PoW / PoS híbrido e, ainda, se utiliza do PoC - *Proof-of-Cooperation* (prova de cooperação). Grøstl é uma nova função de hash criptográfico concebido em resposta à competição de criptografia *Hash Algorithm* anunciado pelo NIST - *National Institute of Standards and Technology* (https://www.nist.gov/). FairCoin é a primeira moeda digital que não é comprada, mas distribuída igualmente entre todos os que, independentemente da sua situação financeira atual, promove a igualdade.

A rede CLAM (http://www.clamcoin.org/), por sua vez, é garantida através da *Proof-of-Stake* (PoS), com o nome de *Digging for fresh CLAMs* (cavar para encontrar moluscos frescos). Cerca de uma vez por minuto, a rede seleciona automaticamente um cliente para processar transações CLAM recentes, recompensando-o com 1 CLAM. É como uma rifa. Enquanto o prêmio permanece sempre o mesmo, as chances de ganhar variam de acordo com quantos bilhetes (CLAMs) o usuário tem. CLAM, ainda, se utiliza da *proof-of-chain* (prova de cadeia), baseada em um balanço feito em 12/05/2014 nas redes BTC, LTC e DOGE, para fins de distribuição inicial da moeda.

Pelo site https://www.coingecko.com/ é possível pesquisar qual é o método de consenso utilizado pela criptomoeda.

Saiba mais no capítulo “LISTA DE ALTCOINS: CONSENSO E *HASH*”.

FORK

A palavra inglesa *fork* significa garfo, mas em relação às criptomoedas é empregada no sentido de galho, forquilha, bifurcação, nova versão, direções paralelas ou corrente secundária. Desse modo, em engenharia de *software*, ocorre um *fork* do projeto quando os desenvolvedores levam uma cópia do código-fonte de um pacote de *software* e iniciam o desenvolvimento independente sobre ela; criando uma peça distinta e separada do *software* original. Entretanto, o termo frequentemente não implica em apenas um ramo de desenvolvimento, mas uma divisão na comunidade de desenvolvedores; uma forma de cisma (divisão). A ocorrência de vários *forks* pode gerar uma árvore de subdivisões de tantos galhos criados do tronco original.

O *fork* ocorre com muita frequência com *software* livre de código aberto (*open source*), pelo fato de dispensar autorização do criador e não implicar em violação de direitos autorais. Explica-se. *Software* de código aberto é aquele que é previamente aberto, liberado e acessível para ser manipulado (copiado, modificado, incrementado, aperfeiçoado, utilizado como base em outro programa, etc.) por qualquer pessoa; e, que normalmente pode ser codificado em comunidade, como a plataforma GitHub (https://github.com/). Portanto, ocorre a bifurcação cada vez que um código fonte é modificado para ser uma nova versão independente (separada da versão original); pois está se criando um novo ramo, rumo, visão, filosofia, utilidade, funcionalidade ou objetivo ao código fonte original. Por exemplo, o Calligra Flow, previamente denominado Kivio, é um editor de diagramas disponível no Calligra, uma suíte de escritório do ambiente gráfico KDE, criada a partir da bifurcação do KOffice.

Um *fork* de sucesso pode poupar tempo de desenvolvimento, inspirar outros usos para código antigo e criar novas oportunidades de negócios. Para ser considerado um *fork*, a versão mais recente do *software* deve ter o seu próprio nome e sua própria comunidade de desenvolvedores. Quando um novo programa continua a ser compatível com o programa original, é denominado *soft fork* (bifurcação leve, suave, rasa, fraca ou flexível).

A bifurcação muitas vezes resulta de um impasse em um projeto *open source*, que por dificuldade de resolução de conflitos pessoais, por não

chegarem a um consenso sobre os próximos passos, pelos membros terem ideias conflitantes, pelo núcleo ou equipe de desenvolvimento não darem ouvidos à comunidade do *software* ou por envolver uma divergência intransponível ao ponto de poder encerrar todo o trabalho, normalmente os membros diante do impasse surgido, tomam caminhos diferentes.

Exemplos históricos e didáticos do significado de cisma são o Grande Cisma, de 1054, que causou a ruptura da Igreja Católica, separando-a em duas, Igreja Católica Apostólica Romana e Igreja Católica Apostólica Ortodoxa, quando os líderes da Igreja de Constantinopla e da Igreja de Roma excomungaram-se mutuamente. E, a Reforma Protestante, em 1517, quando o movimento reformista cristão liderado por Martinho Lutero, resultou na divisão da Igreja do Ocidente entre os católicos romanos e os reformados ou protestantes, originando o protestantismo ou ala evangélica.

Um *fork* na *Blockchain* (database ou banco de dados) não tem nada a ver com um *fork* do código fonte. Um *fork* na *Blockchain* pode acontecer sem haver *fork* no código fonte; já *forks* no código fonte do Bitcoin acontecem todo o tempo. São desenvolvedores criando novas criptomoedas concorrentes ou complementares ao Bitcoin. Esses *forks* criam novas *blockchains* (começadas do zero); ou seja, são *forks* do código fonte, mas não da *Blockchain*.

Quando acontece um *fork*, a transmissão das transações e blocos continua ocorrendo normalmente. Ou seja, os *forks*, em regra, não afetam a propagação de transações pela rede. No caso de um *hard fork*, entretanto, alguns blocos gerados por carteiras de versão diferente ou com *bug* (falha) vão ser descartados como inválidos e não serão gravados na *Blockchain*. Em casos graves, as carteiras que insistirem em enviar blocos “inválidos” podem ser desconectadas da rede P2P. Em alguns casos, essa desconexão pode separar a rede em duas redes que não se comunicam. Esse fenômeno se chama *split* (dividido). Mas, na maioria dos casos, as redes continuam se comunicando, mas ignorando os blocos gerados pela outra rede. Quando há um *split*, criam-se efetivamente duas redes separadas, com duas *blockchains* separadas, praticamente como se existissem duas moedas separadas.

Um eventual *fork* pode resultar no nascimento de uma nova moeda. As Altcoins (criptomoedas alternativas ao Bitcoin), por exemplo, em sua maioria surgiram a partir de bifurcações do código-fonte do Bitcoin, com o intuito de modificar alguns parâmetros internos da rede do Bitcoin ou adicionar novas características ou funcionalidades. A primeira altcoin que foi uma bifurcação (*fork*) do Bitcoin foi a IXCoins; que modificou alguns parâmetros do Bitcoin, acelerando a criação da moeda ao aumentar a recompensa para 96 moedas por bloco. Outros exemplos de altcoins que surgiram de bifurcações do Bitcoin são a Namecoin (http://namecoin.info/) e a Litecoin (https://litecoin.org/pt/). Entretanto, algumas altcoins são implementadas do zero, baseando-se apenas no modelo da *Blockchain*, mas sem utilizar nada do código-fonte do Bitcoin. A CryptoNote (https://cryptonote.org/) é notável por ter sido uma implementação completamente nova de criptomoeda, não tendo sido uma bifurcação do Bitcoin. CryptoNote é uma altcoin de implementação de referência que fornece a base para o dinheiro digital anônimo. Ela foi projetada para ser bifurcada em várias implementações diferentes e possui um mecanismo embutido de reinicialização que a torna inutilizável como moeda por si só. Porém, várias altcoins surgiram a partir da CryptoNote: Bytecoin (https://bytecoin.org/); Aeon; Boolberry (http://boolberry.org/); duckNote, atual DigitalNote (http://digitalnote.org/); Fantomcoin (http://fantomcoin.org/); Monero (https://getmonero.org/); MonetaVerde e Quazarcoin. Outro exemplo de bifurcação é a Komodo, uma criptomoeda segura e anônima baseada na bifurcação da ZCash (https://z.cash/). Uma listagem exemplificativa (não exaustiva) das criptomoedas pode ser vista em http://coinmarketcap.com/.

Recorda-se que, muitas vezes, é o próprio minerador que determina, em certa medida, a configuração do seu próprio nó da rede, estabelecendo de forma livre e competitiva a quais valores e tamanhos de transação ele dará prioridade no processamento, durante a formação dos novos blocos que tenta minerar. Entretanto, algumas características da rede embutidas no código Bitcoin, não são possíveis de customizar ou alterar facilmente; tais como, por exemplos, variáveis como o número total de Bitcoins que serão criados ao longo da história ou a taxa de emissão à qual entrarão na rede. E, pior, diferente das configurações liberadas, estas características não possuem interoperabilidade entre as diversas versões em operação na rede Bitcoin.

Desse modo, se um nó da rede Bitcoin, seja minerador ou usuário comum (recebendo e propagando novos blocos), alterar a versão do *software*, na qual, por exemplo, ao invés de 21 milhões bitcoins sejam gerados 100 milhões, essa alteração resultaria no automático encerramento da comunicação com a rede original. Seria um "fork" na geração de novos blocos, implicando na divisão da rede em duas versões distintas que não são capazes de se comunicarem entre si. Passariam a ser duas cadeias com uma gênese comum e idêntica até o ponto de bifurcação, após esta o que existiria seria exclusivamente em paralelo em cada rede separada; a menos que uma das correntes esteja completamente abandonada. Portanto, qualquer alteração na rede Bitcoin que muda a estrutura de bloco (incluindo o bloqueio de *hash*), as regras de dificuldade ou aumenta o conjunto de transações válidas, é um *hardfork*. No entanto, algumas dessas mudanças podem ser implementadas através de um soft fork (leve, suave ou flexível); tal como o recurso P2SH foi adicionado ao Bitcoin. O P2SH (*pay-to-script-hash*) permite pagar para um *script* ou *hash* de roteiro (endereço começando com 3) ao invés de um *hash* de chave pública (endereço começando com 1).

Saiba mais sobre P2SH nos verbetes *P2P Escrow* e *RedeemScript* do Glossário.

A ***hard fork*** é uma mudança no protocolo, rede ou sistema que exige a atualização do *software* por todos os usuários, sob de considerar inválidos blocos e transações válidas. Desse modo, uma divergência permanente na cadeia de bloco pode ocorrer quando, nós não modernizados podem não validar blocos criados por nós atualizados que seguem as mais recentes regras de consenso.

Hard forks são, portanto, quando alguma coisa impede que um consenso seja atingido ou quando ocorre alguma mudança fundamental no protocolo que torna as versões anteriores incompatíveis. Pode ser um *bug* (falha) no sistema, que cria blocos reconhecidos por algumas versões da carteira, mas não por outras. Pode também ser decisão dos desenvolvedores para acrescentar funcionalidades à moeda. Para evitar que um *hard fork* proposital tenha impacto na moeda, um consenso prévio entre desenvolvedores e usuários costuma ser buscado, e quando o *hard fork* acontece, estão todos (ou quase todos) com a versão correta da carteira e a

cadeia “errada” é rapidamente descartada ou ignorada. Num *hard fork* a *Blockchain* se divide em duas baseada em uma mudança fundamental nas regras que regem o sistema. No caso do Ethereum, por exemplo, o *hard fork* foi resultado de um corte na TheDAO, um contrato inteligente que tinha um código ruim e permitiu um *hacker* desviar dezenas de milhões de dólares em moeda digital. Um *hard fork* foi utilizado para reverter essas transações ilícitas e devolver os fundos roubados aos seus legítimos proprietários. Por ser um *hard fork*, exige-se que cada nó (mineiros, comerciantes e usuários) atualize o *software* para poder validar os novos blocos. Entretanto, uma minoria considerável escolheu não fazer o *hard fork*. O resultado foi a criação de dois grupos: Ethereum e Ethereum clássico.

Sobre o Bitcoin, há uma questão polêmica sobre aumentar, ou não, o tamanho dos blocos. O tamanho atual do bloco é de 1 MB; isto permite cerca de 7 (sete) transações por segundo. O aumento do tamanho dos blocos não é uma mudança trivial (comum ou simples) e, por esse motivo, não pode ser feita com uma mera atualização do *software*. Seria preciso forçar um *hard fork* (pesado, duro ou rígido) na rede Bitcoin. Não existe uma forma de fazer a transição suave (usando *soft forks*), porque os blocos de tamanho maior seriam fatalmente rejeitados pelos *softwares* clientes antigos (desatualizados) e não há uma maneira alternativa de encaixá-los no protocolo já que foi implementado como uma regra fixa em todos os clientes. Entretanto, um *hard fork* na rede Bitcoin é uma medida arriscada, que pode gerar prejuízos se feito apenas por uma parcela da rede. Normalmente um *hard fork* é conduzido com o consenso da comunidade que atualiza os principais nós e clientes da rede antes de um prazo pré-estabelecido. Ainda mais, a implementação do aumento no tamanho dos blocos é um assunto polêmico (não há consenso) e nem se sabe se um dia haverá consenso. Por esses motivos, o Bitcoin XT (https://bitcoinxt.software/) se utiliza de um mecanismo de "votação" para mensurar o consenso da rede, e só após esse consenso ser atingido, é que ele irá ativar as novas funcionalidades. Durante esse tempo, ele opera exatamente igual a um cliente Bitcoin Core. O Bitcoin XT é um *fork* do código do Bitcoin que pretende gerar um *hard fork* da *Blockchain* do Bitcoin, caso sua aceitação passe de 75%. Se o XT não obter os 75% de aprovação, tudo continuará como está. Se aprovado, ele emitirá uma mensagem para todos os clientes da rede informando que haverá um *hard fork* e dando o prazo de duas semanas para que, quem quiser, possa

adequar seus sistemas (atualização da carteira para o XT). Passadas as duas semanas, o XT começará a minerar blocos seguindo as novas regras, gerando assim um *hard fork*. Em todos migrando para o XT, após o *hard fork* ocorrer, não haverá ninguém no lado “antigo” do *fork*, que morrerá rapidamente, e, assim, o XT substituirá o Bitcoin totalmente. Mas os atuais defensores do XT não são suficientes; confira em http://xtnodes.com/. Se após a eventual aprovação, cerca de 20% dos mineradores optarem por não migrar para o XT, após o *hard fork* passará a existir duas moedas com um passado comum. A “Core” minerada pelos que não migraram de sistema e, a "XT", minerada por quem optou pela mudança.

Como a *Blockchain* é uma estrutura de dados descentralizada e democrática, as diferentes cópias dela não estão sempre sincronizadas ou idênticas e, pelo fato dos nós da rede trabalharem simultaneamente nela, é comum ocorrer alguns conflitos na alocação dos blocos. Desse modo, os blocos podem chegar de diferentes nodos (nós da rede) no mesmo instante, fazendo com que os nodos tenham diferentes perspectivas da *Blockchain*; como, por exemplos, entendimentos conflitantes sobre qual bloco deve ser registrado primeiro e qual bloco se liga a qual. Para resolver isso, cada nodo sempre seleciona e tenta estender a corrente de blocos que representa a maior prova de trabalho (corrente mais longa ou corrente com a maior dificuldade acumulada).

Um "fork", portanto, ocorre no Bitcoin sempre que dois mineiros resolverem o algoritmo de prova de trabalho (apresentarem um bloco candidato) dentro de um curto período de tempo um do outro. Como ambos os mineiros descobriram a solução para seus respectivos blocos candidatos, eles imediatamente transmitem seus próprios blocos "vencedores" aos seus vizinhos imediatos na rede P2P, que começam a propagar esses blocos através da rede Bitcoin. Cada nó que recebe um bloco válido irá incorporá-lo em sua versão da *Blockchain*, estendendo a *Blockchain* por um bloco. Se esse nó mais tarde, vê outro bloco candidato estendendo-se do mesmo bloco pai (bloco anterior), ele se conecta ao segundo candidato em uma corrente secundária. Como resultado, alguns nós verão um bloco candidato em primeiro lugar, enquanto outros nós irão ver o outro bloco candidato primeiro e, assim, existirão duas versões concorrentes e distintas da *Blockchain*. Para facilitar a visualização e consequente compreensão,

imagine-se o jogo de dominó, no qual de uma mesma peça se encaixam outras duas, dando origem a duas sequências distintas. Desse modo, sempre que há uma divergência entre mineradores; ou seja, quando conjuntos diferentes de transações são validadas ao mesmo tempo formando blocos diferentes para a mesma posição na *Blockchain*, acontece um fork. Neste caso, portanto, a bifurcação ocorre devido à uma inconsistência temporária entre as versões da *Blockchain*, que só acabará sendo resolvida com a reconvergência, à medida que mais blocos são adicionados a uma das ramificações da bifurcação.

Por outras palavras, sempre que há uma divergência entre mineradores, por exemplo, quando conjuntos diferentes de transações são validados ao mesmo tempo formando blocos diferentes para a mesma posição na *Blockchain*, acontece um *fork*. Esse tipo de *fork* é chamado de “soft fork“ e faz parte do mecanismo de obtenção de consenso. O consenso no contexto do Bitcoin é definido pela *Blockchain*. As discrepâncias temporárias entre as correntes acabam sendo resolvidas à medida em que se adiciona mais prova-de-trabalho (blocos candidatos), estendendo uma das possíveis correntes. Desse modo, os nodos mineradores "votam" com seu poder de mineração ao escolher qual corrente eles irão estender através da mineração do próximo bloco. Ao minerar um bloco novo e estender à corrente que eles escolheram, os mineradores estão "votando" nessa corrente.

Por outras palavras, o método de resolução para saber qual dos blocos (e respectiva corrente) vai ser mantido e qual será descartado, é através do próximo bloco; o qual definirá apenas um dos dois anteriores como “assinado” pelo minerador (que minerou sozinho o bloco atual, sem conflitos e com a sequência mais longa que eventual concorrente). O bloco que ficar de fora, se torna “órfão”. Igual solução se aplica à eventualidade remota de dois mineradores criarem dois novos blocos simultâneos, cada um assinando um dos antecessores concorrentes criados na rodada anterior.

Esclarece-se que, pela programação do sistema, se em algum momento um usuário de Bitcoin recebe uma cadeia maior do que a que ele tem, ele abandona a cadeia que ele tem e passa para outra cadeia de blocos, por ser maior. Por isso, quando uma transação é incluída em um bloco, a transação é considerada como validada, praticamente irreversível. Mas, quando 6

blocos são publicados na frente do bloco em qual a transação é incluída, a transação tem uma chance quase nula de ser revertida, por isso é considerada confirmada e irreversível.

Às vezes, portanto, o bloco novo estende uma corrente (sequência) paralela à corrente principal. Nesse caso, o nodo irá anexar o bloco novo à corrente secundária que ele estendeu e então irá comparar a dificuldade da corrente secundária com a dificuldade da corrente principal. Se a corrente secundária possuir uma dificuldade acumulada maior do que a da corrente principal, o nodo irá convergir novamente para a corrente secundária; ou seja, ele irá selecionar a corrente secundária como sua nova corrente principal, fazendo com que a corrente principal anterior se torne uma corrente secundária. Se o nodo for um minerador, ele irá construir um bloco ao estender essa corrente nova, por ser a mais longa. Se um bloco válido é recebido e nenhum pai (bloco anterior) é encontrado nas correntes existentes, o bloco é considerado um "órfão". Os blocos órfãos geralmente surgem quando dois blocos que foram minerados em um curto espaço de tempo são recebidos em ordem inversa; ou seja, o bloco filho é recebido antes do bloco pai. Os blocos órfãos são salvos na *pool* (piscina) de blocos órfãos, onde eles ficam até que os seus pais adotivos sejam encontrados e os recebam. Assim que o bloco pai é vinculado às correntes existentes, o bloco órfão pode então sair da *pool* e ser vinculado ao seu bloco pai, passando a fazer parte da corrente.

Em razão do grande aumento e aceitação do Bitcoin, a quantidade de transações por bloco está praticamente sendo insuficiente para a demanda. Por outras palavras, esse limite de transações por cada 10 (dez) minutos pode causar colapso no protocolo. Diante disso, atualmente, existe uma divergência sobre o tamanho que o bloco do Bitcoin deve ter e, com isso, surgiram algumas correntes; a Segregated Witness ou SegWit (que propõe uma alteração suave através de um *soft fork*) e a Unlimited (que propõe uma intervenção mais drástica; ou seja, um *hard fork*). O Segwit, em síntese, sugere incluir no bloco apenas um resumo da assinatura do remetente para liberar espaço no bloco. O Bitcoin Unlimited (https://www.bitcoinunlimited.info/) pretende introduzir um nível de democracia no desenvolvimento e gestão da implementação; permitindo que a comunidade vote sobre as mudanças. Diante disso, prega a ausência de um

limite de tamanho de bloco codificado. Por outras palavras, propõe que os usuários definam os limites manualmente em seus próprios nós e, assim, esperam que naturalmente se chegue a um consenso num determinado momento ou ponto (chamado de Schelling ou ponto focal). Já o Bitcoin Classic propõe o aumento do tamanho do bloco de 1MB para 2MB.

INSUMOS NA GERAÇÃO DE BITCOINS

O **principal item no processamento computacional é o CPU** (*Central Processing Unit*, Unidade Central de Processamento, microprocessador ou simplesmente processador), mais especificamente a sua frequência (ou velocidade) de operação; ou seja, o seu *clock* (relógio). Costuma-se confundir CPU com o gabinete (compartimento físico, semelhante à uma caixa, cujo interior estão todos os componentes) de um computador *desktop*.

O processador é um circuito integrado (microprocessador ou cérebro eletrônico em um chip) que realiza as funções de cálculo e tomada de decisão de um computador. É um dispositivo multifuncional programável que aceita dados digitais como entrada, processa de acordo com as instruções armazenadas em sua memória, e fornece resultados como saída. Os dois componentes típicos de um CPU incluem a ALU - *Arithmetic Logic Unit* (ou ULA - Unidade Lógica e Aritmética), que executa operações aritméticas e lógicas e a CU (*control unit* ou unidade de controle), que extrai instruções a partir da memória, as decodifica e executa invocando o ALU quando necessário.

> "PROCESSADOR: É um hardware que executa instruções em linguagem de máquina de forma eficiente e com finalidades especiais.
> Apesar de existirem diversos modelos de processadores há algo em comum entre eles:
> 1. UNIDADE DE BUSCA DE INSTRUÇÕES: Carrega instruções na memória de alta velocidade (Registradores de instrução).
> 2. REGISTRADORES: Guardam dados para uso imediato e são compostos por memórias ultrarrápidas.
> 3. UNIDADE DE CONTROLE (UC): Responsável por gerar todos os sinais que controlam as operações no exterior do CPU, e ainda por dar todas as instruções para o correto funcionamento interno do CPU.
> 4. UNIDADE DE DECODIFICAÇÃO DE INSTRUÇÃO: Interpreta as instruções carregadas e envia para a unidade de execução.
> 5. UNIDADE DE LÓGICA E ARITMÉTICA (ULA): Executa as operações básicas (soma, subtração, multiplicação e divisão e comparações lógicas). Além de executar funções aritméticas, uma ULA deve ser capaz de determinar se uma quantidade é menor ou maior que

outra, e quando quantidades são iguais e se o número é positivo, negativo ou nulo. Podendo até mesmo executar funções lógicas com letras e com números.

6. CACHES: Armazenam uma cópia dos dados da memória principal e possibilitam acesso rápido às informações.

7. INTERFACE DE BARRAMENTO: Permite a comunicação entre o processador e os dispositivos." (http://www.portaleducacao.com.br/informatica/artigos/50740/componentes-de-um-processador).

O processador possui três funções básicas: 1) realizar cálculos de operações aritméticas e comparações lógicas; 2) manter o funcionamento de todos os equipamentos e programas, pois a unidade de controle interpreta e gerencia a execução de cada instrução do programa; e, 3) administrar na memória central (principal) além do programa submetido, os dados transferidos de um elemento ao outro da máquina, visando o seu processamento.

O processador se comunica com outros circuitos e placas que são encaixadas nos "slots" (conectores) da **placa-mãe** (*mainboard* ou *motherboard*, placa de circuitos [*protoboard*] que conecta e interliga todos os componentes) do dispositivo computacional. O caminho pelo qual se dá essa comunicação entre o processador e as outras placas é denominado de barramento. Há dois tipos de barramento mais comuns: ISA ("Industry Standard Architecture") e PCI ("Peripheral Component Interconnect").

É importante notar que quanto mais rápido for o processador, maior será a velocidade com que os dados serão trabalhados e mais rapidamente as instruções serão executadas. Essa distinção é de uso corrente para separar produção elétrica e dissipação térmica.

Quanto maior o *clock* do processador, maior será a quantidade de ciclos executados por período (segundo). A medição do *clock* é feita em hertz (Hz); que é a unidade de medida que expressa, em termos de ciclos, a frequência de um evento periódico, oscilações, vibrações ou rotações por segundo. Assim, por exemplo, megahertz (MHz) significa milhões de ciclos

por segundo; ou seja, instruções (tarefas) por segundo. *Overclock* é o aumento dos níveis do *clock* de um processador.

O segundo elemento importante de um processador é a quantidade de núcleos (*cores*). O *KiloCore* (processador com 1.000 núcleos) tem uma taxa máxima de cálculo de 1,78 trilhão de instruções por segundo, contém 621 milhões de transistores de alta eficiência elétrica e seus mil processadores podem executar 115 bilhões de instruções por segundo dissipando apenas 0,7 watts de consumo de energia elétrica.

- 10^{0} = hertz (Hz);
- 10^{1} = deca-hertz (daHz);
- 10^{2} = hecto-hertz (hHz);
- 10^{3} = quilo-hertz (kHz);
- 10^{6} = mega-hertz (MHz);
- 10^{9} = giga-hertz (GHz);
- 10^{12} = tera-hertz (THz);
- 10^{15} = peta-hertz (PHz);
- 10^{18} = exa-hertz (EHz);
- 10^{21} = zetta-hertz (ZHz);
- 10^{24} = yotta-hertz (YHz).

Uma observação. O chip (circuito integrado) FPAA - *Field-Programmable Analog Array* (Matriz Analógica Programável em Campo) de computação analógica configurável utiliza 1.000 vezes menos energia elétrica do que seu equivalente digital, o FPGA - *Field Programmable Gate Array* (matriz/arranjo de portas programável em campo) e, ainda, pode ser construído até 100 vezes menor.

Saiba mais sobre processadores no capitulo "EQUIPAMENTOS DE MINERAÇÃO", na lista exemplificativa ou sugestiva de processadores.

Enquanto a velocidade de processamento de computadores é expressa em gigahertz por segundo (Ghz/s), **o poder de processamento usado na mineração de criptomoedas é definido como *hashrate* (taxa de hash)**. Hashes por segundo (h/s), portanto, é a quantidade por segundo de funções hash criptográficas executadas pelo hardware de mineração em um

cabeçalho do bloco bitcoin. Por outras palavras, cada tentativa que um computador faz tentando solucionar a “equação” é chamada de hash. Quanto mais rápido o equipamento que "minera", maior a quantidade de hashs por segundo (h/s). Entretanto, em razão da alta capacidade das atuais máquinas mineradoras de bitcoin, essa taxa é de petahashes (10^{15} [10 elevado a 15] ou 1.000.000.000.000.000).

- H/s = Hashes por segundo;
- KH/s = Kilohashes por segundo (milhares de hashes por segundo);
- MH/s = Megahashes por segundo (milhões de hashes por segundo);
- GH/s = Gigahashes por segundo (bilhões de hashes por segundo);
- TH/s = Terahashes por segundo (trilhões de hashes por segundo);
- PH/s = Petahashes por segundo (quatrilhões de hashes por segundo);
- EH/s = Exahashes por segundo (quintilhões de hashes por segundo);
- ZH/s = Zettahashes por segundo (sextilhões de hashes por segundo);
- YH/s = Yottahashes por segundo (Septilhões ou quadriliões de hashes por segundo).

O site http://www.fileformat.info/tool/hash.htm demonstra em tempo real o que é um *hash*.

Em razão da constante alteração para maior do grau de dificuldade do *hash* (*difficulty factor* ou *Bitcoin difficulty*) na rede Bitcoin, a quantidade de *hashes* por segundo que um equipamento consegue fazer vai decaindo. Para saber qual é a capacidade do equipamento existem vários sites com uma calculadora especifica ("Bitcoin Mining Calculator" ou calculadora de mineração bitcoin). Entretanto, calculadoras de taxa de *hash* tem um enorme problema, como resultado da aleatoriedade mostrado pelas estatísticas. Tudo o que eles podem fazer é medir a taxa de eventos e fazer uma estimativa da taxa, com base nas taxas de bloco achado (gerado). Elas não têm nenhuma

maneira de dizer se as estatísticas para um determinado período de tempo foram normais, baixas, altas, muito baixas, muito altas, etc.

- http://block-chaininfo.site/;
- https://alloscomp.com/bitcoin/calculator;
- http://www.coinwarz.com/calculators/bitcoin-mining-calculator;
- http://www.alcula.com/calculators/finance/bitcoin-mining/;
- http://www.vnbitcoin.org/bitcoincalculator.php;
- http://www.bitcoinx.com/profit/;
- https://btcserv.net/bitcoin-mining-calculator;
- http://www.karldiab.com/BitcoinMiningCalculator/;
- http://www.cloudmining.website/calculator.php;
- http://bitcoinminingcalculator.org/;
- https://bitcoinwisdom.com/bitcoin/difficulty.

Quando o Bitcoin foi lançado, sua dificuldade permitia gerar blocos com o computador doméstico; mas, atualmente, essa prática não é mais rentável, pois o rendimento obtido sequer irá pagar pela despesa com a eletricidade.

A mineração de Bitcoin (*Bitcoin miner*) através de um computador doméstico foi se tornando inviável a partir do surgimento de computadores específicos para essa tarefa. O **ASIC** - *Application-Specific Integrated Circuit* (circuito integrado de aplicação específica ou chip criados somente para realização de uma tarefa) é um circuito integrado personalizado (ou específico) para a mineração de Bitcoins. Desse modo, os ASICs, com processadores poderosos e voltados unicamente para mineração de Bitcoin, tornaram a mineração caseira ou solo (*single*) extremamente difícil ou totalmente inviável. Em questão de hardware para a mineração de Bitcoins, os ASICs foram o passo evolutivo após o uso de CPUs (Central Processing Unit, unidade central de processamento ou processador), GPUs (*Graphics Processing Unit*, unidade de processamento gráfico ou placa de vídeo) e FPGAs (*Field-Programmable Gate Array*, campo programável de ordem de entrada ou chips reprogramáveis de imediato; um circuito integrado

projetado para ser configurado e reconfigurado pelo usuário ou pelo projetista após a fabricação). Do ano 2009 até 2011, minerava-se via CPU de forma totalmente descentralizada. Assim, no início, utilizava-se os processadores, que foram substituídos pelas placas de vídeo por serem de 50 a 100 vezes mais eficientes que os processadores. No ano de 2013, enquanto que um processador médio podia executar quatro instruções por ciclo de *clock*, a GPU conseguia realizar 3.200 instruções por ciclo. O trunfo da tecnologia FPGA não é o aumento de potência, mas a economia de energia elétrica, assim enquanto uma placa de vídeo consome cerca de 400w, pela FPGA é apenas 80w. O poder de processamento de um ASIC é de até 300 vezes maior que os das GPUs. E, apesar do script do Litecoin, em tese, ser melhor minerado com CPU / GPU, desde 2014, já existem ASIC's para minerar Litecoins. Os algoritmos cryptonight e X11 seguem a filosofia do Litecoin, ou seja, ser possível minerar com CPU's / GPU's e processadores ARM (*ARM processors*).

- https://www.hobbymining.com/mining-hardware/;
- http://informatica.mercadolivre.com.br/asic-bitcoin.

Saiba mais sobre ASICs no capítulo "EQUIPAMENTOS DE MINERAÇÃO", no item ASICs.

Em http://cryptomining-blog.com/tag/gtx-1080-hashrate/ e http://satoshi.network/as-13-melhores-placas-de-video-para-minerar-ethereum/ há testes de placas de vídeos para mineração.

Em https://www.whattomine.com/ constam informações para auxiliar na escolha de qual moedas criptográficas minerar.

Coinwarz (http://www.coinwarz.com/cryptocurrency) mostra quais são as moedas mais lucrativas para minerar com hardware:

- http://dann.com.br/bitcoin-guia-definitivo-parte-23-tecnicas-de-mineracao-de-criptomoedas/.

O primeiro (ASIC - *Application Specific Integrated Circuits*) apareceu em fevereiro de 2012. O Avalon ASIC foi uma das primeiras máquinas para

mineração de bitcoins e possui um poder de processamento de 60.000 MH/s (Megahashes por segundo), com a possibilidade de aumentar muito mais ainda com a adição de módulos opcionais. Já o BitForce Mini Rig SC, da Buttlerfly Labs, possui 1.500 GH/s de potência. A CoinTerra TerraMiner IV, por sua vez, é composta por quatro chips da Asic de 500 GH/s de potência cada um; juntos, eles totalizam 2 TH/s.

Por volta de 24 de janeiro de 2016, a Rede Bitcoin atingiu um Exahash por segundo pela primeira vez. Isso é um quintilhões, a 1 seguido de 18 zeros ou 10 18 hashes por segundo. Atualmente a rede Bitcoin trabalha com cerca de 1,36 Exahash/s (em torno de 1,358,435 TH/s) de poder de mineração.

O investimento em equipamento de mineração (*mining rig*), em resumo, envolve os custos de hardware, de uma boa conexão à Internet e a despesa com a energia elétrica. Atualmente equipamentos simples, domésticos ou populares não são capazes de renderem o suficiente para sequer pagar a energia elétrica utilizada.

- http://blog.wendelrocha.eng.br/12-bitcoin/14-vale-a-pena-minerar-bitcoins-em-2016.html.

O Watt (W) é a unidade de potência elétrica equivalente a um joule (J) por segundo; que, por sua vez, é a unidade tradicionalmente usada para medir energia mecânica (trabalho) e energia térmica (calor). Watt elétrico (We) corresponde à produção de potência elétrica e, watt térmico (Wt ou Wth) corresponde à produção de potência térmica. Já em mecânica o watt é a potência desenvolvida por uma força de um newton aplicada a um ponto que se move um metro em um segundo.

O termo "Mhash / j" descreve a quantidade de hashes que a GPU pode processar com 1 joule de energia. Esta é uma boa estimativa para a quantidade de energia elétrica gasta com certa quantidade de trabalho.

Para estimar **quanto o equipamento de mineração (*mining rig*) consumirá de energia elétrica** num mês, ficando ligado 24/7 (vinte e quatro horas por dia, sete dias por semana), utiliza-se a seguinte fórmula: P / 1000 * 24 * 30 = x kWh/mês. Explica-se. Divide-se a potência elétrica (W) do

equipamento (como noção média usa-se a potência da fonte de alimentação) por 1000, depois multiplica-se por 24 (horas diárias) e, o resultado obtido, é multiplicado por 30 (um mês). Isso resultará no consumo mensal de energia elétrica que multiplicado pelo custo do kWh dará o custo final de um mês de mineração.

- http://outervision.com/power-supply-calculator.

Em regra (na maioria das vezes), quanto maior a potência (velocidade ou capacidade) de processamento, maior será o consumo de energia elétrica; bem como de aquecimento do processador, com o que aumenta o consumo de energia elétrica pelos coolers (ou *watercooler*, em computadores de alto desempenho) e os ventiladores ou ares condicionados externos que tentarão refrigerar o processador. Por óbvio, no cálculo do consumo da energia elétrica, há de se levar em conta o consumo da placa-mãe, do disco rígido, do processador, dos *coolers*, das placas de vídeos, do monitor, do modem e/ou roteador, da placa de rede ou de Wi-Fi (*wireless*), de eventuais alto-falantes ou caixas de som, da transformação da corrente alternada em corrente contínua pela fonte, etc. Entre desktops (computadores de mesa) e notebooks, estes costumam gastar bem menos energia elétrica. Notebooks normalmente gastam de 15 a 60 Watts por hora enquanto que desktops consomem de 65 a 250 Watts por hora. Um *desktop* com configuração simples ou mais leve (para ser usado apenas para trabalhar texto e navegar na Internet) consome menos energia elétrica do que um projetado para gamers (jogadores) ou trabalhos de edições gráficas (processador potente, placa de vídeo, placa de som e outros componentes profissionais). Além disso, a forma de uso ou a quantidade de esforço do equipamento influi muito, pois um computador não passa o tempo inteiro consumindo a mesma quantidade de energia elétrica. Exemplificando, um computador de configuração simples irá consumir muito mais energia elétrica do que um computador potente quando estiver rodando um jogo (game), pois estará funcionando no limite ou se esforçará bem mais (o processador estará no máximo e, assim, superaquecendo, com isso os *coolers* [ventiladores], também, funcionarão no máximo para tentar esfriar os componentes). O tipo, tamanho e a quantidade em que um monitor (tela ou visor) fica ligado, também, influi muito no consumo de energia elétrica. E, por dedução logica, quanto maior a necessidade de energia elétrica pelos componentes do

dispositivo, mais potente terá que ser a sua fonte de alimentação (conversor de energia elétrica), pois é ela que fornece a energia elétrica aos componentes do dispositivo.

O TDP (*Thermal Design Power* ou Projeto de Força Térmica) é um indicativo do consumo típico de um componente. Entretanto, ele não corresponde ao consumo máximo (que pode exceder o TDP por breves períodos), mas serve como estimativa do consumo contínuo máximo. Outro detalhe, é que, muitas vezes, a potência (capacidade) máxima informada numa fonte, não coincide com a realidade; pois muitos fabricantes esperam um consumo de apenas metade do valor mencionado. Assim, a eficiência de uma fonte genérica é, em torno, de 60% enquanto que, uma boa, possui, em média, a taxa de 80 a 85%. Na Internet existe calculadoras *on line* de potência para fontes de computadores.

- http://outervision.com/power-supply-calculator;
- http://images10.newegg.com/BizIntell/tool/psucalc/index.html?name=Power-Supply-Wattage-Calculator;
- http://physika.info/physika/javascript/pckalc.htm.

Também existe o Joulemeter; um programa desenvolvido pela Microsoft capaz de estimar o consumo de energia de qualquer máquina equipada com o sistema operacional Windows.

- http://www.baixaki.com.br/download/joulemeter.htm.

A mineração, através do conceito de prova de trabalho (PoW), na prática, vai remunerar mais quem tiver o melhor equipamento (maior eficiência energética na mineração) e quem tiver maior capacidade (mais *hashes* por segundo).

Atualmente a mineração de Bitcoin somente faz sentido em locais onde a energia elétrica é muito barata (ou até mesmo gratuita) e através de grandes *data centers* (centros de processamento de dados; ambiente projetado para concentrar servidores, sistemas de rede e equipamentos de processamento e armazenamento de dados). Desse modo, a mineração doméstica, mesmo utilizando-se ASICs - *Application-specific integrated circuit chips* (chips

de circuitos integrados de aplicação específica), não gera Bitcoins suficientes para que o investimento em equipamento e os gastos em energia elétrica sejam pagos. Portanto, a mineração de Bitcoin se tornou uma operação industrial e, assim, grandes empresas fazem parte deste mercado, controlando a rede de processamento do Bitcoin.

No Paraguai, a energia elétrica é barata; já no Chile, é gratuita porque o governo capta e fornece energia solar. Desse modo, os custos seriam apenas em relação ao equipamento e a conta da Internet.

- http://brasil.elpais.com/brasil/2015/09/10/politica/1441837292_242802.html;
- http://exame.abril.com.br/economia/chile-tem-tanta-energia-solar-que-agora-e-de-graca/.

O site http://www.coinwarz.com/cryptocurrency ajuda a calcular a rentabilidade da mineração de vários sistemas de criptomoedas.

No **Brasil**, além dos equipamentos serem mais caros, a tarifa de energia elétrica é muito cara e, ainda, sofre forte tributação pelo governo. A opção para os brasileiros minerarem seria, primeiramente, importar os equipamentos direto da China ou comprarem no Paraguai. E, por óbvio, usarem de fontes alternativas de energia elétrica; tais como, por exemplos, solar ou eólica (vento).

- http://www.portalsolar.com.br/;
- http://americadosol.org/;
- http://sunba.org.br/;
- http://www.neosolar.com.br/;
- http://www.solstar.com.br/;
- http://www.solefic.com.br/;
- http://www.solarbrasil.com.br/;
- http://www.hbenergiasolar.com.br/;
- http://www.geradorsolarfotovoltaico.com.br/;

- http://www.energiapura.com/;
- http://www.ledrenovavel.com.br/;
- http://www.ocaenergia.com/;
- http://www.brasilsolarpower.com.br/;
- http://bluesol.com.br/;
- http://fotovoltaica.ufsc.br/sistemas/fotov/.

Uma opção mais radical é instalar a mineradora em outro país onde a energia elétrica seja bem mais barata, como, por exemplo, o Paraguai.

- http://www.brbitcoin.com.br/custo-de-energia-eletrica-no-brasil-x-outros-paises/.

SolarCoin (http://solarcoin.org/en/front-page/) é uma moeda digital que incentiva a eletricidade solar. Os proprietários das instalações recebem SolarCoin através da geração de eletricidade solar. Por outras palavras, qualquer produtor de energia solar tem direito a receber SolarCoins gratuitamente. Em termos de eletricidade gerada, 1 SLR representa 1 MWh de energia solar. Cerca de 99% dos SolarCoins serão distribuídos aos geradores de energia solar ajudando produzir 97.500 TWh. A tecnologia por trás da SolarCoin é semelhante ao Bitcoin. SolarCoin podem ser trocadas com os comerciantes que participam ou por outras moedas on-line.

Para quem não tem condições de custear um bom equipamento para mineração, existem as opções de gerar bitcoin na nuvem (*cloud*) ou via *pool* (piscina).

- https://coinbr.net/mining;
- https://mercadolivrebtc.wordpress.com/2016/02/11/7-melhores-e-mais-confiaveis-servicos-de-mineracao-de-bitcoin-nas-nuvens/.

Ao juntar-se a um grupo de mineração, torna-se muito mais provável receber Bitcoins, mas a quantidade será bem menor. De qualquer forma, sem um supercomputador ou, ao menos, um equipamento especializado, dificilmente conseguirá algum lucro minerando Bitcoins.

NiceHash (https://www.nicehash.com/) é um serviço de mineração de criptomoeda na nuvem, que vende e compra hashrate para os algoritmos suportados, tais como, por exemplos, Scrypt, SHA256, Scrypt-N, X11, X13, Keccak, X15 ou Nist5 como NiceHash faz.

Confira a participação das piscinas de mineração bitcoin em https://blockchain.info/pools.

BLOCKCHAIN

A *Blockchain* (cadeia de blocos ou blocos em sequência) é um banco de dados *open source* (de código aberto), com registro distribuído (contabilidade distribuída ou "digital ledger") e operadores comunitários e anônimos. É uma espécie de planilha (tabela) de Excel gigante, consistente numa enorme lista de endereços (*address*) Bitcoins, que arquiva todas as transações efetuadas em Bitcoins (transferências de créditos, pagamentos). Mas tal registro da transação somente aparece na *Blockchain* após ter sido reconhecida (validada) pelos demais nós da rede e inseridas as respectivas marcas temporais (*timestamp* - uma cadeia de caracteres que mostra a data e hora em que certo evento ocorreu) e de interligação entre o bloco atual e o seu antecedente.

Já o Banco Central possui bancos de dados sobre todos os clientes bancários. O SRC (Sistema de Informações de Crédito do Banco Central), é um banco de dados alimentado pelas próprias instituições financeiras regulamentadas pelo Bacen; que contém informações sobre todas as operações de crédito (empréstimos, financiamentos, consórcios, limites de cartões de crédito, etc.) realizadas pelas pessoas, de valor total ou igual ou superior a R$ 200,00 (duzentos reais), junto ao sistema bancário brasileiro. Serve de fonte de consulta na análise de crédito, pois mostra de maneira abrangente (valores, pagamentos, limites, atrasos, etc.) as operações de crédito de um consumidor Pessoa Física (CPF) ou de Pessoa Jurídica (CNPJ). O CCS (Cadastro de Clientes do Sistema Financeiro), por sua vez, também é alimentado mensalmente pelas instituições financeiras e contém, basicamente, apenas os nomes das instituições (bancos, financeiras e corretoras) nas quais as pessoas possuem algum tipo de relacionamento. O sistema não apresenta valores, mas tão somente o nome, agência, número da conta e data de abertura e/ou encerramento das constas, aplicações e/ou investimentos. Ambos bancos de dados podem serem consultados no site do Banco Central (http://www.bcb.gov.br/pt-br/#!/p/REGISTRATO).

A *Blockchain* não é nenhum site apesar de constar cópias suas em vários sites. Explica-se. Por se tratar de um banco de dados descentralizado de uma rede P2P, a *Blockchain* não possui servidor e nemhum um site central. Desse

modo, não se deve confundir a *Blockchain* com a carteira (*wallet*) https://blockchain.info/ apesar desta possuir uma cópia da *Blockchain*.

A *Blockchain* não é Bitcoin. A *Blockchain* faz parte do sistema Bitcoin, mas com este não se confunde. A *Blockchain* não é o produto final e nem o início, mas o meio ou o intermediário das criptomoedas.

A palavra *Blockchain* se refere à tecnologia original ou ao livro contábil da rede Bitcoin. Já *blockchain* se refere aos clones da *Blockchain* ou como sinônimo de cadeia de blocos.

Infra alguns links de sites que mostram a *Blockchain*:

- https://blockchain.info/;
- https://bitcoinchain.com/;
- https://blockexplorer.com/;
- https://new.bitcoinchain.com/;
- http://block.oklink.com/;
- https://blockchains.io/;
- https://btc.com/;
- https://bchain.info/BTC/;
- http://btc.blockr.io/;
- https://blockscan.com/;
- https://btc.com/;
- https://bitaps.com/;
- https://www.smartbit.com.au/;
- http://bc.web-automation.ru/.

Confira, ainda, esses sites sobre os blocos do Bitcoin:

- http://btc.blockr.io/;

- https://blocks.wizb.it/;
- https://bitcoinwisdom.com/;
- http://www.thehalvening.com/;
- http://bitcoinclock.com/;
- https://coin.dance/blocks;
- https://data.bitcoinity.org/;
- https://www.blocktrail.com/BTC;
- http://www.bitcoinblockhalf.com/;
- https://bitcoinwisdom.com/bitcoin/difficulty;
- http://xtnodes.com/;
- http://www.bitcoinwatch.com/;
- https://www.smartbit.com.au/.

Já se tratando do Litecoin, o livro contábil ou de registros é em https://block-explorer.com/.

Em https://live.blockcypher.com/ é possível acessar o livro contábil de diferentes criptomoedas.

Descentralizar consiste em redistribuir os poderes ou funções atribuídas à uma autoridade ou entidade central, antes tida por total, plena e absoluta. Difere da desconcentração pelo fato desta ser esta uma distribuição ou delegação interna (dentro da mesma pessoa jurídica) de competências; ou seja, trata-se de uma simples divisão hierárquica de atribuições.

Um tipo de registro fundamental em transações comerciais é o *ledger* (livro-razão em contabilidade) e é justamente isso que a *Blockchain* é. A cadeia ou corrente de blocos (*Blockchain*) é como um livro público de registro de contabilidade compartilhado no qual toda a rede Bitcoin interage e confia. Todas as transações confirmadas são incluídas na cadeia de blocos. Desta forma, as carteiras de Bitcoin podem calcular seu saldo disponível e novas transações podem ser verificadas para que se possa usar bitcoins que

são realmente de propriedade de quem está gastando. A integridade e ordem cronológica da cadeia de blocos são protegidas por criptografia.

A *Blockchain*, portanto, se assemelha ao livro razão da contabilidade. Explica-se. Em contabilidade, o livro Razão registra os movimentos (pagamentos e recebimentos, débito e crédito, entrada e saída, lucros e perdas, etc.) detalhados, individualizados e cronológicos de todas as contas, consistindo no agrupamento de valores em contas de mesma natureza e de forma racional. No livro razão são indicadas todas e cada uma das operações, na medida e ordem em que ocorrem, assim como as alterações qualitativas e quantitativas produzidas nos recursos aplicados e nas origens destes recursos. O livro Razão deve incluir a data, a descrição do lançamento (conta e contra-conta ou contrapartida, acompanhada de histórico e documentos de referência) e os saldos entradas para cada conta contábil.

> "A melhor forma de descrever a blockchain é pensar em um banco de dados. Só que, em vez de ser guardado em um único computador (ou um conjunto específico de computadores), ele é guardado de forma distribuída por toda a internet. Além disso, esse banco de dados é praticamente imutável. Uma vez que algo foi registrado nele, não pode ser apagado ou modificado. A grande vantagem da blockchain é produzir um elemento cada vez mais importante no mundo de hoje: confiança. No mundo em que vivemos, a confiança é gerada por instituições centralizadas. Por exemplo, confiamos no nosso banco para afirmar que há um determinado valor em nossa conta. Confiamos no Estado para emitir um documento de identidade, que confirma quem somos. A blockchain permite gerar esses consensos sem intermediários. O "registro" desses fatos fica distribuído na própria internet." (http://www1.folha.uol.com.br/colunas/ronaldolemos/2016/09/1812287-tecnologia-do-bitcoin-pode-promover-transparencia-e-reduzir-brechas-para-a-corrupcao.shtml).

Em síntese, conforme visto no capítulo "COMO A BITCOIN É FEITA?", a rede Bitcoin compartilha um registro público chamado “Blockchain” (“Cadeia de blocos”). E este livro contábil, público, digital e universal, armazena um histórico de todas as transações já processadas na rede Bitcoin (desde o início até o presente). É como se cada minerador (*miner*) batesse

um carimbo (código ou *hash*) quando houvesse uma transferência autêntica de bitcoin e publicasse isso dentro desse livro público. A informação contida nesses blocos é processada por um sistema de mineração que, basicamente, é o processo de utilizar poder computacional para processar as transações e verificar a validade delas.

Desse modo, na *Blockchain* constam as informações contábeis como se fosse um único extrato bancário para todos os usuários de todos os bancos do mundo. Entretanto, é possível pesquisar transações ou endereços bitcoins específicos. Em cada operação de transferência de créditos são indicadas as contas (endereços Bitcoin) de onde saiu (debitou) e para onde foi (creditou). Apesar de não serem informados nome, documento, foto, endereço, telefone, e-mail ou o IP da conexão à Internet dos participantes da transação, é informado o IP do nó dentro da rede P2P que transmitiu (informou) primeiramente a referida transação, não significando que tenha sido ele que tenha efetuado a transação.

Quando se efetua uma transação (transferência de valores) de uma carteira de Bitcoin para outra, ela é imediatamente autenticada e escrita em um registro de transações gigantesco chamado de *Blockchain*; que possui cópias de segurança, idênticas e atualizadas (sincronizadas), em todos os nós completos da rede; cópia esta que deve ser sincronizada antes de qualquer nova transação.

Sintetizando, a *Blockchain* é comparável ao livro razão de contabilidade, cada bloco é como uma folha preenchida a ser anexada a referido livro e cada transação é como uma linha preenchida numa dessas folhas (blocos). Quando uma folha está cheia ou completa, ela é anexada ao livro. Esse procedimento é semelhante ao feito pelos estudantes que utilizam fichários ao invés de cadernos tradicionais. Durante as aulas eles levam apenas folhas em branco e incompletas para fazerem suas anotações nelas. Mas ao chegarem em casa, eles arquivam as folhas cheias juntamente com as demais cheias, na devida sequência cronológica.

Contraditoriamente ao sistema bancário tradicional onde a segurança está no sigilo, na centralização e no controle rígido sobre o sistema e as informações; a tecnologia da *Blockchain* é justamente baseada na abertura,

na publicidade e no controle comunitário do sistema. A distribuição da validade da transação dificulta extremamente qualquer tentativa de interferir no sistema.

> "Um Blockchain pode ser entendido como uma base de dados distribuída, *peer-to-peer* (não tem um nó central), que só aceita operações *append* (inserção no final) de blocos (daí o nome Blockchain) de informações criptografadas de transações, sendo que cada bloco contém também um hash (operação sobre um conjunto de dados que retorna um valor conciso) do bloco anterior, e que cada operação de *append* só é confirmada após o consenso entre determinados nós participantes." (http://britech.com.br/blog/mercado/blockchain-a-internet-dos-negocios/).

Cada transação é digitalmente assinada por vários membros com o objetivo de garantir sua autenticidade e garantir que ninguém a adultere, de forma que o próprio registro e as transações existentes dentro dele sejam consideradas de alta integridade.

Só passa a fazer parte da *Blockchain* aquele bloco que é reconhecido pelos demais nós da rede (elos da corrente) como verdadeiro; procedimento este efetuado através de algoritmos e cálculos matemáticos e computacionais que confirmam a autenticidade, a unicidade e a segurança da transação. É a partir desse procedimento de validação que novos blocos (informações, transações) vão sendo acrescidos, registrados e armazenadas no livro contábil (*Blockchain*), formando uma sequência de blocos imutáveis, descentralizados e seguros.

A codificação matemática é usada para resumir uma parte da informação original em um código, conhecido como *hash*. Qualquer tentativa de violação de qualquer parte de um bloco é evidenciada porque resulta num hash diferente do previamente conhecido e esperado.

Quando uma nova transação é recebida, grande parte dos nós da rede Bitcoin deve executar alguns algoritmos e, essencialmente, avaliar e verificar o histórico do bloco individual que é proposto e, assim, chegar ao

consenso de que o histórico e a assinatura são válidas, para depois permitir que a nova transação seja aceita no registro e, portanto, fazer com que o novo bloco seja adicionado à cadeia de transações (*Blockchain*). Caso a maior parte dos nós não reconheça a adição ou modificação da entrada de registro, tal entrada é negada e não é adicionada à cadeia. Esse modelo de consenso distribuído é o que permite que a *Blockchain* funcione como um registro distribuído sem a necessidade de que uma autoridade central diga quais transações são válidas e quais não são.

A *Blockchain* (cadeia de blocos ou livro razão) contém a história de toda a transação e propriedade criptográfica de todas as bitcoins desde o endereço criador até o último endereço atual. As informações registradas em *blockchain* são incorruptíveis e imutáveis e para reduzir o espaço de armazenagem são usadas Árvores de Merkle. Portanto, se um usuário tenta reusar moedas já gastas ("gasto duplo"), a rede irá rejeitar a transação. Ressalta-se, assim, que uma vez que se insere um registro na *Blockchain*, nenhum usuário consegue apagá-lo ou modificá-lo; ou seja, as transações ou transferências são irrevogáveis, irretratáveis e sem direito de desistência, arrependimento ou estorno. O que pode ser feito, é as partes entrarem em acordo e quem recebeu indevidamente acabar devolvendo voluntariamente. Numa eventual intervenção judicial, depois que a vítima conseguisse identificar a outra parte ou fornecer meios para que o juiz assim possa fazê-lo, o que um juiz poderia fazer seria, primeiramente, pressionar a parte requerida para efetuar a devolução sob pena de alguma medida coercitiva. Caso isso não resolva não é possível o juiz fazer isso “na marra” e nem há meios para que se possa fazer uma penhora dos bitcoins da parte requerida. Teoricamente o juiz poderia enviar um ofício para a empresa responsável pela carteira bitcoin do requerido, ordenando a realização do estorno; “não custa nada” tentar isso, mesmo que, em teoria, não daria certo porque a empresa não deveria ter acesso ao teor da carteira. De igual modo, o juiz ao receber uma resposta negativa, poderia tentar uma última vez insistir pedindo explicações e provas da impossibilidade de cumprir a ordem judicial, sob pena de crime de desobediência e outras medidas intimidativas. Por fim, caso tudo isso der errado, restará ao juiz efetuar a penhora de dinheiro convencional e/ou de outros bens e valores, caso saiba, ao menos, o CPF ou CNPJ da parte requerida.

Árvore de Merkle, *Merkle trees*, *Merkle root*, caminho de Merkle, *hash trees*, árvore de hash ou árvore de dispersão, é uma estrutura binária (dois nós filhos em cada nó; com dois ponteiros para duas estruturas diferentes, denominadas sub-árvore esquerda e sub-árvore direita) de dados, que contém um arquivo central com informações resumidas de dados maiores; onde as folhas são separações de blocos de dados em um arquivo ou conjunto de arquivos. Os nós de uma árvore binária possuem graus zero, um ou dois. Não confundir com os nós de ume rede P2P. Um nó de grau zero é denominado folha. Cada nó poderá ter até duas folhas. A profundidade de um nó é a distância deste nó até a raiz. Um conjunto de nós com a mesma profundidade é denominado nível da árvore. A maior profundidade de um nó, é a altura da árvore. A raiz da árvore é um valor de *hash* de todos os dados presentes na árvore. A raiz da árvore representa a chave pública. No topo de uma árvore de Merkle há uma dispersão superior (ou dispersão de raiz ou dispersão mestre). Em Bitcoin a árvore Merkle é usada apenas para organizar as transações dentro de um bloco (o cabeçalho do bloco contém apenas um *hash* de uma árvore). Cada bloco é uma estrutura de dados que contém as transações a serem incluídas na *Blockchain* (cadeia de blocos ou livro razão) por meio do trabalho dos mineradores na rede. O valor *hash* da raiz da árvore de Merkle é que contém as transações do bloco (cabeçalho ou ponteiro hash). Desse modo, as transações Bitcoins são hasheadas numa "Árvore de Merkle", onde apenas a raiz é levada em conta para o *hash* do bloco. As folhas são os dados a serem processados e os nós são os valores de *hash* de seus filhos. O *Hashcash* adiciona uma entrada no cabeçalho da mensagem eletrônica (*hash* do bloco ou *block hash*), cujo valor de *hash* deve iniciar com uma certa quantidade de bits de valor zero, que especifica o grau de dificuldade. Esta condição faz com que o remetente gaste processamento buscando satisfazê-la. Portanto, o grau de dificuldade para descobrir o valor de *hash* está na quantidade de zeros no início do cabeçalho do bloco (*block header*). No cabeçalho dos blocos está a chave para a segurança da *Blockchain* proporcionada pelo algoritmo de *proof-of-work* (prova de trabalho). Este elo é *hash* do cabeçalho do bloco anterior (*parent block*). Cada bloco tem um identificador único que é criado a partir do *hash* de seu cabeçalho que serve tanto como identificador único deste objeto na rede Bitcoin, quanto como prova de toda informação contida nele (incluindo as transações). Portanto, o bloco é composto por um cabeçalho contendo metadados sobre o bloco e uma lista de transações. Cada novo

bloco tem ligação matematicamente comprovada com todos os blocos anteriores a ele, pois cada bloco tem um *hash* como identificador único que inclui, em seu resultado, o *hash* do bloco anterior a ele na *Blockchain*. Por outras palavras, cada transação tem o seu id (o *hash* da transação) concatenado ao id da transação vizinha na árvore, que é submetida a uma dupla rodada da função hash SHA-256 sucessivamente até chegar à raiz. A estrutura binária da árvore de Merkle é semelhante à estrutura hierárquica utilizada em MMN (marketing multinível) e pirâmides financeiras (exemplo, BBOM). Árvores de Merkle podem ser usadas para proteger qualquer tipo de dados armazenados, manuseados e transferidos dentro e entre computadores. Atualmente, o principal uso de árvores de Merkle é para garantir que blocos de dados recebidos de outros pares em uma rede ponto-a-ponto são recebidos intactos e inalterados, e até mesmo para verificar se os outros pares (nós da rede P2P) não mentem e enviam blocos falsos. A árvore de Merkle recebida é comparada com a dispersão superior (anterior, antecedente ou histórico) confiável, e verifica-se se a árvore de Merkle está danificada ou falsa. Outra árvore de Merkle vinda de outra fonte será testada até o programa encontrar uma que corresponda (se encaixe) à dispersão superior. Saiba mais, infra, conferindo o termo: semente (*seed*).

A tecnologia da *Blockchain* permite que esses dados sejam distribuídos por todos os participantes, de maneira descentralizada e transparente. Dessa maneira, não é necessário mais a confiança na outra parte contrastante ou em um terceiro para que os dados de contabilidade estejam corretos e não sejam fraudados. Só passa a fazer parte da *Blockchain* aquele bloco que é reconhecido pelos demais elos da corrente como verdadeiro, sendo este processo baseado em algoritmos e cálculos matemáticos e computacionais que confirmam a autenticidade, a unicidade e a segurança da transação. Portanto, não depende da confiança entre os usuários (pessoas detentoras de cada nó da rede Bitcoin), mas na confiança no algoritmo.

Apesar de a *Blockchain* ser um registro global, é possível controlar, separadamente, o movimento de todas as contas. Exemplo: https://www.walletexplorer.com/address/129TQVAroeehD9fZpzK51NdZGQT4TqifbG.

Nos sites https://coin.cz/, https://www.walletexplorer.com/, http://bitcoinwhoswho.com/, https://live.blockcypher.com/ e https://www.biteasy.com/ é possível rastrear as movimentações de endereços bitcoins (*hashes*) específicos.

Através do Circle (https://www.circle.com/pt e https://support.circle.com/hc/pt-br) em vez de endereço Bitcoin são utilizados endereços de e-mail nas transações.

Uma transação consiste na transferência de valor entre carteiras Bitcoin, que é registrada na *Blockchain*. Carteiras Bitcoin mantém uma informação secreta chamada chave privada (*private key* ou *secret key*) ou *seed* (semente), que é usada para assinar transações, fornecendo uma prova matemática de que elas vieram do dono da carteira.

A palavra **semente (*seed*)** é simplesmente uma forma didática de expressar a chave utilizada como raiz, pois ela pode ser convertida algoritmicamente na chave privada raiz e uma única chave pode ser usada para gerar uma árvore inteira de pares de chaves. Usa-se o termo raiz para expressar que de um arquivo saem vários a ele subordinados; é similar (não exatamente semelhante) à pasta que identifica o disco rígido do computador, na qual ao irmos clicando, vão se abrindo outras pastas existentes dentro dessa primeira. Também é similar à uma mãe que gera filhas. Essa chave única não está substituindo todas as outras chaves privadas, mas está sendo usada para gerar elas. Todos os seus endereços ainda têm diferentes chaves privadas, mas todos elas podem ser restauradas por uma única chave. Já em uma carteira não-determinística (aleatória, portanto), cada chave é gerada aleatoriamente e elas não são semeadas (geradas) a partir de uma chave comum. Portanto, todos os *back-ups* (cópias de segurança) da carteira devem armazenar cada chave privada usada como um endereço. Para saber mais, confira, acima, o verbete: Árvore de Merkle.

Por outras palavras. A posse do bitcoin é estabelecida através de chaves digitais, endereços bitcoin e assinaturas digitais. Na realidade, as chaves digitais não são armazenadas na rede, mas ao invés disso, são criadas e armazenadas pelo usuário em um arquivo, um banco de dados simples, chamado de *wallet* (carteira). As chaves digitais em uma carteira de um

usuário são completamente independentes do protocolo Bitcoin e podem ser geradas e gerenciadas pelo software de carteira do usuário sem qualquer referência à *Blockchain* ou acesso à Internet. No Bitcoin usa-se a criptografia de chave pública para criar um par de chaves que controla o acesso aos bitcoins. O par de chaves consiste em uma chave privada ou secreta (similar a um PIN secreto, uma assinatura em um cheque ou a senha de uma conta bancária) e, derivada dessa, uma chave pública única. A chave pública é usada para receber os bitcoins (é o endereço bitcoin; similar ao número de uma conta bancária) enquanto que a chave privada correlata é usada para assinar transações para gastar os bitcoins. Desse modo, toda transação de bitcoin requer uma assinatura válida para ser incluída na *Blockchain*; que só pode ser gerada com as chaves digitais válidas (exclusivas daquele endereço público).

A assinatura também previne que a transação seja alterada por qualquer um depois de emitida. Todas as transações são divulgadas entre os usuários (pela rede Bitcoin) e normalmente começam a ser confirmadas pela rede nos próximos 10 (dez) minutos, através de um processo chamado mineração (*mining*).

A *Blockchain* é vista como a grande inovação tecnológica do Bitcoin, vez que é a prova de todas as transações na rede. Através dos blocos é que a *Blockchain* vai sendo atualizada e registrando todas as transações. Cada vez que um bloco é concluído, ele é ligado aos já existentes na *Blockchain*, como elos de uma corrente; ou seja, de forma linear e em ordem cronológica, com cada bloco contendo um hash do bloco anterior. É similar ao jogo de dominó.

A *Blockchain* é como se fosse o registro histórico de todas as transações bancárias de todas as pessoas no mundo, mas não deixam de ser extratos bancários individuais. Ela pode, portanto, fornecer uma visão sobre fatos como a quantidade de valor pertencia um determinado endereço (*address*), em qualquer momento no passado. Exemplo: https://webbtc.com/address/129TQVAroeehD9fZpzK51NdZGQT4TqifbG.

Portanto, todas as transações realizadas podem ser verificadas através de um registro público que garante a transparência e a inviolabilidade das

transações.

Frisa-se, assim, que apesar de todas as transações de bitcoins serem públicas e a carteira dos usuários pode ser vista por qualquer um, não significa que possa ocorrer manipulação ou que se identifique a pessoa dos usuários. Explica-se. Nenhum arquivo ou informação da rede Bitcoin ou da *Blockchain* é associado ao nome ou qualquer identificação da pessoa. Por exemplo, a carteira do "The Pirate Bay" (https://thepiratebay.org/), o famoso site de pirataria, é identificada simplesmente como "129TQVAroeehD9fZpzK51NdZGQT4TqifbG". Qualquer um sabe esse endereço deles porque eles o divulgam publicamente no site. Por isso, se diz que a bitcoin é "semianônima". Ela funciona desse jeito para promover a transparência e evitar fraudes que desequilibrem o sistema.

- http://btc.blockr.io/address/info/129TQVAroeehD9fZpzK51NdZGQT4TqifbG;
- https://blockchain.info/pt/address/129TQVAroeehD9fZpzK51NdZGQT4TqifbG;
- http://thepiratebayz.org/user/Gileo95/0/4/0/bitcoin:129TQVAroeehD9fZpzK51NdZGQT4TqifbG.

O tamanho sempre crescente da *Blockchain* é considerado por alguns como um problema devido a questões como armazenamento e sincronização. Em média, a cada 10 (dez) minutos, um novo bloco é acrescentado à cadeia bloco através da mineração. De fato, o problema de cada usuário ter de puxar e armazenar todo o histórico vai tornar-se impraticável se o Bitcoin alcançar grande aceitação. Para facilitar isto sem invalidar o hash dos blocos, as transações são hasheadas numa árvore de Merkle, onde apenas a raiz é levada em conta para o hash do bloco. Blocos velhos podem então ser compactados cortando-se os galhos da árvore. Os hashes interiores não precisam ser armazenados. Num cenário em que os usuários de Bitcoin vão criando novas chaves e abandonando as antigas, o histórico pode ser regularmente deletado. Mesmo que assim não faça, considerando a evolução tecnológica, o volume de armazenamento não deve ser um problema mesmo que os cabeçalhos de bloco precisassem ficar na **memória RAM** (*Random Access Memory* ou Memória de Acesso Aleatório); ou seja, na memória

temporária do dispositivo, que é usada pelos programas que estão em execução.

A *Blockchain*, inclusive, pode acabar com Swift (sistema de comunicação interbancária): http://brasilinvestidores.com.br/blockchain/.

Infra alguns dos **benefícios da utilização da *Blockchain***:

- **Transparência** - qualquer membro da rede pode acessar o histórico de registros e rastrear as transações;

- **Confiança** - a informação validada que entra no bloco é imutável, reduzindo as chances de fraude;

- **Segurança** - criptografia e outros aspectos tecnológicos garantem a confidencialidade e integridade das informações;

- **Descentralização** - o conceito de cópias distribuídas reduz as chances de fraude e elas ficam menos suscetíveis a ataques e/ou manipulações;

- **Delegação de funções** – similar à descentralização, ocorre o desmembramento de tarefas e responsabilidades para serem mais, fácil, eficaz e rapidamente, efetuadas por vários membros em trabalhos em conjunto apesar de, física e geograficamente, isolados. Essa nova modalidade de trabalho em equipe de pessoas totalmente estranhas e distantes não é nenhuma novidade para gamers (jogadores de videogames), que estão habituados com isso em jogos on line multiplayers (múltiplos jogadores);

- **Imparcialidade** – como consequência, direta e lógica, da segurança, as informações não sofrem manipulações ou interpretações tendenciosas;

- **Economia** - com a desburocratização e descentralização há substancial redução nos custos;

- **Agilidade** – o procedimento é muito mais rápido do que os convencionais;

- **Preservação** – os dados, arquivos e/ou informações são preservados através das inúmeras cópias idênticas que são constantemente sincronizadas;

- **Poliglota** – através das linguagens universais da matemática e da informática os diferentes idiomas são facilmente superados;

- **Despreconceito** – pelo fato de não envolver contato, relacionamento ou interação humana, mas somente a interação entre máquinas, os seres humanos proprietários ou utilizadores desses equipamentos, ficam impossibilitados de sequer saberem quem são as outras pessoas (sexo, idade, etnia, religião, filosofia, credo, time de futebol, nacionalidade, região geográfica, grau de instrução, quociente de inteligência, ideologia política, aparência física, vestimentas, saúde, voz, situação econômica, vícios, hábitos, defeitos, trejeitos, manias, etc.) "por trás" demais máquinas; mesmo que soubessem, não tem como evitar a interação indireta com quem quer que seja;

- **Interação global** – o sistema envolve um trabalho comunitário mundial, que pode ser o primeiro passo ou o trampolim de algo maior;

- **Trabalho em conjunto** – o sistema implica em algo muito superior a qualquer dinâmica de trabalho em equipe anteriormente utilizada por qualquer empresa ou entidade;

- **Colaboração** – possibilidade de ser programado para executar operações específicas quando outras estão concluídas ou determinados eventos ocorreram. Isso ajuda a todos os envolvidos sem aumentar o risco em operações com várias agências ou autorizados por diferentes partes;

- **Escalabilidade** - capacidade e preparação prévia para manipular a crescente demanda de trabalho de forma uniforme, sem comprometer a continuidade, qualidade, quantidade e velocidade;

- **Constância** – em razão de ser um sistema on line de abrangência internacional, opera 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

- **Internacionalidade** – através da Internet as fronteiras dos países são superadas;

- **Ecológico** – através da eliminação de papéis, metais, tintas, solventes, plásticos, carimbos e assinaturas físicas e do transporte de tais elementos através de veículos automotores movidos à combustíveis fósseis, o meio ambiente é poupado;

- **Compactação estrutural** – através da desburocratização, desmaterialização e conectividade, há uma enorme diminuição das estruturas físicas e, com isso, a economia do espaço que era utilizado por elas;

- **Diminuição de erros** – pelo fato de grande parte do trabalho ser feita pelo algoritmo, existe significativa diminuição de falhas humanas;

- **Redução de encargos trabalhistas** – além da diminuição da infraestrutura física, ocorre uma grande diminuição na necessidade de trabalhadores humanos, com o que, há uma enorme economia com encargos trabalhistas;

- **Independência** – pelo fato dos trabalhos serem em conjunto e do banco de dados ser distribuídos em várias cópias idênticas e atualizadas, cada unidade do sistema ou rede pode sofrer pane, falha ou defeito e, até mesmo, ser desligada para reparos, manutenção ou aperfeiçoamento sem prejudicar a continuidade dos trabalhos;

- **Estímulo *high-tech*** – através da valorização, aplicação e investimentos na referida tecnologia, cria-se um *habitat* virtual ou ecossistema cibernético (conjunto de circunstâncias, meios, recursos, fatores e condições favoráveis, propícias, adequadas e estimuladoras à geração, criação, surgimento, estabelecimento, organização, desenvolvimento, integração e continuidade), no qual outras tecnologias, serviços (consultorias, cursos, palestras, treinamentos, suporte, incubadoras, etc.) e produtos surgem ante a necessidade ou demanda surgida. Em suma, ocorre um progresso ou desenvolvimento tecnológico direto e integrado, tal como, por exemplo, o que ocorre no chamado Vale do Silício (*Silicon Valley*), que é a região (entre o sul da área da baía de São Francisco até os subúrbios de São José, na Califórnia, Estados Unidos) na qual está situado um conjunto de empresas implantadas à partir da década de 1950 com o objetivo de gerar inovações científicas e tecnológicas, destacando-se na produção de circuitos eletrônicos, na eletrônica e informática, que se tornou um grande polo industrial dessas áreas. Em Israel existe o *Silicon Wadi*, uma área com alta concentração de indústrias de tecnologia de ponta;

A tecnologia da *Blockchain*, o coração do Bitcoin, está ganhando força em um número crescente de aplicações comerciais, atiçando o interesse dos investidores.

- https://jornalbitcoin.pt/index.php/noticias/item/358-blockchain-doze-novos-bancos-aderem-ao-consorcio-r3.

O método de controle de consenso do Bitcoin (PoW - prova de trabalho ou de esforço) não é necessariamente o mesmo em todas as implementações de *blockchain*. Desse modo, é perfeitamente possível programar essa estrutura de dados de forma que alterações somente sejam permitidas a partir de nós com a permissão adequada.

Como a estrutura da *Blockchain* pode armazenar praticamente qualquer dado, a criatividade é o limite para seu uso; desde a liquidação de transferências de fundos até o controle de propriedade de ativos reais ou virtuais.

- https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Oportunidades%20com%20Blockchain%20-%20Paschoal%20Pipolo%20Baptista%20-%2023_06_2016.pdf.

A tecnologia da *Blockchain*, portanto, pode ser usada para qualquer coisa que represente valor. A plataforma Ethereum, por exemplo, permite que qualquer programa seja incorporado à *Blockchain* de forma a desfrutar de suas vantagens. Por outras palavras, é possível usar o sistema da *Blockchain* para registrar digitalmente qualquer coisa: a existência de um documento, a notarização, a autenticação, títulos de propriedade, ativos, ações, contratos, etc.

> "Um Bitcoin pode ser dividido em até 100 milhões de unidades, e cada unidade é individualmente identificável e programável. Isso significa que usuários podem designar propriedades para cada unidade. Usuários podem programar uma unidade para representar 1 centavo de euro, ações de uma empresa, 1 kWh de eletricidade, ou um certificado de posso digital. Por isso, Bitcoin é muito mais que apenas dinheiro e pagamentos.
>
> Um Bitcoin pode representar vários tipos de propriedade: Mil barris de petróleo, prêmios, ou um voto nas eleições, por exemplo. Além disso, Bitcoin nos permite deixar nossa moeda mais inteligente, e automatizar nosso dinheiro e o fluxo monetário. Imagine um subsídio de plano de saúde em dólares ou euros que só pode ser usado para pagar convênios em determinados hospitais. Neste caso, se alguém segue as regras, o processo não é verificado em um processo burocrático. Você simplesmente programa essas regras no dinheiro, e o resultado é um registro imediato. A unidade pode ser programada de modo que volte automaticamente para o fornecedor, se o destinatário não a usar após determinado período. Deste modo, o fornecedor pode garantir que subsídios não serão acumulados.
>
> Uma empresa pode controlar seus gastos da mesma forma, programando orçamentos para salários, maquinário, materiais e manutenção para que o dinheiro em questão não possa ser gasto m outras coisas. Automatizar tais tarefas nos leva a uma diminuição considerável na burocracia que poupe um bom tempo de contadores, controladores e empresas em geral. O aspecto programável e aberto do Bitcoin nos

permite reconstruir e inovar nosso setor financeiro e nossos processos administrativos. Torná-los mais eficientes e transparentes, e diminuir bastante a burocracia.

E ainda tem mais: em uma "internet das coisas", nossa economia trabalhará com máquinas que participam ativamente da nossa economia. Na verdade, elas já estão aqui. Pense em uma máquina de vendas, ou drones de entrega. Estas máquinas não conhecem o conceito de confiança, mas o Bitcoin conhece. Graças ao Bitcoin, o drone pode ter certeza absoluta que vai entregar o pacote ao destinatário certo e saber com certeza se ele já foi pago. E nós podemos programar a máquina de vendas de modo que ela automaticamente mantenha o registro de seus produtos, encomendar novos produtos do fornecedor e pagar por eles automaticamente. Você precisa entender que isso é apenas o começo. A tecnologia da internet é disruptiva e quebra o *estatus quo*. Ela abre mercados e toma o lugar do intermediário o tempo inteiro. Bitcoin e criptomoedas causaram uma mudança de paradigma." (http://www.moedasdigitais.com.br/o-blockchain-da-criptomoeda-claramente-explicado/).

As **cadeias laterais (*sidechains* ou *Blockchain* 2.0)** são extensões para *blockchains* existentes, melhorando a sua privacidade e funcionalidade, adicionando recursos como contratos inteligentes e transações confidenciais.

- https://blockstream.com/technology/#sidechains;
- https://www.blockstream.com/sidechains.pdf.

Para quem ainda não percebeu, não estamos falando de ficção científica ou de algo que, em tese, somente acontecerá daqui a décadas. Não! Nem do iminente (que está prestes a acontecer) ou do presente (agora) estamos nos referindo. Muita coisa de que estamos falando já é passado (já virou realidade, já aconteceu e já faz parte do cotidiano). O que está prestes a acontecer é a quarta geração dessa revolução e, muitas pessoas nem sequer sabiam que o bisavô tinha nascido.

O mercado de *fintechs* no Brasil não para de crescer. Já são mais de 200 iniciativas que estão facilitando a vida das pessoas e empresas e/ou criando

condições para que o ecossistema digital evolua, colocando o Brasil à frente de todos os seus irmãos da América Latina!

- http://fintechlab.com.br/index.php/2016/09/08/novo-radar-fintechlab-ja-sao-mais-de-200-empresas/.

Em conclusão, não se sabe se o Bitcoin "veio para ficar". A única coisa certa é que a *Blockchain* se consolidou como um marco, "um divisor de águas", que provocou uma revolução no processamento e na validação de dados e arquivos; tanto que deu origem às *blockchains* alternativas (altchains) e, disso, surgiram as Sidechains (cadeias laterais); que é uma *blockchain* que valida dados de outras *blockchains*. Essa tecnologia foi desenvolvida como uma alternativa para promover integração entre *blockchains* e adicionar funcionalidades, sem a necessidade de se modificar os scripts das cadeias. Não confundir com Side chain (método de compressão de áudio) e nem com SwissSidechain (base de dados de mecânica estrutural e molecular de centenas de cadeias laterais de aminoácidos não naturais que podem ser utilizados para estudar *in silico* sua inserção em péptidos ou proteínas naturais).

Sidechains (https://elementsproject.org/sidechains/) é uma tecnologia que pretende estender as funcionalidades do protocolo bitcoin de forma a permitir uma maior interoperabilidade entre esta rede e outras redes. É um projeto desenvolvido pela Blockstream (https://blockstream.com/). A Ripple (https://ripple.com/) também apresentou uma prova de conceito (Interleger) para responder ao mesmo problema.

A **Lisk** (https://lisk.io/), é a primeira criptomoeda modular a utilizar sidechains; ou seja, a colocar em prática o tão discutido conceito de usar sidechains para ampliar infinitamente a facilidade de expansão de um ecossistema de ativos digitais sem impactar na velocidade de desempenho da *blockchain* central. Os sidechains são livros contábeis criptográficos independentes que se ligam a *blockchain* principal, mas não impactam na velocidade ou na segurança da cadeia principal.

A **Accenture** (https://www.accenture.com/br-pt) patenteou uma nova ferramenta para edição da tecnologia *Blockchain*.

O **ChronoBank** (https://chronobank.io/) é um ambicioso e abrangente projeto de *blockchain*.

Existem diversos modelos de negócios surgindo a partir do conceito de plataforma descentralizada utilizando a *blockchain*, como a Internet descentralizada do MaidSafe (https://maidsafe.net/), o Uber sem intermediário do Arcade City (https://arcade.city/), a distribuição de músicas pelo Ujo Music (http://ujomusic.com/), o comércio eletrônico P2P do OpenBazaar (https://openbazaar.org/), os contratos inteligentes da Rootstock (http://www.rootstock.io/), seguro peer-to-peer da Dynamisapp (http://dynamisapp.com/), certificados de autenticidade da Stampery (https://stampery.com/), entre diversos outros.

> "Fintech é o nome dado a negócios inovadores que trabalham com tecnologias financeiras e entregam uma solução (serviço ou produto) diferenciada ao cliente (B2B ou B2C). Eles podem oferecer os mesmos serviços que um banco (como liberação de empréstimos, emissão de cartões, contratação de seguros) ou serviços que complementam aqueles oferecidos pelas instituições financeiras. Possuem estrutura mais enxuta, o que gera serviços mais eficientes e baratos. Transformando o setor, as Fintechs obrigam grandes corporações a se adaptarem para oferecer serviços mais práticos e tecnológicos, visando um público que começa a focar mais em mobilidade, praticidade e personalização." (Fonte: http://www.bigdatabusiness.com.br/4-tendencias-que-estao-transformando-o-setor-financeiro/).

No final de 2015, o mundo já contava com 268 *startups* (empresas novas, até mesmo embrionária ou ainda em fase de constituição) financeiras baseadas em *Blockchain*.

- http://startupmanagement.org/2015/12/08/update-to-the-global-landscape-of-blockchain-companies-in-financial-services/.

NXT (https://nxt.org/) é uma plataforma *blockchain* avançada.

O **OneCoin** (https://www.onecoin.eu/pt/) é considerado, por alguns, a mais avançada *blockchain* do mundo e o único pronto para uso de forma comercial, que a colocaria na liderança para se tornar a primeira

criptomoeda de reserva global no mundo. A OneCoin é uma empresa de educação financeira com foco em moedas criptografadas, que busca revolucionar o mercado econômico por meio de conceito pioneiro em criptomoeda e modelo de negócios. A OneLife (https://www.onelife.eu/pt/) é a comunidade on line que reúne os usuários globais da OneCoin e traz informações sobre novos produtos da empresa que está presente em quase todos os países.

O **Orisi** (http://www.oraclize.it/) oferece soluções para implementação de oráculos inteligentes nas cadeias de blocos.

O objetivo da **Ripple** (https://ripple.com/) é criar uma rede paralela à Swift, a cooperativa que gere as mensagens interbancárias a nível mundial, que deverá funcionar como player mundial no domínio dos pagamentos internacionais no segmento bancário e corporativo.

A **Stellar** (https://www.stellar.org/) foi criada pelo mesmo fundador da Ripple, que entrou em dissidência com esta. Dedica-se ao mercado das microfinanças, como o mesmo objetivo de criar uma Swift para as MFIs (*Microfinance Institutions*). Microfinanças é uma fonte de serviços financeiros para os empresários e pequenas empresas que não têm acesso aos serviços bancários e serviços relacionados.

O **BigchainDB** (https://www.bigchaindb.com/) é um banco de dados descentralizado, federado e customizável, capaz de armazenar um milhão de registros por segundo, pentabytes de capacidade, e uma rica variedade de queries e permissões.

A **DECENT Network** (https://sale.decent.ch/) é um projeto de longo prazo que quer resolver os problemas atuais dentro da distribuição mundial de conteúdo através da implementação de princípios de descentralização no fluxo de comunicação da sociedade atual. A tecnologia *Blockchain* poderia se tornar um sistema unificado de compartilhamento e publicação de conteúdo digital por todo o mundo. O objetivo geral do DECENT de criar um sistema mundial confiável e totalmente integrado de distribuição de conteúdo digital já está formado.

Colored Coins (http://coloredcoins.org/) é um protocolo *open-source* para a criação de novos ativos digitais utilizando a infraestrutura da *Blockchain*.

O **BitProof** (https://bitproof.io/) é o melhor dos aplicativos de marcação de tempo (data e hora) em documentos. Existem similares gratuitos como o Blocksign (https://blocksign.com/) e o OriginStamp (http://www.originstamp.org/), mas o BitProof oferece mais serviços, incluindo um que visa a proteção de propriedade intelectual. O BitProof, ainda, colocou na *Blockchain* os certificados acadêmicos estudantis da Holberton School de São Francisco.

- http://bravenewcoin.com/news/timestamping-on-the-blockchain/.

A tecnologia da *Blockchain* permite que qualquer pessoa valide um **certificado acadêmico** (diploma) sem precisar contatar a universidade.

- http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/;
- http://blog.bitcuners.org/post/141677189258/sony-comenzó-a-usar-blockchain-para-certificados.

O projeto **Hyperledger** (https://www.hyperledger.org/) permite que as pessoas assinem digitalmente os dados e pode ser configurado para ser público, anônimo, sem assinatura ou com dados cifrados, com políticas de controle.

A **Ascribe** (https://www.ascribe.io/) permite que artistas reivindiquem propriedade e emitam impressões numeradas de edição limitada de todo tipo de obra de arte em seu formato digital com o uso da *Blockchain*.

- http://bravenewcoin.com/news/ascribe-wants-to-build-the-ownership-layer-of-the-internet/;
- https://jornalbitcoin.pt/index.php/noticias/item/601-deloitte-demonstra-a-utilizacao-do-blockchain-para-o-negocio-das-artes;
- http://www2.deloitte.com/lu/en/pages/technology/articles/blockchain-proof-concept-solve-traceability-issues-art.html.

O **Verisart** (https://www.verisart.com/) confirma a autenticidade e a autoria da obra artística.

O **Blockverify** (http://www.blockverify.io/) usa a *Blockchain* para autenticar uma grande variedade de bens de alto valor.

O **UProov** (https://uproov.com/) é efetua marcação de tempo (data e hora) em fotos e vídeos. É criada uma chave exclusiva de marcação de tempo a partir do arquivo (foto ou vídeo), que é posteriormente inserida na *Blockchain*. O arquivo, então, é bloqueado, com o que a alteração de um simples pixel no arquivo fará com que a chave não corresponda. Trata-se de uma prova de integridade sólida do arquivo.

Já em arquivos de áudio, o serviço é através do http://myceliaformusic.org/.

- http://www.bitcointoyou.com/blog/blockchain-direitos-autorais/.

O **SingularDTV** (https://singulardtv.com/) é um projeto que usa a *blockchain* do Ethereum para *streaming* (projeto Mycelia); é como se fosse uma descentralização do Netflix (https://www.netflix.com/br/).

A **Colu** (https://www.colu.com/) é a primeira empresa a permitir que outras empresas emitam ativos digitais com uma vasta variedade para várias utilizações, desde o setor financeiro (participações, títulos, ações), registros (certificados, direitos autorais, documentos) e até propriedade (ingresso de eventos, *vouchers* e cartões presente). A **Warranteer** (http://www.warranteer.com/) usa a Colu para levar as garantias de seus produtos do papel para a *Blockchain*, mantendo-as atualizadas e facilmente transferíveis. Embora a carteira gratuita de bitcoin Counterparty (http://counterparty.io/) já permitisse a emissão e negociação de códigos simples entre os donos de carteiras; os códigos da Colu, além de poderem ser de várias formas e tamanhos, podem sair e entrar novamente em seus sistemas e, até mesmo, armazenar dados na rede BitTorrent quando forem grandes demais para serem colocados na *Blockchain*.

A **DIGIX** (https://www.dgx.io/) é uma plataforma de ativos de tokenização construído sobre Ethereum, que aproveita a imutabilidade, transparência e auditabilidade da *Blockchain* em ativos físicos preciosos.

O Google Cloud, imitando a Amazon, Microsoft e IBM, passando a oferecer os serviços da *Blockchain* a seus clientes.

- http://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=43598&sid=97;
- http://tecnologia.uol.com.br/noticias/reuters/2015/11/10/microsoft-lanca-plataforma-blockchain-em-parceria-com-empresa-iniciante.htm;
- http://guiadobitcoin.com.br/microsoft-disponibiliza-servico-de-criacao-de-blockchains-no-azure-baas/;
- http://news.microsoft.com/pt-br/microsoft-e-bank-of-america-azure-blockchain-como-servico/#sm.00000zwxjbdh9hda3znlssqkgb9kh#HvczgL9Wz22IWCx8.97;
- http://www.forbes.com/sites/laurashin/2016/05/02/amazon-steps-up-blockchain-commitment-web-services-partners-with-digital-currency-group/#1b9f1eed712e;
- http://economia.uol.com.br/noticias/bloomberg/2016/09/23/google-cloud-imita-amazon-e-ibm-e-oferece-blockchain-a-clientes.htm.

A **Genecoin** (http://genecoin.me/) coloca uma cópia do genoma (DNA sequenciado) do cliente na *Blockchain*.

A estrutura da *Blockchain* é excelente para o acompanhamento da instalação, realização e locomoção de coisas, objetos, bens, produtos, recursos e trabalhos numa cadeia logística, desde o início da aquisição dos insumos necessários (controle do estoque, cada item na linha de montagem da fábrica, fornecedores, linhas de transmissão, etc.) até o atendimento ao cliente ou consumidor final.

A tecnologia da *Blockchain* pode ser usada não só para rastrear em tempo real verbas, bens, pessoal e serviços púbicos, como, também, pode ser utilizada para dificultar fraudes eleitorais.

- http://www1.folha.uol.com.br/tec/2016/06/1783365-por-transparencia-grupo-quer-usar-tecnologia-do-bitcoin-em-eleicoes-de-sp.shtml;
- http://news.chinacybersafety.com/20160823148.html;

- https://jornalbitcoin.pt/index.php/item/444-eleicoes-na-ucrania-podem-vir-a-ser-efectuadas-no-ethereum-blockchain;
- https://cripto-pay.com/2015/12/elecciones-con-blockchain/;
- https://cripto-pay.com/2016/06/como-votar-con-blockchain/.

BitCongress (http://www.bitcongress.com/) é uma plataforma descentralizada de votação.

Em **hospitais**, a tecnologia da *Blockchain* pode administrar os diferentes tipos de indivíduos envolvidos (pacientes, visitantes, médicos, enfermeiros, técnicos de enfermagens, secretárias, cozinheiras, faxineiras, zeladores, estoquistas, seguranças, etc.) com as diferentes tarefas relacionadas. Assim, à medida que cada pessoa atualiza seu *status* (chegada, saída, localização, conclusão de tarefa, requisição de material ou serviço, etc.), o sistema não só repassa a informação, como, também, já emite as ordens de serviços correspondentes e relacionadas e aciona as pessoas responsáveis pelos atos. Em resumo, além das funções básicas de registro e busca de recursos, conecta identidades e aplicações e, inclusive, restringe o acesso a arquivos confidenciais somente às pessoas necessárias e somente informa o que for necessário para a atividade dessa pessoa.

- https://gem.co/health/.

A **Everledger** (http://www.everledger.io/) usa a *Blockchain* para rastrear diamantes individualmente desde a mina até o pós-venda. Everledger é, portanto, um livro contábil permanente de certificação de diamantes e histórico de transações relacionadas; realizando verificações para seguradoras, proprietários, requerentes e autoridades de aplicação da lei.

A **Provenance** (https://www.provenance.org/) visa o registro na *Blockchain* de cada detalhe (todas as etapas, trajetos e intermediários) do que acontece na cadeia de suprimento de varejo mundial, tornando todas essas informações acessíveis e pesquisáveis em tempo real pelos consumidores. É semelhante ao Everledger, só que abrange todos os produtos. É justamente isso que a IBM quer fazer com seus parceiros de

negócios (http://www.bitmag.com.br/2016/09/ibm-blockchain-alem-da-bitcoin/).

Já a **Wave** (http://wavebl.com/) foca na cadeia de fornecimento mundial, especialmente nos documentos de importação (conhecimentos de embarque) a serem inseridos na *Blockchain*; com o que todos os membros (fabricantes, transportadoras, bancos, despachantes de mercadorias, negociadores, seguradoras, importadores, etc.) da cadeia de fornecimento ficam interligados e podem efetuarem trocas diretas de documentos entre eles.

A **Filament** (https://filament.com/) usa dispositivos de hardware pequenos e avançados para colocar todos os tipos de eletrônicos, especialmente equipamentos, na *Blockchain*, criando uma internet das coisas (conjunto de tecnologias capazes de conectar aparelhos e objetos entre si, sem intervenção humana e por meio de sensores).

O **Hyperledger** (https://www.hyperledger.org/) é um projeto que tenta unificar todas as abordagens de código aberto da *Blockchain* que existem atualmente, objetivando um *framework* (ou biblioteca) de *blockchains* de propósito geral que possa ser utilizado em vários setores da indústria, dos serviços financeiros, varejo, fabricação, etc. De modo semelhante, a **IBM** (http://www.ibm.com/blockchain/) está adaptando a metodologia da *Blockchain* para desenvolver um sistema sem moeda que poderia ser usado para qualquer fim, como, por exemplo, a execução de contratos mediante entrega.

O **Slock.it** (https://slock.it/) visa a integração do conceito de Internet das coisas (*Internet of things*) com a *Blockchain* aplicado aos sistemas de travas físicas de segurança. O *software* "smart locks" pode ser controlado por um aplicativo de *smartphone*. A ideia é alugar (cofre, caixa postal, armário, garagem, armazém, etc.) ou vender qualquer coisa sem nenhum intermediário; inclusive imóveis como faz o https://www.airbnb.com.br/.

- https://www.docyousign.com.br/blog/o-futuro-da-locacao-de-veiculos-e-simples-basta-clicar-assinar-e-dirigir/.

O projeto teste "**TransActive Grid**" (http://transactivegrid.net/) está permitindo vizinhos comprarem e venderem energia renovável entre si,

oferecendo micro redes elétricas comunitárias como um modo de criar um mercado de energia local e, ao mesmo tempo, reduzem a emissão e poluição (e também reduzem gastos com altos encargos do setor elétrico).

No setor de **videogames**, existem vários jogadores (*gamers*) que acumulam itens virtuais repetidos, desnecessários ou inúteis em jogos como parte de suas conquistas, mas ainda não há uma maneira de converter esses prêmios (recompensas, bônus, brindes) de seu trabalho em dinheiro. Por outro lado, existem outros jogadores que desejam conseguir tais itens no mesmo jogo, mas nenhum deles sabem como concretizar isso. A tecnologia da *Blockchain* poderia ajudá-los a criar novos ativos e a vendê-los ou trocá-los com outros jogadores. Mas eis que surge a **FreeMyVun**.

O **Eth-Tweet** (http://ethertweet.net/ui/ e https://github.com/yep/eth-tweet) é uma espécie de rede social descentralizada (sem controle central), que garante a plena liberdade de expressão e de que a conta e a postagem não serão excluídas por desagradar alguém e nem serão desprezadas por causa da maior divulgação de anúncios pagos e postagens patrocinadas.

A **Synereo** (https://www.synereo.com/) pretende descentralizar as redes sociais, partilhando receitas em função do grau de participação dos utilizadores.

O **Projeto Maelstrom** (http://blog.bittorrent.com/tag/maelstrom/), da BitTorrent (http://www.bittorrent.com/lang/pt/downloads/win), é um navegador de torrents via P2P que vai permitir que o usuário lance seu site em torrent e hospede nos computadores dos *peers* da rede!

- http://utorrent.us5.list-manage.com/subscribe?u=a3baea4e54ff8e8b235488c11&id=508b75f69b.

A **ZeroNet** (https://zeronet.io/) é a Internet descentralizada, aberta, livre e sem censura de sites, usando a criptografia do Bitcoin e a rede BitTorrent.

O **BitCloud** (http://bitcloudproject.org/) propõe substituir toda a Internet por um sistema descentralizado (http://www.wired.co.uk/article/bitcloud).

A **IBREA** - *International Blockchain Real Estate Association* (Associação Imobiliária Internacional do Bitcoin; http://www.ibtcrea.org/conference/) promove a ideia de modernização dos **negócios imobiliários**, incluindo o processo de escrituração, registro de imóveis e até mesmo as cauções. Do mesmo modo, o **Factom** (https://www.factom.com/), pretende criar um grande **notário para registos imobiliários**, tendo desenvolvido acordos com Estados norte-americanos e países centro-americanos, bem como parcerias com investidores asiáticos.

Gana está implementando um sistema que usa a *Blockchain* para reconhecer a posse e propriedade de 28 comunidades; objetiva com isso acabar com toda a problemática da **legalização da terra**, envolvendo escrituras, "grileiros" e outras fraudes.

- http://www.portaldori.com.br/2016/09/29/a-tecnologia-blockchain-aplicada-ao-registro-imobiliario/;
- http://www.slideshare.net/IribImprensa/a-tecnologia-blockchain-aplicada-ao-registro-imobilirio.

O governo de **Singapura** tem projetos de usar a *Blockchain* para evitar fraudes em seu **sistema financeiro**, principalmente em relação a traders.

- http://www.fcasingapore.com/index.php?action=displayEvent&eventID=362;
- http://nextbillion.net/news/singapore-government-joins-ibm-to-create-blockchain-innovation-center/;
- http://bravenewcoin.com/news/hitachi-and-bank-of-tokyo-mitsubishi-start-testing-blockchain-technology-for-electronic-check-processing-in-singapore/.

O **OriginalMy** (https://originalmy.com/) é uma espécie de **cartório digital** que arquiva online, de maneira privativa, segura, confidencial e inviolável, um registro único e exclusivo que garante a existência e a autenticidade de quaisquer documentos; inclusive assinando e validando contratos, comprovando sua integridade através de um certificado digital criptográfico que pode ser utilizado como prova legal.

O governo da **Estônia** estabeleceu um programa de **e-residência** no qual qualquer pessoa do mundo pode se candidatar e se tornar um e-residente

(residente virtual) da Estônia. Como tal recebe um cartão ID digital (Identificação digital) dotado de uma chave criptográfica para assegurar assinaturas digitais de documentos (eliminando a necessidade de assinaturas físicas em papel). Um e-residente, também, pode abrir contas em bancos usando um serviço de *e-banking system* (sistema bancário on line). Desse modo, através da *Blockchain* a Estônia está aumentando a quantidade de residentes virtuais no país e, com isso, faturando novos fluxos de receita. A Nasdaq está usando a tecnologia *Blockchain* para permitir que os residentes internacionais da Estónia votem nas assembleias de acionistas, mesmo quando estão no exterior.

- https://e-estonia.com/e-residents/about/;
- https://en.wikipedia.org/wiki/E-residency_of_Estonia;
- http://www.estoniancompanyregistration.com/estonian-e-residency;
- https://www.eesti.ee/eng/topics/citizen/kodakondsus/eesti_kodakondsus/e_residency.

O **Bitnation** (https://bitnation.co/ e https://blog.bitnation.co/) visa a criação de uma nação digital, com registro de identidade e serviços geralmente governamentais baseados na confiança e segurança que a *Blockchain* transmite. A ideia está ligada ao conceito de "Citizen Chain"; ou seja, cidadãos da *Blockchain*. Este conceito é expresso no **artigo de Shermin Voshmgir** (https://medium.com/blockchain-hub/citizen-chain-1c219d9a06e5#.lm2j47qyz). É um conceito ligado a escolha de cidadania.

Uport (https://uport.me/) é um **cartão de identidade**, descentralizado, baseado na tecnologia *Blockchain*.

Através do projeto piloto ***Blockchain ID*** (http://blog.onename.com/blockchain-id/) do **Bitnation** (um grupo de promoção da governação descentralizada), Janina Lowisz, a "Menina *Blockchain*", seria a primeira cidadã do mundo na *Blockchain*.

A liberdade de ser um cidadão de determinado povo, ideal, cultura ou credo. Shermin Voshmgir, em seu artigo, dá o exemplo do e-Estonia. Se estamos falando em nações digitais e empresas digitais usando a *Blockchain*,

não podemos deixar de falar no conceito de *criptoequity* (equivalência criptográfica), que é o mercado de ações e títulos de empresas digitais. O próprio conceito de DAO (*Descentraliza Autonomous Organizated*) pode prever a emissão de ações de uma empresa digital; que é bem fácil emitir através de um *smart contract* (contrato inteligente). No contrato inteligente ambas as partes se reúnem e acordam o que quiserem e quem faz o controle do contrato é a própria *Blockchain*.

- http://convergecom.com.br/tiinside/16/09/2016/ibm-e-banco-japones-vao-usar-blockchain-para-gestao-de-contratos-entre-as-duas-empresas/.

A expressão **"smart contracts"** foi cunhada por Nick Szabo a partir do artigo "Formalizing and Securing Relationships on Public Networks" (disponível em http://journals.uic.edu/ojs/index.php/fm/article/view/548/469). A linguagem **Solidity** representa um novo paradigma na computação descentralizada. Em termos muitos básicos a Solidity é a junção de uma linguagem de alto nível, similar a JavaScript, com um token que serve como meio de pagamento, aos membros da rede de computadores peer-to-peer, e proporcional ao tamanho das instruções (objetos, scripts reunidos em *smart contracts*) que são gravadas e depois são executadas automaticamente, sem possibilidade de intervenção humana. As instruções dos contratos inteligentes são assim consideradas como auto-reguladas (*self-enforceable*) no momento em que são inseridas na *Blockchain*.

BitShares (https://bitshares.org/) é uma plataforma livre contraparte-confiança para os contratos inteligentes financeiros que opera através da Internet e oferece um conjunto de instrumentos financeiros, que inclui CFDs (*contracts for difference* ou contratos por diferença). Esses contratos são instrumentos derivativos. Ferramentas digitais de instrumentos financeiros, tais como ativos de mercados atrelado (MPA) ou "SmartCoins" que representam um derivado com moeda fiduciária, ouro ou, até mesmo, outras moedas digitais como ativo subjacente estão atualmente disponíveis na BitShares.

- http://docs.bitshares.eu/_downloads/bitshares-financial-platform.pdf.

Os *Smart Contracts*, via *Blockchain*, também podem ser usados em legalização e escritura de terras. E mais útil ainda, um *smart contract* (contrato inteligente), devidamente bem elaborado por advogados em conjunto com programadores, constitui a resolução pacífica, privada e ágil das controvérsias (método consensual de solução de conflitos); ou seja, dispensa o moroso, custodioso, burocrático, tendencioso, corrupto e ineficaz Poder Judiciário. Por outras palavras, por consistirem em códigos de computador, são autoexecutáveis. Diante disso, o código é lei ("Code is law"). Em síntese, é um sistema que não depende de confiança entre as partes, pois é confiável em si mesmo (*trustless trust*). Essas regras (ou cláusulas) serão gerenciadas e executadas exclusivamente pela tecnologia, e não por pessoas, que são passíveis de corrupção ou dolo.

Em Direito é sabido que o contrato, acordo ou convenção faz lei entre as partes (*pacta sunt servanda*); ou seja, deve ser cumprido. Se as partes, previamente, já estabeleceram o que deve ocorrer na ocorrência de determinadas situações, eventos ou atos, em regra, não há necessidade e nem possibilidade de intervenção judicial. Por exceção a pessoa descontente pode alegar, por exemplos, vício do consentimento, erro substancial, falso motivo determinante, coação, estado de perigo, dolo, dano ou lesão, ser impossível ou indeterminável o seu objeto, inobservância de forma ou solenidade prescrita em lei, não cumprimento da contraprestação, não ocorrência do evento ensejador da obrigação, ocorrência de fato posterior relevante e imprevisível, má fé, violação à tradição e aos bons costumes, infringir a ordem pública, fraude, crime, ilicitude, ilegalidade, inconstitucionalidade, irregularidade, abuso, desvantagem ou cobrança excessiva, enriquecimento sem causa ou alguma nulidade para invalidar, anular ou revisar o contratado.

- Código Civil - http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

Ainda mais, o CPC - Código de Processo Civil (Lei nº 13.105/2015 - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm), no artigo 2º, § 1º, diz que: "É permitida a arbitragem, na forma da lei"; já no § 3º do mesmo artigo, prescreve que: "A conciliação, a mediação e outros métodos de solução consensual de conflitos deverão ser estimulados por

juízes, advogados, defensores públicos e membros do Ministério Público, inclusive no curso do processo judicial". Em reforço, no § 6º do artigo 337, reza que: "A ausência de alegação da existência de convenção de arbitragem, na forma prevista neste Capítulo, implica aceitação da jurisdição estatal e renúncia ao juízo arbitral". Por fim, no artigo 485, inciso VII, determina que o juiz não resolverá o mérito (o processo será extinto sem a análise da questão apresentada) quando acolher a alegação de existência de convenção de arbitragem ou quando o juízo arbitral reconhecer sua competência. Na Lei da arbitragem (Lei nº 9.307/1996 - http://www.planalto.gov.br/ccivil_03/leis/L9307.htm), artigo 13, consta que: "Pode ser árbitro qualquer pessoa capaz e que tenha a confiança das partes"; já no § 3º, diz que: "As partes poderão, de comum acordo, estabelecer o processo de escolha dos árbitros, ou adotar as regras de um órgão arbitral institucional ou entidade especializada". No artigo 18, determina o CPC que: "O árbitro é juiz de fato e de direito, e a sentença que proferir não fica sujeita a recurso ou a homologação pelo Poder Judiciário".

Algumas questões legais a serem consideradas são a forma prescrita ou não proibida em lei; objeto lícito, possível, determinado ou determinável; a capacidade de contratar (idade da pessoa e sua sanidade mental); a supremacia do interesse público ou coletivo; a liberdade contrataual; a autonomia de vontade da parte; a compreensão do teor e das implicações do contrato; o equilíbrio contratual; o foro de eleição (local competente para discutir o teor ou exigir o cumprimento via judicial); a possibilidade de execução (cumprimento) forçada; a duração do contrato; a renovação do contrato; a possibilidade de revisão do contrato; a transferência da titularidade no contrato (venda da posição ou herança); as assinaturas de testemunhas identificadas; o que a legislação equipara como assinatura; a publicidade e transparência do contrato; etc.

É aconselhável a promulgação de uma lei prevendo expressamente essas possibilidades para evitar que sejam levadas ao Poder Judiciário as demandas envolvendo os *Smart Contracts* por qualquer motivo.

Bitshares (https://bitshares.org/) é uma rede *blockchain* programável **dedicada a contratos inteligentes** para manipulação de ativos digitais.

A empresa anteriormente denominada Eris Industries (https://monax.io/docs/documentation/?redirect_from_eris=true) passou a ser chamada de **Monax** (https://monax.io/). Com a plataforma do Monax diferentes tecnologias podem ser integradas para criar aplicativos modulares que atendem às altas exigências de aplicações de um ecossistema de nível empresarial. Os engenheiros jurídicos da Monax constroem uma **biblioteca de contratos inteligentes** para reduzir o tempo dos clientes e, ao mesmo tempo, aumentar a segurança jurídica através de um ecossistema de participantes.

Loyyal (http://loyyal.com/) é uma **plataforma universal** construída com tecnologia contrato inteligente da *Blockchain*.

O **Open Bazaar** (https://openbazaar.org/) utiliza bitcoins na área de mercados online descentralizados. O seu objetivo é suplantar as falhas do polêmico mercado Silk Road. Não arquiva nem executa contratos inteligentes na *blockchain* do bitcoin.

A **Storj** (https://storj.io/) é um sistema de **armazenagem na *cloud* (nuvem)**, descentralizado, compartilhando o espaço disponível de cada utilizador, similar ao Bittorrent, mas com um token que permite desenvolver um modelo de recompensa.

A **Borderless.tech** (http://www.borderless.tech/) é uma aliança de serviços de governança acessíveis mundialmente e formada por contratos inteligentes que ficam na *Blockchain* do Expanse (http://www.expanse.tech).

A *Allianz Global Corporate & Specialty* (AGCS), resseguradora do Grupo Allianz, através de seu centro de competência *Allianz Risk Transfer* (ART) e em parceria com a *Nephila Capital Limited* anunciou que teve êxito na utilização da tecnologia *Blockchain* de **contratos inteligentes para realizar transações de *swap* em catástrofes naturais**.

- http://searchcompliance.techtarget.com/definition/smart-contract;
- https://smartcontract.com/;
- https://www.ethereum.org/greeter;

- http://www.blockchaintechnologies.com/blockchain-smart-contracts;
- http://computerworld.com.br/bitcoins-blockchain-e-chegada-dos-contratos-inteligentes;
- https://www.bitcoinnews.com.br/bitcoinbrasil/somente-os-contratos-inteligentes-podem-salvar-o-brasil/;
- https://guiadobitcoin.com.br/cresce-o-uso-da-blockchain-e-dos-contratos-inteligentes-do-ethereum-na-america-do-sul/;
- http://www.criptomoedasfacil.com/2016/07/expanse-lanca-contratos-inteligentes-baseado-em-plataforma-governanca-descentralizada-blockchain.html.

A plataforma **Ethereum**, por exemplo, possibilita a criação de Organizações Autônomas Descentralizadas (DAOs - *Decentralized Autonomous Applications*), que permitem a criação de uma sociedade completa, com atribuição de poderes sobre funções diversas, divisão de cotas societárias e mecanismos de interação com terceiros.

Ethereum (https://www.ethereum.org/) é uma plataforma digital cuja missão principal é a implementação de **Dapps** - *Descentralized Apps* (aplicações descentralizadas) e de *smart contracts* (contratos inteligentes). Dapps são, portanto, programas de computador que removem a necessidade de intermediários em basicamente qualquer serviço centralizado existente ao permitirem que qualquer pessoa confie em uma contraparte desconhecida para realizar os mais variados tipos de negócios e acordos de forma 100% digital. De modo semelhante, existem as **DAOs** (*Descentralized Autonomous Organizations*); que são organizações autônomas descentralizadas. Para mais informações sobre DAPPS, acesse: http://dapps.ethercasts.com/.

VEX - Venture Equity Exchange (https://dappslist.com/dapp/vex/) é um projeto que pretende disponibilizar, na *blockchain* da Ethereum, um pacote completo de soluções de gestão e finanças para empreendedores, para capitais de risco e *business* (negócios), de forma a automatizar todas as operações relacionadas com investimentos em empresas *startups*.

Costuma-se chamar de **Name Coin** (https://namecoin.org/) o sistema que usa a *Blockchain* para identificar endereços de sites. Uma espécie de DNS

descentralizado. A NameCoin (NMC) foi a primeira criptomoeda com a função de dar endereço ".bit" aos sites (exemplo, www.blogdowendel.bit); mas não deu muito certo, porque poucas pessoas aderiram; a indexação pelo Google, Yahoo e Bing era meio difícil; e, ainda, ficou pouco prático porque para acessar um site ".bit" era preciso uma extensão do Firefox ou do Chrome. Entretanto, há grupos de discussões querendo implementar DNS's descentralizados na *Blockchain* do Ethereum, com isso o TLD - *Top-Level Domain* (a última parte do domínio: ".com", ".net", ".com.br", etc.), deixa de ser controlado por uma autoridade central ou por um governo. Por causa dos problemas com uma autoridade central controladora do domínio dos sites é que surgiram redes como o Tor, I2P e Freenet para dar mais privacidade e liberdade aos usuários; ou seja, uma internet livre. O Ethereum Project tem discutido a implementação de "descentralized DNS" como ".eth", ".dao", entre outros.

O governo da **Geórgia** está desenvolvendo um projeto focado em **registros públicos**, inclusive de nascimento e identificação, baseados na *Blockchain*. O governo está querendo mostrar que o país é livre de corrupção, moderno e transparente. Isso sim que é transparência da coisa pública, e não aquela coisa "feita para inglês ver", que temos no Brasil (http://www.portaldatransparencia.gov.br/).

- http://www.altcointoday.com/georgia-blockchain-land-registry/;
- http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#449150d06550.

A **Suécia** está planejando levar à *Blockchain* **todas as transações** do estado envolvendo bancos, governo, agentes, compradores e vendedores (licitações) e trazendo acordos transparentes envolvendo a negociação. Isto traria negociações instantâneas com níveis de segurança e integridade bem altos para a sociedade sueca. Outro exemplo de transparência governamental.

- https://cartorios.org/2016/06/18/registro-de-imoveis-sueco-e-o-blockchain/;
- http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV;
- http://www.diariobitcoin.com/index.php/2016/06/18/suecia-pone-a-prueba-la-tecnologia-blockchain-en-el-registro-de-la-propiedad/;

- http://fin-tech.es/2016/07/suecia-blockchain-para-el-registro-de-la-propiedad.html.

O **Reino Unido (Inglaterra)** está cogitando usar a *Blockchain* para monitoramento e controle de subsídios para evitar fraudes e abusos.

- https://jornalbitcoin.pt/index.php/noticias/item/566-reino-unido-estuda-blockchain-como-forma-de-proporcionar-transparencia-no-que-toca-a-utilizacao-do-dinheiro-dos-contribuintes;
- http://criptonoticias.com/aplicaciones/sistema-bienestar-reino-unido-utilizar-tecnologia-blockchain/#axzz4MoZItLzP;
- https://www.gov.uk/government/speeches/digital-transformation-in-government-and-blockchain-technology;
- https://www.gov.uk/government/news/government-explores-blockchain-technology-to-improve-public-services.

Dubai usará a tecnologia *Blockchain* **em todos os documentos públicos** (http://www.diariobitcoin.com/index.php/2016/10/05/dubai-usara-la-tecnologia-blockchain-para-todos-los-documentos-publicos/).

As instituições financeiras, na sua maioria, não estão interessadas no bitcoin, mas estão muito interessadas na *Blockchain*.

> "Ninguém poderia ser mais interessado em desenvolver novas tecnologias que poderiam evitar fraudes financeiras do que o banco suíço UBS. Em setembro de 2011, o tradicional banco suíço anunciou perdas de US$ 2 bilhões devido a operações não autorizadas realizadas pelo trader Kweku Adoboli na mesa de Synthetic Equity do escritório do banco em Londres. As perdas foram tão significativas que o CEO do banco na época pediu demissão. Passados 4 anos deste incidente, o banco suíço acaba de anunciar que vai abrir um laboratório em Londres para explorar maneiras de utilizar a tecnologia do blockchain em transações financeiras. O laboratório irá tentar desenvolver novas tecnologias para lidar com questões da indústria financeira em geral, como a necessidade de gerenciar e analisar grandes quantidades de dados, ou como melhorar a análise de risco. Exatamente o que poderia ter protegido o banco e seus acionistas em 2011. Como as operações

feitas por Adoboli possuíam contrapartidas (*hedges*) falsos que ele mesmo imputava e aprovava no sistema de *backoffice* do banco, um sistema de liquidação por consenso na linha do blockchain e aberto a outros bancos participantes poderia ter detectado os trades fraudulentos. É claro que isso não é algo trivial e deve ser justamente por isso que o UBS está sendo um dos pioneiros entre os grandes bancos de investimento a experimentar com o blockchain. Além do UBS, vários outros bancos já sofreram enormes prejuízos com esse tipo de trades fictícios. Na lista estão Société Générale, o extinto Barings e outros. Acreditamos que outros bancos devem seguir os passos do UBS em procuras de soluções usando algo similar ao blockchain." (http://www.brbitcoin.com.br/ninguem-melhor-do-que-o-ubs-para-reconhecer-o-poder-do-blockchain/).

A Bolsa norte-americana **Nasdaq** realiza testes em seu ambiente e o **Goldman Sachs** investiu recentemente numa *startup* de Bitcoin chamada **Circle** (https://www.circle.com/pt), que promete tornar o envio de dinheiro de uma pessoa para outra algo tão simples quanto uma mensagem de texto. O BNY Mellon criou os **BKcoins** (http://www.bkcoin.com/) e o Citi criou os **Citicoins** (http://finnovation.com.br/citicoin/). Já a Ripple criou o seu próprio protocolo de *cross border transfers* (transferência de recursos entre países), que vem sendo usada por diversos bancos com sucesso.

Em uma matéria publicada no *International Business Times*, intitulada "Codename Citicoin: Banking giant built three internal blockchains to test Bitcoin technology" relata que o Citigroup já criou algumas *blockchains* para começar a testar a tecnologia Bitcoin.

- http://www.ibtimes.co.uk/codename-citicoin-banking-giant-built-three-internal-blockchains-test-bitcoin-technology-1508759.

O banco **J. P. Morgan Chase** está construindo uma *blockchain* pública para garantir transações confidenciais (http://www.wsj.com/articles/j-p-morgan-has-a-new-twist-on-blockchain-1475537138). Já o banco **Barclays** efetuou uma transação comercial de exportação utilizando uma tecnologia de *Blockchain* da **Wave** (https://www.waveapps.com/), uma *startup* israelense (http://www.voit.com.br/startup-israelense-e-barclays-fazem-exportacao-usando-blockchain/).

O Banco **Santander**, décimo maior banco do mundo, encontrou mais de 25 possíveis usos da *Blockchain* que poderiam ser aplicados aos sistemas bancários tradicionais e, ainda, poderia eliminar até 20 bilhões de dólares de custos bancários. O Santander, ainda, está trabalhando em um projeto que pesquisa como poderia digitalizar o dinheiro do cliente usando a *Blockchain* pública do Ethereum.

- http://www.santander.com/csgs/StaticBS?blobcol=urldata&blobheadername1=content-type&blobheadername2=Content-Disposition&blobheadername3=appID&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3Bfilename%3D256%5C466%5CSantanderbecomes.pdf&blobheadervalue3=santander.wc.CFWCSancomQP01&blobkey=id&blobtable=MungoBlobs&blobwhere=1278728059727&ssbinary=true;

- https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf;

- http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf;

- https://foxbit.com.br/blog/santander-publica-relatorio-sobre-bitcoin/.

O **BBVA** - Banco Bilbao Vizcaya Argentaria SA, contribuiu em 75 milhões de dólares em uma rodada de investimentos para a Coinbase; já o Goldman Sachs investiu 50 milhões de dólares em uma rodada de financiamento para Circle Inc.

- http://www.centrodeinnovacionbbva.com/ebook/ebook-tecnologia-blockchain.

O **Barclays** lançou uma aceleradora de startups chamada *Barclays Accelerator*, que é dedicado a tecnologias financeiras e startup relacionadas à tecnologia *Blockchain*.

O **Westpac** e o ***Commonwealth Bank of Australia*** se associaram à Ripple Labs para incorporar a tecnologia *Blockchain* em seus sistemas. Enquanto Westpac foi integrado ao protocolo Ripple para rastrear as transações e operações, o *Commonwealth Bank of Australia* está tentando implementar o protocolo para liquidar pagamentos internacionais rapidamente.

No Brasil, o banco **Bradesco** agendou para o final de 2016, em São Paulo, um teste de uso da *Blockchain* (carteira digital da eWally, transferência de dinheiro por meio de remessas internacionais pela BitOne e/ou Ripple Labs, etc.). **Os bancos Bradesco e Itaú integram o consórcio R3CEV** (https://r3cev.com/), que reúne mais de 50 bancos de todo o mundo para estudar e criar padrões para o uso do sistema.

Para entender melhor, ou se profundar, sobre o que são as bitcoins e como elas são feitas, confira os capítulos: "*HASH*", "CERTIFICADOS DIGITAIS", "*PEER-TO-PEER* (P2P)", "BITCOIN", "COMO A BITCOIN É FEITA?" e "COMO MINERAR BITCOINS E ALTCOINS".

VALOR DA BITCOIN E DAS ALTCOINS

A concepção de uma moeda criptográfica sem qualquer tipo de interferência governamental em sua circulação situa-se no contexto de uma economia do conhecimento como descrita por Ladeur (http://www.e-law.net.br/Governanca). Nessa concepção, as pessoas assumem riscos que nem sempre podem ser previstos antecipadamente; mas, ao assim procederem, criam direitos exclusivos que independem de fatos passados inseridos na tradição social e que não são, necessariamente, extensivos aos membros do grupo social não participantes do empreendimento.

Como a moeda virtual não possui lastro e não está vinculada à nenhuma âncora, sendo fiduciária, nada garante o seu valor. Assim, a Bitcoin fica permanentemente à deriva (na dependência da aceitação popular) e não há como saber com precisão qual será a sua variação. Desse modo, as moedas virtuais não são indicadas para quem desejar fazer altos investimentos, mas não está disposto a correr riscos.

As maiores críticas à bitcoin consistem no fato de que ela não é garantida por absolutamente ninguém ou nada, não possui lastro e não tem valor intrínseco enquanto que as moedas tradicionais são sustentadas pelos governos e respectivos bancos centrais.

Entretanto, nenhuma das moedas tradicionais é segura, pois não possuem lastro (não existe nada com valor em si mesmo que lhes sustentem), sendo puramente fiduciárias e, em razão disso, são instáveis e, portanto, sujeitas à oscilações e desvalorizações. Por outras palavras, pelo fato das moedas governamentais não possuírem mais lastro, seus valores estão sujeitos aos caprichos dos políticos e burocratas das políticas monetárias dos respectivos países. As únicas coisas próximas do antigo lastro seriam a balança comercial e os certificados públicos (outro tipo de moeda ou de ativo fiduciário), mas tais coisas dependem puramente do mercado (periódica e constante aceitação popular).

A topologia P2P da rede Bitcoin, e a ausência de uma entidade administradora central torna inviável que qualquer autoridade,

governamental ou não, manipule o valor de bitcoins ou induza inflação "imprimindo" mais notas.

O problema é que para gerar esta moeda sem lastro (não se baseia em algo como ouro ou o Banco Central), que determina seu valor apenas pela especulação em Bolsas de Valores virtuais, é necessário tempo e, ironicamente, dinheiro real. Assim, a moeda flutua nas leis da oferta e demanda/procura.

A quantidade de bitcoins a ser criada é fixa. No início, o autor de cada bloco recebia 50 bitcoins pelo seu trabalho. Depois de uma certa quantidade de blocos pré-definidos, a recompensa caiu pela metade (*bitcoin halving*): hoje o criador dos blocos pode incluir para si apenas uma transação gerando 25 bitcoins. Se algum minerador hoje publicar um bloco criando 50 bitcoins, ao invés de 25, o bloco será rejeitado sumariamente pelos outros usuários. E daqui a alguns anos, a recompensa vai cair para 12.5 bitcoins por bloco, e assim por diante (sendo reduzida pela metade), até que em algumas décadas, todos os 21 milhões de bitcoins estarão geradas e, assim, mais nenhuma unidade de bitcoin será criada.

Estima-se que a produção da moeda irá somente até 2030 (data prevista para atingir 21 milhões de unidades de bitcoins). Depois disso, não haverá mais criptografia para ser quebrada e restará apenas negociações com moedas já "descobertas" (mineradas).

Alguns pontos confirmam uma possível ruína do Bitcoin: a escassez da moeda e o desafio de minerá-la. O que acontecerá quando encerrar a produção de Bitcoin ao atingir o limite de 21 milhões de unidades?

A oferta monetária de bitcoins é finita e fixa em 21 milhões. Não é possível emitir mais bitcoins além deste limite, o que torna muito pouco atrativa, para qualquer economia, a adoção de bitcoins como moeda. O mundo adotou moedas fiduciárias em 1971, quando os acordos de Bretton Woods e o que sobrou do padrão-ouro deram seus últimos suspiros. A adoção de bitcoins pelos Estados modernos implicaria deflação e desencorajaria a atividade econômica, favorecendo a acumulação. Evidentemente, é possível criar uma estrutura de criptomoeda diferente

(Novacoin, por exemplo prevê uma inflação dinâmica através do aumento da oferta monetária). O problema que emerge é qual seria a autoridade monetária, em um sistema distribuído e internacional, responsável por esta decisão.

No Bitcoin não é possível uma emissão extra surpresa, pois é o algoritmo que regula o ritmo de produção de bitcoin, que é previsível e conhecido por todos. O software Bitcoin de referência é de código aberto e pode ser inspecionado por qualquer um. Qualquer um também pode alterar o código do aplicativo Bitcoin de referência. Também é possível ou propor melhorias ao protocolo, que depois de aprovadas pelos desenvolvedores mais ativos são ultimamente votadas pelos mineradores através do próprio protocolo Bitcoin. O voto da maioria dos mineradores é que decide qual mudança pode entrar no protocolo ou não.

Para uma moeda ganhar poder de comprar (apreciar-se), não basta uma política monetária relativamente mais rígida se sua demanda despencar. Da mesma forma, uma política monetária frouxa e expansionista não necessariamente irá causar a depreciação do dólar, por exemplo, se a demanda pela moeda norte-americana seguir aumentando.

Pensar que a bitcoin não tem valor porque foi artificialmente criada e porque não tem lastro, é o mesmo que acreditar que o dólar ou o euro também não possuem valor.

O que dá valor ao dinheiro convencional não é o papel ou metal em sim dos quais são feitos, nem as meras inscrições de valores em seus corpos, mas os bancos centrais e, principalmente, o mercado. Desse modo, de nada adianta um banco central querer impor um determinado poder aquisitivo para um pedaço de papel (cédula) se o mercado discorda dessa valoração.

Para algo ser classificado como dinheiro, precisa reter valor ao longo do tempo (possibilitar o acúmulo de riqueza para posterior uso), ser um padrão (referência generalizada) de medida (preço) para o valor relativo das coisas e ser usado para comprar e vender produtos e serviços. Os dois últimos requisitos, portanto, envolvem a aceitação e uso pelas pessoas em geral.

O que aconteceria se, de repente, o mundo passasse a rejeitar o dólar americano como forma de pagamento? Será que o valor do dólar iria permanecer? Claro que não! A cotação do dólar iria despencar! Mas como muitos países, empresas, instituições e pessoas possuem créditos a receber em dólares americanos, não lhes seria nada benéfica a queda da cotação do dólar. Diante dessa situação hipotética, a melhor forma de manter uma estabilidade de preço em contratos em moeda estrangeira, é enumerar as de maiores valores e aceitação, elegendo-se a média, a de maior ou de menor cotação na data do pagamento. Do mesmo modo, em relação a ativos ou comódites, há de se enumerar determinadas bolsas ou *exchanges*, definindo-se o critério do preço na data do pagamento; e, inclusive, em caso de supervalorização ou desvalorização muito grande, utilizar outro bem semelhante ou similar como referência de preço. Igual procedimento deve ser adotado em relação à definição de índice econômico, de inflação ou de correção monetária.

Outro detalhe, a inflação corrói o poder de compra da moeda nacional ou oficial em comparação com moedas estáveis e faz com que as pessoas (físicas e jurídicas) busquem por alternativas de reserva de valor para preservar a riqueza. E, no longo prazo, aquelas moedas que forem relativamente mais inflacionadas que as demais acabarão se desvalorizando inevitavelmente.

Por outras palavras, faz muito tempo que o dinheiro não é algo que possui um valor em si mesmo ou em algo que lhe dá utilidade.

A prova de que os lastros de moeda também são vulneráveis, está no ocorrido com os investimentos feitos na Fazenda Boi Gordo e na Avestruz Master (vide o capítulo sobre pirâmides financeiras). Explica-se. Trataram-se de situações onde os investidores recebiam certificados (pedaços de papel) garantindo-lhes as propriedades dos animais citados, sem nunca os terem visto e, muito menos, terem tido sequer a posse indireta. Enfim, no mundo atual, toda moeda, ativo e título de crédito (cheque, nota promissória, etc.) não passa de promessa e, como tal, pode não ser verdadeira e, muito menos, honrada.

Que valor tem um cheque sem fundos de alguém que não possui nenhum patrimônio, receita ou crédito em seu nome?

Por outras palavras, conforme ocorrido no governo norte americano, o próprio lastro era um juramento (uma promessa) de que as cédulas possuíam o equivalente em ouro e, ainda, que elas seriam prontamente trocadas por ouro a todos que assim pedissem. Só que tudo isso era mentira.

Mesmo o ouro, por exemplo, a partir do momento em que passa a ser negociada a sua propriedade de forma digital, ele não depende mais da propriedade intrínseca do metal precioso, mas sim na confiança do sistema digital em questão.

Em regra, salvo exceções, tudo que é escasso, até que se prove o contrário, possui considerável valor.

O fator determinante do valor do ouro é, sem dúvida, a sua escassez; apesar de que ele não é tão raro a ponto de ninguém conseguir obtê-lo.

Independentemente de ser meio de pagamento, o ouro tem valor como mercadoria (valor intrínseco ou utilidade própria); vez que, por ser maleável, pode ser manipulado e transformado em vários objetos (joias, baixelas, castiçais, folheamentos, obras de arte, contatos em circuitos integrados, etc.). Soma-se a isso o fato de ser lustroso, brilhante, antiferrugem e durável, com o que possui grande aceitação e preferência, conferindo-lhe longevidade para poder ser utilizado como acúmulo de riqueza. Antes de o ouro se tornar um meio comum de troca (dinheiro), as pessoas o valorizavam por causa de seu valor intrínseco. Portanto, mesmo que, por ventura, o ouro seja abandonado como moeda, valor monetário, reserva de valor ou ativo financeiro, ainda assim continuará tendo valor em razão de suas qualidades e de seus usos alternativos (utilidade); tal como, por exemplo, uso ornamental. Inobstante isso, o ouro tem grande valor porque é dinheiro e as pessoas, ao longo do tempo, lhe agregaram valor e não porque possui múltiplas utilidades ou só porque é escasso; vez que existem várias coisas que são escassas ou que possuem múltiplas utilidades, e até são indispensáveis, mas que não possuem grande ou qualquer valor. Desse modo, o que valoriza muito algo é o fato das pessoas acharem tal

coisa útil e dela ser escassa. O valor do ouro não vem da utilidade, pois a água, por exemplo, é muito mais útil do que ouro e, inclusive, essencial, mas vale bem menos do que o ouro; exceto se a pessoa estiver morrendo de sede no deserto, aí a água valerá bem mais que o ouro. Portanto, qualquer bem, item ou coisa somente possui valor porque as pessoas decidiram que tem valor e, assim, continuam dando valor. Em síntese, todo valor é convenção social, com o que o valor é algo subjetivo coletivo. Em conclusão, qualquer sociedade ou comunidade, dadas suas características físicas e raridade, o ouro foi e é valorizado. Por esse motivo é que a origem das cédulas envolveu uma promessa do equivalente em ouro. Ressalta-se, assim, que pelo fato do ouro ter sido uma mercadoria de valor antes de ser moeda, acabou sendo o lastro das cédulas (dinheiro).

O programador do algoritmo do Bitcoin deu seu máximo tentando copiar o ouro. Exatamente como o metal, cuja presença na superfície terrestre é vista por muitos como limitada, a bitcoin também e limitada artificialmente (através da programação de seu algoritmo), ao teto de 21 milhões de unidades. Satoshi Nakamoto (pseudônimo do criador do Bitcoin), portanto, pegou as propriedades que fazem o ouro ter valor e as programou na forma da bitcoin, fazendo a moeda digital mais eficiente e fácil de usar que o ouro. Por esse motivo, a bitcoin é vista como uma espécie de ouro digital: ela é escassa; ou seja, apenas uma quantidade limitada de bitcoins vai existir. O que é completamente diferente das moedas dos governos que são emitidas a bel-prazer dos governantes.

Todo bem tem seu valor, seja o bem material, imaterial, livre, econômico, não econômico, de consumo, de produção, de reprodução, de capital, complementar, passivo ou ativo. E o valor é a percepção dos benefícios, vantagens, utilidades ou proveito de um bem; sendo econômico se divide em valor de uso e valor de troca.

O valor de uso enfatiza as propriedades intrínsecas do próprio bem com enfoque do indivíduo, o que o subjetiva. Já o valor de troca possui enfoque social, o que lhe confere uma projeção objetiva.

A teoria subjetiva do valor é uma doutrina de valor que propaga a ideia de que o valor de um bem não está em si mesmo e não é determinado por

qualquer qualidade, característica, atributo ou propriedade inerente do bem, nem pela quantidade de trabalho necessária para produzi-lo ou os produtos agregados; mas sim pela sua importância pessoal (individual) para a realização de fins desejados, ou seja, está na mente de quem quer adquiri-lo. Em última análise os produtos só têm valor porque as pessoas os desejam. Logo, quanto mais as pessoas quererem os produtos, maior será o valor dos mesmos.

Portanto, o valor subjetivo significa que não se pode arbitrariamente (ou por decreto) impor ou numerar, cardinal ou nominalmente, o valor de algo. O valor intrínseco, por outro lado, significa que o objeto possui utilidade; ou seja, que não serve somente como moeda (meio de troca ou de pagamento).

A tese marxista é a de que o valor é determinado pelo trabalho; o que é refutada por esse artigo: http://www.mises.org.br/Article.aspx?id=1386.

Antigamente se pensava que existia alguma entidade mística escondida no bem e desse entendimento surgiram as teses do valor intrínseco, do custo de produção e da quantidade de trabalho necessária. Entretanto, o valor do bem não surge de dentro para fora, mas surge de fora (pelos humanos) e para fora (para os humanos). Além de o valor ser subjetivo, a medida para se determinar o valor também é de natureza totalmente subjetiva também. Em resumo, quem define o preço é quem deseja o bem; ou seja, é definido por quanto o consumidor está disposto a pagar pelo bem ou o quanto o bem vale para ele. Em outras palavras, o valor é subjetivo, não intrínseco. Desse modo, em refutação à teoria marxista do valor trabalho, diz-se que nada tem valor intrínseco e que todo valor é subjetivo. Mas tal afirmação somente se aplica neste contexto específico. Explica-se, quando a mercadoria leva em si um caráter fetichista geral (valor social, imagem, *status*, fama, prestígio, etc.), ela tem valor de troca intrínseco.

A utilidade constitui o valor de uso, a serventia prática que o bem possui, vinculando-se como tal às propriedades físicas ou intrínsecas do objeto, com o que se diz objetivo. O valor de uso está relacionado ao próprio bem, estando, portanto, imanente ligado ao bem em questão. Entretanto, o valor de uso, envolve a pessoa que o utilizará, logo também pode ter peso subjetivo e pessoal. Uma obra de arte não possui verdadeiramente valor de troca, pelo

que o seu preço deverá ser explicado por considerações inteiramente diferentes das que permitem explicar o preço de um utensílio qualquer.

Para os neoclássicos a utilidade é subjetiva, enquanto para os clássicos (Marx, Smith, etc.) a noção de útil é objetiva.

Valor de troca, no sentido de relação de preço, é valor objetivo. O valor de troca (objetivo) de uma mercadoria é simplesmente o montante pelo qual será trocada por outras mercadorias. Os valores de troca refletem mais o que as mercadorias têm em comum entre si, do que suas qualidades específicas. O valor de troca é o que permite comparar diferentes valores de uso numa relação de troca. Portanto, em regra, o valor de troca é objetivo (tantas quantidades disso por tantas quantidades daquilo); mas, também, pode ter valoração subjetiva (beleza, satisfação pessoal, valor sentimental, necessidade específica do indivíduo, etc.). Desse modo, o valor de troca subjetivo é determinado pela utilidade marginal que depende das coisas obtidas em troca do bem. Portanto, depende do preço, do valor de troca objetivo dos bens. Valor, em Menger, é valor subjetivo pessoal.

A valoração subjetiva é o que uma pessoa atribui ao bem por acreditar que ele pode saciar suas necessidades particulares, específicas ou exclusivas.

Quem possui algo sobrando que todas as outras pessoas demandam (querem, desejam, precisam, buscam, sentem falta, etc.), normalmente não vai guardar para si mesmo e nem consumir referido bem através do uso próprio (valor de uso); antes vai preferir utilizar esse bem valioso para adquirir outras coisas ou serviços outras coisas que lhe tragam utilidade (valor de troca).

Para Marx não existe bem ou valor sem o trabalho empregado. Entretanto, independentemente da quantidade de trabalho que tenha uma mercadoria, se ela não tiver utilidade para ninguém, seu valor será igual a zero. O ar tem utilidade, mas não tem trabalho. Um buraco cavado no jardim tem trabalho, mas não tem utilidade. Portanto, ar e um buraco inútil não são mercadorias.

A palavra necessidade deve ser frisada, pois ela remete à utilidade. Segundo a teoria marxista, tanto utilidade, quanto necessidade são frutos da chamada vida social, a não ser que você viva ilhado, sozinho, sem nenhum tipo de comunicação com o mundo. Imaginemos o personagem Robinson Crusoé sozinho na ilha isolada. Ele não tem nada na ilha para comprar ou vender, vez que está sozinho e tudo o que existe na ilha, ele tem acesso e uso gratuito. Diante disso, dinheiro, metais raros ou joias preciosas não lhe têm nenhum valor monetário ou de troca; tais coisas seriam simplesmente aproveitadas por ele (como material na confecção de uma cabana, por exemplo) como qualquer outro bem ou as guardaria para um, eventual e remoto, uso posterior. Assim, apesar de não terem valor de troca, onerosidade ou preço, possuem algum uso (valor intrínseco). O ar que respiramos, por exemplo, tem utilidade, mas nem por isso os indivíduos atribuem um valor econômico para ele. O valor (preço) dos bens depende de nossas necessidades, não sendo intrínseco a eles. Mas, quando Crusoé sai da ilha e volta à civilização, ele recorda que dinheiro, metais raros ou joias preciosas valem muito mais do que comida, água potável, fogo e armas de caça; os itens indispensáveis e escassos para sua sobrevivência na ilha deserta.

Considerando que o custo é definido pela oferta (disponibilidade, quantidade) e demanda (procura, necessidade) em um mercado, o valor é subjetivo. E, sendo subjetivo, obviamente não pode ser intrínseco. Portanto, se as pessoas acreditarem que tem valor ou darem valor, logo terá valor, porque o valor de tudo é criação da mente humana, portanto é algo subjetivo.

A ação é um método para se alcançar um desejo e que cada indivíduo terá seus desejos e métodos próprios. Portanto, o valor é subjetivo. Por outras palavras, o valor de troca, por envolver a interação entre os seres humanos visando o consenso na negociação e respectivo juízo de valor, é subjetivo. Por outras palavras, o valor não é intrínseco; ou seja, ele não está nas coisas em si mesmas. O valor está em nossas mentes e condutas; que é a forma na qual o homem reage às condições do seu ambiente. Não é o que um homem ou grupo de homens dizem sobre o valor que conta, mas como eles agem a respeito.

Tudo o que foi criado dentro dos computadores (softwares e serviços) ou na mente humana, não possuiriam valor e nem serviria como meio de troca, pois seriam desprovidos de valor intrínseco no mundo real, exterior ou físico. Um software editor ou processador de textos, por exemplo, possui muitas funções, entretanto, não existiriam características físicas que o permitiria ter um valor intrínseco fora do mundo virtual ou digital; aliás nem existiria. Como atribuir valor a algo imaterial e objetivo num mundo material (físico) e subjetivo? Algo virtual (sem existência física) e objetivo, no entanto, possui utilidade e valor.

A valoração do bitcoin como algoritmo, normalmente, só existe para quem é da área de informática (utilidade intrínseca), mas pode não fazer o mínimo sentido para as demais pessoas.

A opinião subjetiva, de um, alguns ou até vários indivíduos, de que o bitcoin é inútil, não afeta em nada o fato de que ele é útil para várias outras pessoas. Isso, combinado à escassez, faz com que ele tenha valor monetário.

Há de ser feita uma analogia da bitcoin com as cédulas (dinheiro de papel), que surgiram não como uma mercadoria em si mesmo, mas como um meio de pagamento; ou seja, um título de reivindicação sobre o dinheiro metálico lastreado nelas. As cédulas foram inicialmente utilizadas como sendo uma maneira mais conveniente de se transferir a propriedade do ouro ou da prata. Tão logo as cédulas passaram a ter ampla aceitação geral (credibilidade) como meio de troca, o ouro que as lastreava pode ser abandonado sem que isso afetasse o uso das cédulas como dinheiro; vez que, por convenção social, elas já haviam se tornado dinheiro por si mesmas.

Bitcoin ainda é uma unidade de armazenamento de dados, um registro dentro de um banco de dados. Comprar bitcoin é como comprar uma planilha do Excel que está armazenada num servidor on line (Dropbox, Google Drive, etc.) ou qualquer outro banco de dados acessível pela Internet. A diferença é que não existe provedor, pois o banco de dados é descentralizado (rede P2P).

Existem muitos fatores e elementos que dão valor à bitcoin. Estes podem sustentá-la perfeitamente ideológica, tecnológica e monetariamente.

Em síntese, a bitcoin é uma moeda totalmente digital (não materiais), online, privada (não emitida por nenhum ente público ou país), descentralizada (sem nenhum órgão regulador ou controlador), popular (não pertencente a nenhuma empresa ou organização privada), democrática (sujeitas à vontade da maioria) e internacional (aceita no mundo todo).

Bitcoin é uma moeda como o real, o dólar ou o euro, só que é virtual. Ela não é emitida por nenhum Banco Central, mas é fruto da iniciativa popular (privada coletiva). Ela não pertence a nenhum país, mas é global (universal, mundial). Ela não é emitida ou impressa, mas sim gerada por um software.

Bitcoin não tem nenhuma nação ou instituição internacional que a adote como moeda oficial. A bitcoin permanece, "com vento em popa", porque muitas pessoas veem nela o seu pleno potencial. Em outras palavras, são pessoas com diferentes utilizações dadas a Bitcoin no contexto de cada país, que dão um valor nos mercados mundiais. O que lhe dá valor, além do consenso de sua utilização e da lei da oferta e procura, é a sua utilidade (meio de pagamento; produtos e serviços que podem ser adquiridos) e o seu valor intrínseco (em si mesmo), consistente na sua tecnologia muito útil que ela proporciona: a *Blockchain*; uma rede segura e confiável, superior a qualquer outra rede de computadores do mundo e que pode dar à humanidade mais liberdade.

O valor da bitcoin não é definido por governos, políticos, burocratas, economistas ou baseado em qualquer elemento ou atividade humana. A rede Bitcoin é baseada na *Blockchain*; ou seja, não depende da confiança em pessoas. Ela funciona baseada inteiramente na lógica de inteligência artificial, criptografia e princípios matemáticos.

O *hash* é uma sequência aleatória de letras e números e seu grande valor está no fato de que é bastante fácil transformar qualquer tipo de informação (palavras, números, equações, detalhes de transações financeiras, etc.) em um *hash*; mas é praticamente impossível fazer o caminho inverso e transformar o *hash* nas informações originais. Outra propriedade característica dos *hashes* é que se mudar apenas um dos caracteres, ele se transformará em um hash completamente diferente. Ainda mais, o *hash*

subsequente é atrelado ao *hash* anterior e, assim, sucessivamente, fazendo que o *hash* de um bloco sempre esteja atrelado àquele imediatamente anterior. Portanto, cada bloco da *Blockchain* é um *hash* específico e impossível de ser fraudado.

O valor da bitcoin, em suma, está relacionado ao protocolo que permite a propriedade de uma unidade digital sem que para isso seja necessária uma autoridade central. Desse modo, a propriedade de uma unidade digital é garantida por uma fórmula matemática e uma rede de computadores descentralizada ao invés do modelo tradicional onde a propriedade de moeda é garantida pela confiança em um governo ou empresa, ambas sujeitas a fraudes, erros, dolos, corrupção e demais mazelas do ser humano.

Ainda mais, o fato de envolver uma rede aberta, segura, estável, confiável, semianônima, transparente, democrática (popular) e com capacidade de revolucionar os pagamentos on-line, também lhe agrega valor.

Em suma, não devemos esquecer que o valor da bitcoin é determinado pela confiança de seus usuários, bem como pela oferta e demanda nos mercados de câmbio.

O valor que existe na bitcoin é determinado pelo mercado de troca com outras moedas. E, como toda bolsa, é o mercado quem de fato determina este valor. E o valor da cotação (não o valor que cada indivíduo pensa) é subjetivo coletivo (e não individual).

A popularidade se traduz em um aumento no valor da Bitcoin como moeda.

> "É difícil dizer porque tem ela um valor, mas a razão será em primeiro lugar pelo facto de as pessoas estarem dispostas a comprá-la, porque acreditam que outras pessoas farão o mesmo. É uma espécie de ouro virtual: pode-se escavar Bitcoins, ou seja, criar novos Bitcoins, resolvendo problemas de matemática muito complexos, o que, no entanto, exige um alto desempenho de computação e um grande consumo de energia eléctrica para o funcionamento do computador. E, justamente porque estão disponíveis na Islândia electricidade barata e ar frio

suficiente para arrefecer o computador em sobreaquecimento, será aí o lugar ideal para a mineração de Bitcoins." (http://resistir.info/financas/moedas_digitais.html).

Portanto, um fator chave que determina o valor da Bitcoin é a sua popularidade. Quanto mais as pessoas usarem bitcoins como meio de pagamento, mais as empresas investirão na implementação do Bitcoin. E quanto mais as empresas aderirem e investirem na bitcoin, mais irá aumentar a confiança popular na bitcoin e mais empresas irão aderir e, assim, sucessivamente.

Confira-se alguns dos **locais onde aceitam Bitcoins**:

- https://localbitcoins.com/pt-br/;
- https://coinmap.org/;
- http://lista.mercadolivre.com.br/aceito-bitcoin;
- http://lojabitcoin.blogspot.com.br/;
- http://www.negociecoins.com.br/lojas-aceitam-bitcoins;
- http://spendbitcoins.com/;
- http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing;
- https://www.tecnisa.com.br/lp/bitcoin;
- https://guiadobitcoin.com.br/tag/paypal/;
- https://www.bitcoinmais.com/blog/lojas-que-aceitam-bitcoins/;
- http://www.hashbtcbrasil.com.br/2016/06/algumas-lojas-que-aceitam-bitcoins.html;
- https://www.bitcoin.com/spend-bitcoin-online;
- http://blogs.microsoft.com/firehose/2014/12/11/now-you-can-exchange-bitcoins-to-buy-apps-games-and-more-for-windows-windows-phone-and-xbox/#sm.00000zwxjbdh9hda3znlssqkgb9kh.

A aceitação popular da moeda tem que partir dos industriários, comerciantes, empresários e profissionais liberais, que costumam serem

mais instruídos, cultos e informados do que o restante da população, com o que ao aderirem a essa forma de pagamento, estarão não só divulgando a moeda, mas, também, despertando a curiosidade e o interesse das pessoas, que irão querer saber mais e, principalmente, se inteirarão de como adquirirem e usarem essa forma de pagamento. Não podemos ignorar a importância das celebridades, artistas, formadores de opinião, escolas, universidades, entidades de classe, sindicatos, associações, mídias sociais e Mídia/Imprensa no trabalho de divulgação e esclarecimento. Assim, por exemplo, se a Bitcoin começasse a ser aceita na *night* ou na balada no Brasil, isso iria repercutir muito rápido.

A maioria das pessoas pensam no bitcoin como um sistema de pagamentos, mas a rede de pagamento não tem muito valor se não houverem muitas pessoas que tenham a moeda requerida para utilizarem na rede de pagamentos. Quando um número grande o suficiente de pessoas tiver bitcoins, somente então a bitcoin se consolidará como um meio de troca. Por outras palavras, poucas pessoas têm utilizado bitcoin para muitos de seus pagamentos no varejo, porque um número insuficiente de pessoas possui bitcoins como uma reserva de valor; ou seja, apesar da grande quantidade de unidades, estas ainda estão nas mãos de poucas pessoas. Essas pessoas que estão dominando a posse da bitcoin, devem forçar a sua circulação para que a adesão ao Bitcoin aumente. Por outras palavras, devem reduzir a quantidade utilizada como reserva de valor, colocando um bom percentual em circulação, para que as que lhes sobrarem como reserva de valor, sejam mais valorizadas.

A “lei” de Gresham diz que a moeda ruim retira a moeda boa do mercado. Uma moeda experimentando mais inflação que as moedas substitutas seriam utilizadas no comércio mais frequentemente. Isso serviria a dois propósitos. Primeiro, o dono da moeda ruim iria preferir usá-la no comércio para manter a moeda mais estável e robusta em mãos. Exemplos, acumular ouro e usar a prata no comércio. Segundo, um indivíduo em posse de moeda que perde valor iria correr para trocá-la para obter bens que perdem valor menos rapidamente que a dita moeda. Porém, é importante perceber que a moeda apenas seria vista como ruim desde que esteja perdendo valor relativo a outras moedas na economia. Adicionalmente, se continuasse a perder valor, seu efeito destrutivo na economia eventualmente

iria terminar, já que em último caso ela se tornaria uma moeda praticamente inútil, limitando seu uso a transações minute. Não é provável que nenhuma nova moeda substitua uma moeda incumbente ao menos que a incumbente sofra uma grande perda de valor, de modo que as maiores transações nessa moeda se tornem impossíveis. Isto porque a “lei” de Gresham garante que moedas inferiores serão as primeiras a serem negociadas, e leis de curso legal obrigam a aceitar qualquer moeda com o status de curso legal. Porém, mesmo em casos onde a moeda mais popular utilizada para o comércio sofra um declínio massivo em valor, ela não será substituída pela moeda mais robusta. Ela será substituída pela próxima pior. Enquanto as moedas que depreciam mais vagarosamente são usadas para poupança, o sistema monetário de Zimbábue incentiva o uso das moedas menos estáveis nas transações diárias. Enquanto as leis de curso legal removem o problema de efeitos de rede, elas criam um novo problema, uma situação em que permite que moedas inferiores dominem o comércio.

Por fim, o que estabelece o valor da bitcoin é a regra básica da economia: oferta e procura. O número de bitcoins em existência é limitado e as pessoas querem comprar bitcoin, seja como forma de poupança, com a intenção de revenda (investimento) ou para realizar transferências e compras, locais ou internacionais. Diferente da moeda comum, não há a obrigação de aceitar bitcoin como forma de pagamento ou quitação de dívidas em nenhum lugar do mundo. Por esse motivo, o bitcoin hoje tem apresentado grande volatilidade, variando de acordo com a utilidade, especulação e novas regulamentações em cada país. Essa variação é um tanto semelhante à do real em relação a moedas internacionais e inflação; com a agravante de que o mercado do bitcoin é menor, o que significa que pequenas "turbulências" chacoalham bastante o mercado.

A lei de oferta e demanda é inexorável, e ela atua igualmente sobre qualquer mercadoria, até mesmo a moeda; que também é um bem, com particularidade de ser o bem mais líquido do mercado. Isso significa que, quando aumenta a oferta da quantidade de uma moeda, o seu preço (valor) diminui. Ou seja, quanto mais aumenta a quantidade de dinheiro em circulação, menor tende a ser o poder de compra de cada unidade monetária. Em suma, a moeda perde valor.

Está em circulação hoje, pouco menos de, 16.100.000 bitcoins, algo avaliado em torno de R$ 46.426.121.000,00 (quarenta e seis bilhões, quatrocentos e vinte e seis milhões e cento e vinte e um mil reais).

- https://blockchain.info/pt/charts/total-bitcoins.

Em 1998, quando a bitcoin foi lançada, era possível comprar 1.309,03 bitcoins por apenas um dólar. Atualmente, uma bitcoin custa cerca de R$ 2.916,00 (https://www.mercadobitcoin.com.br/).

No mês de julho de 2015, o Brasil bateu seu recorde local de transações em bitcoins, contabilizando 10 mil bitcoins, equivalentes a 9,3 milhões de reais (http://www1.folha.uol.com.br/colunas/ronaldolemos/2015/08/1666120-brasil-bate-recorde-em-bitcoins.shtml).

Para saber **converter os satoshis (centavos de bitcoin) em Reais** basta pegar o valor de uma bitcoin em Reais (exemplo R$ 957,30), dividi-la por 100000000 (porque os centavos do bitcoin possuem 8 [oito] casas decimais) e se terá o valor de cada Satoshi. Depois é só multiplicar o valor obtido pela quantidade de satoshis (com as 8 casas decimais depois da vírgula). Outra forma é simplesmente multiplicar 0,00000001 pelo valor de um bitcoin em Reais.

Confira o valor da bitcoin em Reais em http://preev.com/btc/brl.

O **IXBTC** é o primeiro índice de bitcoin do Brasil - http://www.brbitcoin.com.br/ixbtc/.

A **cotação da bitcoin** pode ser conferida em vários sites:

- http://bitvalor.com/;
- https://www.ripio.com/pt/cotizacion-bitcoin/;
- https://bter.com/;
- http://bravenewcoin.com/;
- http://br.investing.com/currencies/btc-usd;

- https://markets.blockchain.info/;
- http://exchangewar.info/;
- https://btc-e.com/;
- https://bter.com/;
- https://www.nyse.com/quote/index/NYXBT;
- https://bleutrade.com/exchange/VTA/BTC;
- https://bleutrade.com/exchange/EXP/BTC;
- https://bleutrade.com/exchange/ETH/BTC;
- https://testnet.blinktrade.com/pt_BR/#market;
- https://bitkonan.com;
- https://www.bitvc.com;
- https://hitbtc.com;
- https://www.okcoin.com/;
- https://www.tradingview.com/chart/?symbol=BTCYOU%3ABTCBRL;
- http://bitcointicker.co/;
- https://bitcoinchain.com/markets/btcusd-okcoin.

O site https://cointracking.info/ ajuda a estudar as cotações das criptomoedas. No site https://www.worldcoinindex.com/ existem as cotações de 472 criptomoedas enquanto que no http://www.coinwarz.com/cryptocurrency só tem de 72 moedas.

Já o site https://cryptolization.com/ utiliza nos cálculos 228 altcoins: 1CRedit, 2GIVE, Adzcoin, Aeon, Agoras Tokens, AmberCoin, Anoncoin, AntShares, Applecoin, Ardor, AsiaCoin, Asiadigicoin, AudioCoin, Augur, Auroracoin, BellaCoin, BilShares, BitBay, bitCNY, Bitcoin Plus, BitcoinDark, Bitcrystals, Bitland, Bitmark, BitShares, MUSE, Bitstar, bitUSD, BlackCoin, Blocknet, BlockPay, Boolberry, Breakout, Breakout Stake, BritCoin, BTCtalkcoin, BTSR, Burst, Bytecoin, CannabisCoin,

Capricoin, CasinoCoin, Circuits of Value, Clams, CloakCoin, Coin2.1, Jumbucks, Colossuscoin V2, Counterparty, Crown, Cryptonite, CureCoin, Darknet, Dash, Decred, Diamond, Diem, DigiByte, Digitalcoin, DigitalNote, DigixDAO, Dimecoin, DNotes, Dogecoin, DubaiCoin, EarthCoin, Einsteinium, Electronic Gulden, Emercoin, Energycoin, Ethereum, Ethereum Classic, EuropeCoin, EvergreenCoin, Expanse, Factom, FairCoin, Fantomcoin, Feathercoin, FedoraCoin, FlorinCoin, Flycoin, FoldingCoin, FuelCoin, Gambit, GameCredits, GetGems, GeoCoin, Global Currency Reserve, GoldCoin, GridCoin, Groestlcoin, Gulden, Gycoin (*Public Credits*), HempCoin, HiCoin, HitCoin, HTMLCOIN, HunterCoin, I0Coin, ICO OpenLedger, Iconomi, Infinitecoin, InstantDEX, I/O Coin, ION, Jewels, Jinn, Joincoin, KiloCoin, LeafCoin, LBRY Credits, Librexcoin, Lisk, Litecoin, LoMoCoin, LTBcoin, Magi, MaidSafeCoin, MaxCoin, MazaCoin, MediterraneanCoin, Megacoin, Mintcoin, MMNXT, MonaCoin, Monero, Mooncoin, Myriad, Namecoin, NautilusCoin, NAV Coin, NEM, NeosCoin, NeuCoin, Horizon, Nexus, NobleCoin, Novacoin, NuBits, NuShares, Nxt, Obits, OKCash, Omni, Orbitcoin, Pandacoin, Pangea Poker, Peercoin, Peerplays, Pepe Cash, Pesobit, PinkCoin, PLAY, PotCoin, Primecoin, Project Decorum, PutinCoin, Qora, Quark, Radium, ReddCoin, Riecoin, Rimbit, Ripple, Rise, Round, Rubycoin, Safe Exchange Coin, SaluS, SARCoin, Scotcoin, SecureCoin, ShadowCash, Shift, Siacoin, SIBCoin, Silk, SingularDTV, SkyNET, SmileyCoin, SolarCoin, SpreadCoin, StabilityShares, Startcoin, Stealthcoin, Steem, Steem Dollars, Stellar Lumens, Storjcoin X, Stratis, Stress, SuperNET, Swiscoin, Sync, Synereo, Synergy, SysCoin, TagCoin, Tether, Triggers, TrumpCoin, UnionCoin, Unobtanium, Vcash, Verge, VeriCoin, Vertcoin, Viacoin, Virtacoin, VootCoin, Voxels, VPNCoin, vTorrent, Waves, Wild Beast Block, Woodcoin, WorldCoin, Xaurum, XCurrency, YbCoin, Yocoin, Zcash, ZcCoin, ZClassic, ZCoin, Zeitcoin, Zetacoin, etc.

BITCOINERS - LOCAIS ONDE ACEITAM BITCOINS

Bitcoiners são os locais onde aceitam bitcoins:

- https://localbitcoins.com/pt-br/;
- http://mercadobitcoin.com;
- https://coinmap.org/;
- http://lista.mercadolivre.com.br/aceito-bitcoin;
- http://lojabitcoin.blogspot.com.br/;
- http://www.negociecoins.com.br/lojas-aceitam-bitcoins;
- http://spendbitcoins.com/;
- http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing;
- https://www.tecnisa.com.br/lp/bitcoin;
- https://guiadobitcoin.com.br/tag/paypal/;
- https://www.bitcoinmais.com/blog/lojas-que-aceitam-bitcoins/;
- http://www.hashbtcbrasil.com.br/2016/06/algumas-lojas-que-aceitam-bitcoins.html;
- https://www.bitcoin.com/spend-bitcoin-online;
- http://blogs.microsoft.com/firehose/2014/12/11/now-you-can-exchange-bitcoins-to-buy-apps-games-and-more-for-windows-windows-phone-and-xbox/#sm.00000zwxjbdh9hda3znlssqkgb9kh.

O Bitcoin World Map (https://play.google.com/store/apps/details?id=com.bubelov.coins) ajuda a localizar comerciantes que aceitam Bitcoin.

A loja **Drop Center** (http://dropcenter.com.br/loja/) é uma importadora que vende produtos cotados em Bitcoins para o mercado brasileiro.

É possível fazer apostas online com bitcoins:

- https://bitcasino.io/;
- https://www.cloudbet.com/;

- https://fortunejack.com/;
- http://www.bestbitcoincasinos.net/.

Para encontrar mais *bitcoiners*, basta pesquisar na Internet através dos seguintes termos: "accepts Bitcoin", "bitcoin accepted", "aceito bitcoin", "aceita-se bitcoins" ou "aceitamos bitcoin".

Inclusive, pode-se usar **Bitcoin em sites de apostas e casinos:**

- http://apostasbitcoin.com/;
- https://primedice.com/welcome;
- https://www.gambit.com/;
- https://peerbet.org/;
- https://www.satoshidice.com/.

Alguns **sites intermediários para poder efetuar pagamentos em bitcoins** (*Bitcoin banking*) são:

- https://www.bitbol.com.br/;
- https://paguecombitcoin.com/;
- https://www.coinbr.net/servicos#a-pay-bills;
- https://coinverse.com.br/pt-BR;
- https://xapo.com/pt/wallet/.

Na prática, existem várias **opções para pagar algo com bitcoins**:

- O estabelecimento aceitar o pagamento diretamente em bitcoin;
- O estabelecimento aceitar o pagamento através do Paypal (https://guiadobitcoin.com.br/tag/paypal/);

- O estabelecimento permitir o pagamento por boleto bancário, que será pago através de site de conversão da bitcoin na moeda de pagamento requerida;

- O estabelecimento tiver o sistema da PapPop (https://www.pagpop.com.br/);

- O estabelecimento aceitar algum cartão de débito que seja recarregado com bitcoins ou vinculado à uma *Wallet* (carteira) Bitcoin;

- O estabelecimento usar um sistema de pagamento por cartão de crédito que aceita o Paypal (exemplo, https://www.adyen.com/pt_BR/metodos-pagamento);

- O estabelecimento utilizar o Telegram Wallet (http://www.telegramwallet.io/);

- Utilizar uma *Wallet* (carteira) Bitcoin que tenha a opção de pagamento de contas;

- Efetuar a conversão das bitcoins em alguma *exchange*;

- Vender bitcoins para transformá-las na moeda necessária.

PayPal (https://www.paypal.com/br/home) é um sistema que permite a transferência de dinheiro entre indivíduos ou negociantes usando um endereço de e-mail, assim, evitando métodos tradicionais como cheques e boleto bancário.

O site https://www.virwox.com/ negocia bitcoins e aceita Paypal (https://www.paypal.com/), Skrill (https://www.skrill.com/), Paysafecard (https://www.paysafecard.com/pt-pt/), OK Pay (https://www.okpay.com/pt/), Sofort banking (https://www.sofort.com/) e cartões de crédito.

O banco **Bitinvest** (http://www.bit-invest.com/) aceita Payza (https://www.payza.com/), Perfet Money (https://perfectmoney.is/), OK Pay (https://www.okpay.com/pt/), Payeer (https://payeer.com/en/) e bitcoin.

Com o **cartão de débito Uquid** (https://uquid.com/) é possível enviar as bitcoins para o Paypal. Outras opções constam em https://cointopal.com/.

A dica é pesquisar por *exchanges* (casas de câmbios) que trabalhem com bitcoin e Paypal.

Detalhe, cartão pré-pago de débito não pode ser atrelado a uma conta Paypal e nem em sites nos quais a plataforma de pagamento é administrada pelo Paypal.

Outra pesquisa a ser feita é sobre quais cartões de débito trabalham com bitcoin, quais são as formas de carregá-los e onde eles são aceitos.

BitcoinCard (http://www.bitcoincard.com.br/) um cartão pré-pago brasileiro de bitcoin. Funciona como um cartão de crédito pré-pago que transforma bitcoins em dinheiro convencional, permitindo compras nas lojas credenciadas ao VISA e saques em moeda local nos caixas eletrônicos da Rede24Horas.

Existem vários **cartões de débito em bitcoins**:

- https://anxpro.com/pages/card;
- http://advcash.com/en/;
- https://www.e-coin.io/multisig-wallet-and-bitcoin-card-benefits#benefit-ecard;
- https://wirexapp.com/pt/cards/index.html;
- https://wirexapp.com/pt/bitcoin-debit-card.html;
- https://in.xapo.com/campaign/debit/;
- https://xapo.com/pt/card/;
- https://satoshitango.com/iniciacao;
- https://bitpay.com/visa/;

- https://www.shiftpayments.com/card;
- https://unichange.me/;
- https://www.neteller.com/pt;
- https://shakepay.co/#/;
- https://cryptopay.me/bitcoin-debit-card;
- https://bitnation.co/bitcoin-debit-card/;
- https://spectrocoin.com/en/bitcoin-debit-card.html;
- https://bitplastic.com/;
- https://www.bitwa.la/;
- https://www.bitnovo.com/;
- https://www.bitstamp.net/;
- https://www.coinizy.com/;
- https://coinsbank.com/cards;
- https://www.ebanx.com/br;
- https://moneypolo.com/;
- https://www.getonebit.com/;
- https://payeer.com/en/;
- https://www.wagecan.com/;
- https://www.satoshitango.com/;
- https://www.ecopayz.com/en-gb/ecopayz;
- https://plutus.it/;
- https://www.wmtransfer.com/;
- https://uquid.com/;
- https://therocktrading.com/;
- https://www.xmlgold.eu/;

- https://www.goldmoney.com/.

O grande problema dos cartões AdvCash, Wirex e Xapo, são os encargos: para emissão do cartão, mensal, ATM (*Automated Teller Machine* ou caixa eletrônico ou automático), por transação, para fazer depósito, saques e conversão de moeda (de 2% a 6%). Uma opção, é o **Intermedium** (https://www.intermedium.com.br/), que possibilita ter um cartão de débito Internacional com a bandeira MasterCard sem custo para realizar compras. É possível fazer saques ilimitados e gratuitos nos caixas eletrônicos do Banco24Horas (http://banco24horas.com.br/). O Intermedium permite o depósito mediante boleto bancário, que é gerado sem custo e pode ser pago através de sites como o https://paguecombitcoin.com/ ou https://www.bitbol.com.br/. Essa é a maneira mais rápida e mais barata para usar os Bitcoins no Brasil. A única taxa será a do serviço de boleto.

- https://www.intermedium.com.br/conta-corrente.jsf;
- https://www.conta-corrente.com/conta-digital/intermedium/conta-digital-intermedium-e-unica-100-gratuita/;
- https://www.conta-corrente.com/conta-digital/intermedium/conta-intermedium-permite-emitir-boleto-bancario-de-graca/.

O **Nubank** (https://www.nubank.com.br/) é um cartão de crédito internacional da Mastercard, na variante Gold (http://www.mastercard.com/br/consumidores/gold-mastercard.html), livre de anuidade e de taxas de cadastro, emissão e manutenção (serviços básicos), com as demais taxas e os juros inferiores aos concorrentes convencionais, o primeiro cartão gratuito e com controle total através do smartphone com sistema iOS ou Android (cadastro e solicitação 100%, atendimento 100% via chat, faturas 100% online se possuir conta bancária com acesso ao *internet banking*, etc.). Um dos seus concorrentes é o **Digio** (http://digio.com.br/); administrado pelo Banco CBSS (http://www.bancocbss.com.br/), uma instituição financeira pertencente a Elo Participações S/A (*holding* do Banco do Brasil, do Bradesco e da Caixa Econômica Federal), que oferece os mesmos benefícios do Nubank; mas com a bandeira Visa, na modalidade Classic (https://www.visa.com.br/pague-com-visa/cartoes/cartoes-de-credito/visa-classic-detalhes.html). Nos dois o

desbloqueio é feito de forma online no próprio aplicativo e funciona instantaneamente. Nenhum dos dois oferece pontos ou milhas; mas o Nubank possui os pontos do MasterCard Surpreenda (https://surpreenda.naotempreco.com.br/rewards/vouchers/surpreenda) e o Digio pode passar a ter os pontos do programa Livelo (http://www.pontoslivelo.com.br/). Não existem seguros de viagem, locação de veículos, seguro saúde e outras vantagens de alguns cartões comuns. Não há crédito rotativo para quem quiser parcelar a fatura em atraso, o cliente terá que parcelar o valor. O Nubank possibilita que o cliente em dificuldade pague um valor mínimo na data de vencimento de sua fatura, pagando juros pelo restante até que haja quitação total ou parcial. O Digio não oferece essa opção, assim que ocorrer o atraso o cliente terá que parcelar a dívida total, acordando uma taxa de juros no momento do parcelamento. A modalidade é parecida com uma renegociação da dívida, a diferença é que a fatura do cartão de crédito se torna um empréstimo pessoal com juros também bastante altos. **Dos dois, o Nubank é o melhor** por cobrar menos taxas, a bandeira Mastercard Gold oferecer mais vantagens que o Visa Classic e o atendimento do Nubank ser muito superior. O Nubank só perde por ainda precisar de convite e por ter passado a cobrar anuidade pelo programa de fidelidade do cartão. Conselho, não use o Nubank para pagar compras no Ebay (PayPal) para evitar dupla conversão Real - Dólar

- http://emalta.com.br/visa-ou-mastercard-comparativo-cartoes-credito/.

Outra opção é o **Banco Intermedium** (https://www.intermedium.com.br/), que é um banco completo 100% gratuito, online, isento de tarifa bancária e com cartão de débito Mastercard. O usuário abre uma conta corrente como se fosse um banco comum e passa a ter acesso a todas as opções geralmente reservadas a bancos convencionais, como transferências TED e DOC para outros bancos, pagamentos de boletos através do Pague Fácil Intermedium e saques em caixas eletrônicos do Rede Banco 24 horas. No Intermedium a conta é totalmente gratuita e isenta de tarifas até mesmo para serviços como TED e Saque na rede 24h. Enfim, a propaganda é de tudo ser sem taxas, cobranças ou limites de transações; mas deve ter algumas exceções. O cliente recebe um cartão múltiplo habilitado na função débito. A ativação do cartão de crédito pode ser solicitada e passa por uma análise. Não há a cobrança de anuidade! O cliente Intermedium tem

lastro garantido para investir nas opções de LCI da instituição (CDI, IPCA e IGPM) e, ainda, conta com os outros produtos de investimentos do banco, como o CDB. Todo o atendimento é feito via smartphone (sistemas Android e iOS), além de chat, no horário bancário, para pendências mais detalhadas. Depois de aberta a conta, é possível enviar um e-mail com documentos (RG e comprovantes de endereço e de renda) solicitando a liberação de limite de crédito no cartão MasterCard. **Com a Conta Digital Intermedium é possível efetuar depósitos em bitcoins, que serão creditados em reais na conta.** Explica-se. A Conta Digital Intermedium possui um sistema gratuito de geração de boleto para fins de depósito na referida conta bancária, que pode ser pago através de Bitcoins em sites especializados (por exemplos, https://www.bitbol.com.br/ e https://paguecombitcoin.com/).

- https://www.conta-corrente.com/conta-digital/intermedium/conta-intermedium-permite-emitir-boleto-bancario-de-graca/.

Acesso (https://www.acessocard.com.br/) é um cartão pré-pago da MasterCard que permite saques nas redes Cirrus ou Camisarias Colombo. O cartão possui custo e é cobrada mensalidade.

Conta Super (http://www.contasuper.com.br/), do Santander, é um cartão pré-pago internacional da Mastercard, com diferentes planos de taxa. Só é possível sacar na rede Banco24Horas (que possui taxa) e só dá para transferir dinheiro para outras pessoas que também tenha Conta Super (sem pagar nenhuma taxa).

PayPaxx (https://paypaxx.com.br/) é um cartão pré-pago para empresas para controle de despesas pelos funcionários.

Contaum (https://www.contaum.com.br/) é uma conta corrente digital com um cartão de crédito internacional e pré-pago, que incorpora benefícios, promoções e serviços exclusivos. Para carregar o cartão basta entrar no site e gerar um boleto com o valor que desejado para disponibilizar na conta. Usufrui dos benefícios do programa MasterCard Surpreenda. É voltada para as necessidades empresariais. Os usuários das contas salário possuem taxas de movimentação da conta menores que de um banco tradicional e podem fazer pagamentos de contas, transferências, consulta de saldo e extrato, saques, recarga de celular, a qualquer momento e sem taxas com direito a

todo o suporte de atendimento através do menu Ajuda do aplicativo, no próprio celular.

O **Banco Sofisa Direto** (http://www.sofisadireto.com.br/) é digital, mas voltado apenas para quem deseja investir. Oferece uma conta corrente sem tarifas, porém sem cartão de crédito ou débito. É possível realizar pagamentos de boletos com o saldo da conta. Só é possível receber transferências de outros bancos (DOC e TED) de contas com a mesma titularidade. A abertura da conta é através de formulário no site e a assinatura da proposta é digital.

Há, ainda, o **Banco Neon** (https://www.banconeon.com.br/), com cartões (um físico e outro virtual) internacional, de débito, na bandeira Visa, sem mensalidade e nem anuidade, participante do programa de benefícios "Vai de Visa" (https://www.promocoesvisa.com.br/vaidevisa/site) e que também é operado por aplicativo de smartphone. O usuário poderá fazer operações diversas pelo celular, como verificar saldo, realizar transferências, pagar contas, receber pagamentos. Os usuários podem fazer um saque pela rede 24horas e um TED por mês de graça. Para fazer um depósito para a conta, o Neon recorre ao bom e velho boleto. Quando a transação é solicitada, o app gera um boleto que o usuário pode pagar em qualquer lotérica. O cartão do Neon só permite compras na função débito atualmente. O atendimento ao cliente é feito, 24 horas por dia, 7 dias por semana, por telefone 0800, por chat dentro do próprio aplicativo e através das redes sociais (Facebook, Twitter, Instagram e LinkedIn).

O **Unobank** (https://www.unobank.com.br/) não é uma instituição financeira, mas um correspondente bancário. Assim não cobra ou solicita nenhum tipo de pagamento dos clientes para nenhum tipo de produto uma vez que é remunerado pelas instituições financeiras parceiras. É sem agência, sem fila e sem burocracia! Contratação online, desde a simulação até assinatura digital do contrato. Os serviços disponíveis são: conta digital UNO, sem tarifa de manutenção, gerenciada pelo smartphone; empréstimo pessoal online; cartão internacional, de crédito (Mastercard) ou de débito pré-pago (Visa), sem anuidade e vinculado à conta UNO; pagamentos de contas de consumo ou boletos pelo App; transferências para contas UNO ou outros bancos; saques na rede 24h; depósitos por boletos bancários; etc. O

Unobank é propriedade de uma *offshore* norte americana chamada Latinvest Capital e está registrado no Brasil como sendo a empresa GLX Serviços Empresariais Ltda, localizada na Barra da Tijuca/RJ.

A **Conta.Mobi** (http://conta.mobi/) é uma conta corrente 100% digital, aberta pelo celular, destinada ao MEI (Microempreendedor Individual), que possui funções parecidas com a de uma conta corrente tradicional: permite emitir boleto bancário e fazer transferências via DOC ou TED para qualquer banco; possui cartão de débito internacional com a bandeira VISA; consulta e emissão de extrato pela internet; saque de dinheiro em caixas eletrônicos com o cartão de débito da conta; envio de SMS e e-mail; auxílio contábil sem custo por meio do programa contadores do bem (http://conta.mobi/contadoresdobem/); etc.

- http://conta.mobi/campanha-adwords/.

O **PagSeguro** vende para seus clientes da leitora moderninha, um cartão pré-pago internacional da MasterCard, sem anuidade, sem mensalidade e sem fatura (https://pagseguro.uol.com.br/pre-pago/). O cartão, além de usar o saldo da conta do cliente no PagSeguro (dinheiro das vendas realizadas), ainda pode ser recarregado por Boleto bancário, débito online de conta bancária e por depósito em conta. **De forma semelhante, o SumUp** (https://sumup.com.br/cartao) também concede um cartão da MasterCard sem conta bancária, vinculado à Rede 24H; só paga a taxa de saque, sem custos adicionais, sem mensalidades ou taxas surpresas. A SumUp, em 2016, celebrou fusão com a **Payleven** (https://payleven.com.br/). Também a **Pagcom** (https://www.pagcom.net/site/conta_pagcom).

O **Brasil Pré-Pagos** (https://www.brasilprepagos.com.br/brasil-prepago-digital.html) possui o cartão pré-pago digital que permite compras em sites internacionais sem precisar de um cartão de crédito internacional. O cartão é carregado, através de boleto ou cartão de débito, com o qualquer valor e o controle é feito em tempo real pelo app disponível para iOS e Android.

Também existe a conta corrente 100% digital, sem tarifas e cartão de crédito com condições especiais do **Banco Original** (https://www.original.com.br/), do grupo J&F, dono de empresas como a

Friboi e Havaianas. A conta é totalmente digital (desde que a conta corrente seja aberta através do aplicativo do Banco Original para Android ou iOS) e tudo é feito de forma online. Se o cliente abrir a conta pelo seu smartphone, em momento algum precisa imprimir, assinar ou enviar papéis. A exceção fica para a conta aberta pelo computador (restrita à algumas cidades), onde um gerente do banco irá até sua residência coletar os papéis da abertura de conta assinados. O aplicativo permite depósito de cheque através de fotografias enviadas pelo smartphone. Existem, ainda, alguns locais chamados de "espaço original", onde o cliente pode realizar depósitos em espécie. Caso precise sacar dinheiro em espécie, a opção é realizar saques pelo Banco24Horas (http://banco24horas.com.br/). Quem ainda trabalha com dinheiro vivo pode ter muitas dificuldades em realizar depósitos e custos altos para realizar saques no Original. O foco não é ser uma opção 100% gratuita, e sim apostar na praticidade e redução de custos nas suas operações. Diferente do Digio e do Nubank, que se restringem ao serviço de cartão de crédito, o Banco Original oferece conta corrente, com cartão (https://www.original.com.br/pessoafisica/cartoes/) de débito ou crédito (se aprovado) e opções para aplicação de valores (CDB e não é possível aplicar em fundos de investimento ou no Tesouro Direto, aplicação mínima de R$ 5.000,00 [cinco mil reais], não há aplicação automática, oferece gerenciador financeiro completo). Não há opção para pagamento de boletos de arrecadação (luz, água, telefone, etc.), apenas boletos de cobrança comuns. O cliente conta com atendimento personalizado, com um gerente e consultores, através por telefone, site oficial, vídeo chamada ou via chat no aplicativo do celular. Trata-se de um banco tradicional cujo principal diferencial é a forma de atendimento. As tarifas cobradas são em geral iguais ou superiores às dos bancos tradicionais. A "franquia original", como é chamado o pacote básico de conta corrente do banco, oferece mensalmente 10 folhas de cheque, 5 saques na Rede24horas, 2 transferências entre bancos que podem ser via TED ou DOC e transferências entre contas do banco ilimitadas.

Outros bancos tradicionais também estão migrando para a virtualização. O Banco do Brasil, conta com a **Conta Fácil BB**, que pode ser aberta por meio de um aplicativo para celular nos sistemas Android e IOS.

- http://www.bb.com.br/pbb/pagina-inicial/voce/produtos-e-servicos/cartoes/cartoes-com-promocoes-e-vantagens-especiais/conta-facil#/.

O Itaú, por sua vez, possuía a **iConta** (https://www.itau.com.br/conta-corrente/abra-sua-conta/iconta/); uma conta digital e sem tarifa, que é operada por um aplicativo para smartphones.

Diferentemente da Digiconta do Bradesco (http://banco.bradesco/html/classic/produtos-servicos/conta-corrente/digiconta.shtm), no Intermedium não há a necessidade de comparecer até uma agência para abrir conta, pois todo o processo é feito online.

O **MotionCode** é apenas uma tecnologia da Oberthur Technologies (http://www.oberthur.com/motioncode/), que altera o código de segurança (três dígitos que ficam na parte de trás) do cartão de tempo em tempo. Após esse intervalo, o código não é mais válido. Desse modo, o código CVV, impresso e estático impresso, é substituído por uma minitela, que exibe um código atualizado automaticamente gerado por um algoritmo carregado no chip incorporado no corpo do cartão (CVV dinâmico).

Economize em compras no exterior usando cartão de débito Internacional (como, por exemplo, o **ADVCash** - http://advcash.com/en/), em dólar, emitido por uma empresa estrangeira (sem IOF, portanto) e carregado em bitcoins (podendo comprar dólar mais barato do que a cotação do dólar turismo), por exemplo, na **FOXBIT** (https://foxbit.com.br/). Também há opção do cartão da **Neteller** (https://www.neteller.com/pt). O cartão **InstaForex Benecard** (https://www.instaforex.com/pt/instaforex_benecard), fornecido aos clientes da InstaForex (https://www.instaforex.com/pt/), também pode ser uma opção; ainda mais que, também, trabalha com Bitcoins (https://www.instaforex.com/pt/bitcoin_trading). A **Bitnovo** (https://www.bitnovo.com/tarjeta-monedero-bitcoins), é uma plataforma espanhola de pagamentos com Bitcoin, que conta com cartões de débito carregados com Bitcoin para serem usados em lojas e caixas eletrônicos que aceitem MasterCard. Outra dica, a **Paysafecard** (https://www.paysafecard.com/pt-pt/) é líder no mercado europeu de meios de pré-pagamento. Confira, ainda, os seguintes links:

- https://www.weswap.com/it/;
- https://www.schwab.com/;
- https://www.okpay.com/pt/personal/payment-cards/;
- https://www.okpay.com/pt/personal/fees/;
- https://www.bil.com/en/Pages/Index.aspx;
- https://www.dkb.de/;
- https://www.wirecardbank.com/;
- https://avuba.de/;
- https://www.fidor.de/;
- https://www.fidorbank.uk/;
- https://www.hype.it/;
- https://worldcore.eu/;
- https://www.leupay.eu/;
- https://n26.com/;
- https://www.paymix.eu/;
- https://www.papaya.eu/;
- https://www.paysera.com/;
- https://www.paxum.com/;
- https://www.payoneer.com/;
- https://revolut.com/;
- http://www.smartpaycard.net/si/default.wlgt;
- http://www.veritascard.com/;
- https://vikingcard.com/en/;
- https://www.viabuy.com/;
- http://boonpayment.com/.

Pelos sites http://www.goodfinancialcents.com/best-cash-back-credit-cards/ e http://www.mybanktracker.com/credit-cards é possível **comparar os cartões americanos** e, em http://www.comparecards.com/reward os programas de recompensas de cartões americanos. Já em https://www.comparaonline.com.br/cartao-de-credito e https://comparabem.com.br/cartoes-credito compara-se os **cartões de créditos brasileiros**. Também é possível comparar os bancos em https://wallethub.com/banks/ e http://banks.credio.com/; em http://www.findabetterbank.com/ é possível localizar mais bancos. Já no Brasil, é possível comparar as tarifas bancárias em http://www.febraban-star.org.br/ e http://www.febraban-star.org.br/CompararTarifaPasso1.asp. Sobre bancos europeus, há uma relação em https://pt.wikipedia.org/wiki/Lista_de_bancos_da_Europa.

O **BTCjam** (https://btcjam.com) funciona como um intermediador de negócios permitindo que os investidores escolham a quem emprestar o seu dinheiro diretamente e em troca cobra uma taxa sobre o valor total de cada empréstimo realizado. Também há o https://bitlendingclub.com/.

- http://blogs.estadao.com.br/link/brasileiro-cria-no-vale-do-silicio-sistema-de-emprestimo-de-bitcoins/;
- https://yeppudaproductions.wordpress.com/2015/03/27/btcjam-e-genericos-nao-use/.

Também existe o BitLendingClub (https://bitlendingclub.com/).

Para quem pretende aceitar pagamentos em bitcoins, basta oferecer essa opção para seus clientes.

Existem ferramentas disponíveis para permitir aos comerciantes aceitar pagamentos tanto *on* (conectado) e *offline* (desconectado).

O jeito mais fácil de o empresário e qualquer pessoa receber pagamentos em Bitcoins e/ou altcoins, é simplesmente usando uma carteira (*wallet*) como qualquer outra pessoa. Assim, no caso do Bitcoin, pode-se instalar no dispositivo o software cliente original do Bitcoin (http://bitcoin.org/en/download); o qual irá criar um endereço bitcoin para

enviar e receber o dinheiro virtual e armazenar a chave privada que protegerá a conta. Além dessa carteira, existem várias outras muito utilizadas como, por exemplo, a Multibit (https://multibit.org/).

Empresários que aceitam Bitcoin como forma de pagamento, podem usar o *smartphone* ou *tablet* para completar as transações. Tudo que precisam é de um aplicativo que transforme seu dispositivo iOS ou Android em uma "maquininha" POS (*Point Of Sale* [ponto de venda] ou *Point of Service* [ponto de serviço]). Não confundir com PoS - *Proof of Stake* (prova de jogo ou de participação).

- https://www.carteirabitcoin.com.br/como_funciona/para_comerciantes;
- https://www.pagpop.com.br/;
- https://www.snapcard.io/masspay;
- https://xbterminal.io/pt-br/;
- https://bitpay.com/;
- https://www.coinbase.com/merchants;
- https://www.pagcoin.com/;
- http://bit.one/;
- https://stripe.com/us/payments;
- https://stripe.com/bitcoin;
- http://www.cryptopag.com/2016/08/adote-criptomoedas-em-seu-negocio.html;
- https://www.paypal.com/br/webapps/mpp/merchant-integration;
- https://www.braintreepayments.com/payment-methods/accept-bitcoin;
- https://bitcoinpay.com/en/;
- https://www.bitkassa.nl/;
- https://bitpos.me/;
- https://www.coinpip.com/;
- https://airbitz.co/;

- https://bitstraat.nl/;
- https://www.bitpagos.com/pt/;
- https://www.ripio.com/pt/;
- https://www.xtechcommerce.com/;
- https://www.carteirabitcoin.com.br/.

Uma opção no Brasil é a utilização da Snapcard Bitcoin através da parceria da **Snapcard** (https://www.snapcard.io/) com a brasileira **PapPop** (https://www.pagpop.com.br/). Através da PapPop é possível receber pagamentos em Bitcoin, Litecoin ou Dogecoin. Pelo gateway de pagamento da **Azpay** também (http://www.azpay.com.br/gateway-de-pagamento-multicoin-bitcoin-litecoin-dogecoin/).

A Coinpayments (https://www.coinpayments.net) é um gateway de pagamento integrado que aceita mais de 50 moedas virtuais (https://www.coinpayments.net/supported-coins).

XBTerminal (https://xbterminal.io/en/) é a maneira rápida, simples e de baixo custo para os comerciantes para começar a aceitar bitcoin imediatamente. A empresa oferece um dispositivo POS bitcoin que permite aos clientes do comerciante a pagar a partir de qualquer carteira bitcoin móvel por código NFC ou QR. Ressalta-se, assim, que POS (*Point Of Sale* [ponto de venda] ou *Point of Service* [ponto de serviço]) é a leitora ("maquininha") de cartão bancário. Não confundir com PoS - *Proof of Stake* (prova de jogo ou de participação).

Com sede em Londres, Bitcoinpay.com (https://bitcoinpay.com/en/) é uma das empresas que mais crescem no Bitcoin *commerce*. BitcoinPay fornece um gateway de pagamento global e instantânea construído em cima da bitcoin.

PayStand (http://www.paystand.com/) é um sistema de verificação de pagamento e *e-commerce* que permite às organizações tomar crédito, e-cheque e bitcoin a 0% de honorários.

Existem diversos sites que prestam serviço similar:

- https://www.bitpagos.com/pt/;
- https://www.gocoin.com/;
- https://www.coinjar.com/spend;
- https://cryptopay.me/accept-bitcoins;
- https://www.coinbase.com/merchants;
- https://blockchain.info/api/api_receive;
- http://www.bitcoinway.com/;
- https://paybycoin.intuit.com/.

O Ripple (https://ripple.com/) permite aos bancos para enviar pagamentos internacionais em tempo real através de redes e trabalha com Ripple (XRP), Bitcoin, Litecoin, Namecoin, NoFiatCoin, Dólares norte-americanos, Euros, Dólar da Nova Zelândia, Yuan chinês, Yen japonês, Dólares australianos, moeda brasileira e Pesos mexicanos.

Outra forma do empresário "fisgar" clientela da comunidade Bitcoin, é aceitar pagamento através de boleto bancário e divulgar que aceita pagamentos em bitcoins através do site que permite pagar boletos com bitcoins. E, uma opção disso é usar a Conta Digital Intermedium; onde é possível efetuar depósitos em bitcoins, que serão creditadas em reais na conta. Explica-se. A Conta Digital Intermedium possui um sistema gratuito de geração de boleto para fins de depósito na referida conta bancária, que pode ser pago através de bitcoins em sites especializados (por exemplos, https://www.bitbol.com.br/ e https://paguecombitcoin.com/).

- https://www.conta-corrente.com/conta-digital/intermedium/conta-intermedium-permite-emitir-boleto-bancario-de-graca/.

Pode-se, ainda, socorrer-se do auxílio de vários sites de desenvolvimento das moedas digitais.

Bitcoin Hub (http://itsrio.org/projects/bitcoin-hub/) é um projeto do Instituto de Tecnologia e Sociedade (ITS) do Rio de Janeiro.

UNIDADES DA BITCOIN (SATOSHIS)

A (moeda) bitcoin pode ser dividida em subunidades até 8 (oito) casas decimais (0,000.000.01); ou seja, cem milhões de centavos. Em suma, são necessários 100.000.000 (ou 10^8) satoshis para se ter 1 (uma) bitcoin.

Pequenas quantidades de bitcoin usadas como unidades alternativas são o milibitcoin (mBTC), microbitcoin (µBTC) e satoshi. Nomeado em homenagem ao criador do bitcoin, um satoshi é a menor quantidade do sistema, representando 0,00000001 bitcoin, um centésimo de milionésimo de um bitcoin. Um milibitcoin (mBTC) equivale a 0,001 bitcoin, que é um milésimo de bitcoin. Um microbitcoin (uBTC) equivale a 0,000001 bitcoin, que é um milionésimo de bitcoin. Um microbitcoin às vezes é chamado também de um bit. 1 mBTC é uma milibitcoin, que é exatamente 0.001 BTC. 1 µBTC, ou somente uBTC, significa 1 microbitcoin. Isto é 1 milionésimo de bitcoin, que é 0.000001 BTC. Confira em http://satoshi.24ex.com/.

Já no Litecoin a unidade dos centavos se chama litoshi.

1 Satoshi significa 0.00000001 BTC, e é o valor mais pequeno de BTC que pode ser usado. Satoshi Nakamoto é o inventor da bitcoin e esta unidade ganhou esta designação em homenagem ao autor.

Confira as unidades de bitcoin em https://en.bitcoin.it/wiki/Units.

Abreviatura	Nome	Número (BTC)
MBTC	Megabitcoin	1.000.000
kBTC	Kilobitcoin	1.000
hBTC	Hectobitcoin	100
daBTC	Decabitcoin	10
BTC	Bitcoin	1
dBTC	Decibitcoin	0.1
cBTC	Centibitcoin	0.01
mBTC	Millibitcoin	0.001
µBTC	Microbitcoin	0.000001
satoshi		0.00000001

Satoshis	Bitcoins
1	0.00000001
10	0.0000001
100	0.000001
1.000	0.00001
10.000	0.0001
100.000	0.001
1.000.000	0.01
10.000.000	0.1
100.000.000	1

BTCs	Satoshis
1 BTC	100.000.000
1 BTC	1.000.000
1 BTC	1.000
1 BTC	100
0.00000001 BTC	1
0.01 uBTC	1
0.00001 mBTC	1
0.000001 cBTC	1
1 uBTC	100
1 mBTC	100000
1 cBTC	1000000

BTC	BTC
1 uBTC	0.001 mBTC
1 uBTC	0.0001 cBTC
1 uBTC	0.000001 BTC
1 mBTC	1000 uBTC
1 mBTC	0.01 cBTC
1 mBTC	0.001 BTC
1 cBTC	10000 uBTC
1 cBTC	10 mBTC
1 cBTC	0.01 BTC

Existem vários sites conversores (*converters*) que realizam a conversão (*conversion*) para facilitar o manuseio das unidades bitcoin.

- http://bitsusd.com/;

- http://satoshitobitcoin.co/;
- http://xapo24.eu/satoshi-converter/;
- https://milli.io/satoshi-usd-converter/;
- https://www.coinstaker.com/calculators/;
- http://www.btcsatoshi.com/;
- http://satoshitimes.wikidot.com/blog:2;
- http://pt.coinmill.com/BRL_BTC.html;
- https://pt.coinmill.com/BTC_calculator.html.

ONDE SE GUARDAM AS BITCOINS E ALTCOINS?

O (protocolo) Bitcoin permite a propriedade, a posse e a transferência anônimas de bitcoins. Para fins didáticos, pode-se dizer que as bitcoins podem ser salvas em computadores através de programas (*softwares*) carteira (*wallet*) ou em serviços online de carteira provido por terceiros; em ambos os casos, as bitcoins podem ser enviadas pela Internet para qualquer pessoa que tenha um endereço de Bitcoin (chave pública).

Não é necessário fornecer nenhum documento, nem mesmo fornecer os números dos documentos. Não exige identificação, foto, comprovante de endereço residencial e nem número de telefone fixo; exceto o de celular se usar carteira móvel. Não é preciso pedir permissão para ninguém. Não se exige convite. Não existe valor mínimo para investir. Muito menos exige-se comparecer pessoalmente em algum estabelecimento e assinar papelada. Nada disso é necessário. Também não é necessário entender conceitos complexos ou compreender como ele funciona; basta saber para que serve e como usar. Qualquer pessoa no mundo em qualquer país com acesso à Internet pode gerar um endereço Bitcoin, se conectar e participar da rede Bitcoin. Não horários e nem feriados. Não há fronteiras. Não há limites impostos.

Para poder manter, receber e usar as bitcoins é necessário possuir uma conta ou carteira virtual. As carteiras bitcoin são similares aos vários caixas de um banco ou de um supermercado, registrando individualmente as entradas (recebimentos) e saídas (pagamentos) e que, ao mesmo tempo, todos informam ao sistema central onde todas as informações são reunidas e registradas. Igualmente, são parecidas com os vários caixas eletrônicos de um enorme banco com agências em todos os países; vez que quando as carteiras bitcoin estão conectadas (online) estão interligadas, sincronizadas e todas as operações efetuadas em cada uma delas é imediatamente comunicada por toda a rede ou sistema. Pode-se, ainda, comparar as carteiras bitcoins com contadores de um imenso escritório de contabilidade mundial que estão conectados, interligados, sincronizados e convergem todos os seus trabalhos, de forma sequencial, organizada e harmônica, para o mesmo livro digital contábil (no caso, a *Blockchain*). Desse modo, as

carteiras bitcoin são terminais de acesso (*nodes*, nós, pontos ou clientes) de uma grande rede ou sistema (P2P, *peer-to-peer* ou ponto a ponto).

De forma didática, pode-se assemelhar as carteiras bitcoins com vários pedreiros construindo em conjunto a mesma imensa parede ou muro (*Blockchain*). Assim, apesar de serem várias pessoas trabalhando, cada qual com suas ferramentas e materiais, todas elas estão trabalhando ao mesmo tempo e na mesma obra específica. Apesar de ser uma única parede (ou muro) que está sendo levantada por vários pedreiros ao mesmo tempo, não há nenhuma confusão, bagunça, desordem, desorganização, conflito ou atrito; vez que cada pedreiro assenta um tijolo (bloco) sobre o tijolo imediatamente anterior assentado por outro pedreiro e, assim, sucessivamente e em sequência.

As carteiras bitcoin não são muito diferentes dos aplicativos de celulares (*smartphones*) dos bancos e de seus serviços de *internet banking*; vez que tais facilidades fornecidas pelos bancos substituem o atendimento pessoal dos caixas e dos terminais de autoatendimento (caixas eletrônicos).

Feitas estas explanações iniciais, podemos agora dizer que, tal como no serviço de *internet banking* dos bancos convencionais, nos quais não existe e nem sai nenhum dinheiro no computador, no celular ou no *tablet* do cliente, não passando tudo de meros dígitos binários (caracteres, dados ou bytes) num dispositivo computacional, o mesmo ocorre com as carteiras bitcoin. O que as carteiras bitcoin guardam, na verdade, são apenas as chaves de acesso aos valores existentes no grande livro contábil, a *Blockchain*. De modo semelhante ao utilizar-se do serviço de *internet banking* dos bancos convencionais, se está acessando os dados contábeis no sistema do banco, onde é possível transferir créditos (valores, dígitos) para outra pessoa.

Portanto, de forma semelhante a um cartão bancário que não tem nenhum dinheiro dentro dele, mas tão somente o acesso ao livro contábil no banco, de forma semelhante, as carteiras físicas (*hardware*) de bitcoin, não possuem nenhum bitcoin dentro delas, mas apenas as chaves de acesso aos dados constantes na *Blockchain*.

A *Blockchain* é semelhante a um enorme livro digital de registro de contabilidade pública e compartilhada, que registra cada transferência de bitcoin que for realizada no mundo, autenticando cada uma dessas transações ao combinar as assinaturas digitais do remetente e do destinatário com os endereços de envio e de recebimento (que possuem de 34 a 36 caracteres formados de números e letras maiúsculas e minúsculas). O endereço bitcoin (chave pública ou chave simples), por padrão, começa com o número 1. Mas se for múltipla assinatura (*multi signature*), começa com o número 3.

Cada entrada de dados na *Blockchain* é feita através de blocos, como se fossem folhas de caderno cheias (totalmente escritas) sendo inseridas num livro, caderno ou fichário. E, como folhas de caderno, possuem várias linhas onde cada linha corresponde a uma transação bitcoin.

A cadeia de blocos que constitui a *Blockchain*, tal como num dos exemplos acima, é similar aos tijolos que vão sendo assentados para formar uma parede ou muro; só que os blocos são mais semelhantes aos elos de uma corrente, pois precisam ser anexados em sequência para poder-se formar uma corrente ininterrupta, ordenada e cronológica. É semelhante a inserção das folhas escritas de um caderno fichário para que mantenham a sequência temporal pela qual foram escritas. Portanto, um bloco é ligado ao bloco imediatamente anterior informando qual foi o "hash" (código calculado, conferido e aceito pela rede Bitcoin), formando a corrente de blocos até o primeiro bloco do Bitcoin.

Uma carteira bitcoin armazena as informações que são necessárias para se fazer transações com bitcoin; o que passa disso é uma consulta de saldo positivo suficiente, o que não deixa de ser algo necessário para a transação. Embora as carteiras bitcoin frequentemente sejam descritas como sendo um lugar para guardar, carregar ou armazenar bitcoins, no entanto, os bitcoins são inseparáveis do registro da *Blockchain*; ou seja, eles nunca saem dela. Portanto, uma carteira de bitcoins é como algo que armazena as credenciais digitais que permitem o acesso e uso dos fundos bitcoin. Simplificando, uma carteira é como um chaveiro, contendo duas chaves criptográficas, uma pública e outra privada.

Embora as carteiras frequentemente sejam descritas como um lugar para guardar, carregar ou armazenar bitcoins, em razão da natureza do sistema, os bitcoins são inseparáveis do registro da *Blockchain*; ou seja, eles nunca saem dela. Portanto, uma carteira de bitcoins é onde se armazena as credenciais digitais que permitem o uso de bitcoins. Explica-se. Como o Bitcoin usa criptografia de chave pública, na qual duas chaves criptográficas são geradas (uma pública e uma privada), a carteira bitcoin é como se fosse um chaveiro onde essas chaves ficam armazenadas.

Por outras palavras, tecnicamente é incorreto dizer que uma careteira (*wallet*) armazena ou guarda bitcoins, pois os bitcoins só existem na cadeia de blocos da rede Bitcoin (*Blockchain*). O que efetivamente é armazenado nas carteiras são apenas os pares de endereços ou de chaves (pública e privada).

Outro detalhe, as bitcoins não são enviadas para uma carteira, não saem de uma carteira e nunca estiveram e nem estarão numa carteira. As bitcoins saem de endereços Bitcoins (chaves públicas) e são enviadas para outros endereços Bitcoins (chaves públicas). Na tentativa de quererem serem didáticos, muitos utilizam o termo carteira dando a falsa ideia de que as bitcoins estão salvas dentro delas. Quando utilizamos a expressão “conta” não estamos nos referindo ao porta chaves ou chaveiro (carteira Bitcoin), mas sim ao registro existente dentro da *Blockchain* (cadeia de blocos), que é identificado pelo endereço Bitcoin (chave pública). As carteiras Bitcoin são mais semelhantes aos terminais de autoatendimento dos bancos; ou seja, são simplesmente formas de acesso à conta e não a conta propriamente dita.

A grosso modo, encriptação é o processo de transformação de dados (arquivos ou informação) num formato inacessível, ininteligível, incompressível e/ou imodificável para terceiros; já a decriptação (operação inversa da encriptação) é o desfazimento da encriptação, ou seja, a restauração do arquivo ao seu formato original.

Numa carteira Bitcoin, uma das **chaves** (meio de cifrar e decifrar), a pública (***public key***; que toda a comunidade Bitcoin pode verificar na *Blockchain*), é o endereço Bitcoin (*Bitcoin address*) pelo qual se recebe pagamentos; a outra chave, privada (***private key***), é a que somente seu dono

conhece (daí seu nome), vez que é a usada (assinatura digital) para ordenar pagamentos. Como o sistema de encriptação é assimétrico (uso de par de chaves ou criptografia de chave pública), apesar das chaves serem diferentes, elas são matematicamente ligadas, formando um par exclusivo (casamento monogâmico, fidedigno e eterno). Desse modo, para cada endereço criado (chave pública), existe uma única e exclusiva chave privada associada a ele. Pode-se fazer a analogia de um cadeado com uma combinação única e sua chave exclusiva; assim tal como uma fechadura numa porta de vidro à prova de balas, as pessoas podem ver o que tem dentro, mas não conseguem entrar ou acessar se não tiverem a chave exclusiva para abrir a porta.

Outra analogia é que a chave pública é semelhante às informações bancárias necessárias para efetuar um depósito (nome do banco, número da agência, tipo de conta e o número da conta bancária) e a chave privada, é semelhante à senha de referida conta bancária. E, a *Blockchain*, seria similar ao banco onde a pessoa tem conta e estão guardados os seus créditos.

Ressalta-se que a chave pública é criada a partir da **chave privada**. Para cada endereço Bitcoin (chave pública) criado, existe uma única e exclusiva chave privada associada a ele, que seria o equivalente a uma "senha". A chave privada é obrigatória para que se possa fazer (assinar) transações gastando os Bitcoins relacionados ao endereço associado a ela. As chaves privadas dos endereços geralmente são representadas através de uma sequência aleatória de números e letras maiúsculas e minúsculas. Uma chave privada tem 51 a 52 caracteres de comprimento e inicia com 5 (cinco), L ou K.

Detalhe, uma chave criptográfica de nada serve sem a outra; ou seja, tal como achar uma chave metálica (ou uma senha) não servirá para nada se não souber onde ela deve ser usada. Mas não é por essa razão que se pode correr risco de divulgar a chave privada; pois a descoberta da respectiva chave pública correspondente (que não é tão difícil) é muito mais fácil se saber a quem pertence. E, mesmo não sabendo a chave pública e nem a quem ela pertence, não é impossível descobrir onde a chave privada serve; nem que for através da tentativa e erro (*brute force*), tal como alguém que sai

testando uma chave metálica em todas as fechaduras para descobrir de qual porta é.

Por essa razão a carteira em papel possui o inconveniente de mostrar de uma só vez as duas chaves juntas. Tal como um cartão bancário que não deve ter a senha anotada junta ao mesmo, as carteiras Bitcoin em papel, por medida de segurança, devem separar as chaves para serem guardadas em locais diferentes.

Ressalta-se que a criação da carteira deve ser feita exclusivamente pelo próprio interessado. Jamais poderá ser feita através de outra pessoa ou com alguém assistindo. Explica-se. A pessoa que gera o endereço Bitcoin tem conhecimento prévio da chave privada (a senha necessária para gastar os Bitcoins). Desse modo, se não foi o próprio usuário que gerou o seu endereço Bitcoin (chave pública), ele precisa confiar muito na pessoa ou empresa que fez isso para ele; ou seja, de que esse intermediário não usará a chave privada se apropriar de seus Bitcoins.

O Endereço Bitcoin ("Bitcoin Address"), que é a **chave pública**, funciona como se fosse a identificação de uma conta bancária (nome do banco e os números da agência e respectiva conta) e, assim, é utilizado para receber (crédito) ou enviar (débito) Bitcoins que estão armazenados na *Blockchain* (que funciona como se fosse o banco). Portanto, para poder receber Bitcoins, o beneficiário só precisa fornecer sua chave pública; já para poder efetuar pagamentos, além de precisar identificar de onde sairão os valores, o pagador precisa utilizar a chave privada (que funciona como uma senha bancária ou uma assinatura digital) para poder concretizar a operação. Detalhe, através do Endereço Bitcoin, qualquer pessoa consegue visualizar na *BlockChain* todas as transações envolvendo dito endereço. Tomemos, por exemplo, endereço bitcoin do The Pirate Bay: 129TQVAroeehD9fZpzK51NdZGQT4TqifbG.

O endereço de Bitcoin funciona de modo semelhante ao e-mail. Qualquer pessoa pode enviar ao destinatário; ou seja, o destinatário pode receber de qualquer pessoa. Entretanto, para que se possa enviar algum e-mail dessa conta, é indispensável fornecer a senha de acesso e somente o titular a sabe e possui.

O endereço Bitcoin (chave pública) serve como identificação do remetente (quem está pagando) e do destinatário (quem está recebendo) das transações Bitcoins.

Quando se fala em manusear (receber ou enviar) Bitcoins, por óbvio, também está se referindo às suas frações; ou seja, aos satoshis, que são os centavos do Bitcoin.

Ao serem gerados, os endereços Bitcoins (chaves públicas) não são incluídos na cadeia de blocos (*Blockchain*) da rede Bitcoin. O novo endereço (recém-criado) só será adicionado à cadeia de blocos quando fizer parte de alguma transação como destinatário, na qual receberá Bitcoins que estejam vinculados a um endereço remetente. Por outras palavras, na *Blockchain* os endereços Bitcoins somente aparecem pela primeira vez quando estão sendo beneficiados com alguma transação; é como se fosse o depósito inaugural que termina o procedimento de abertura da conta bancária e a ativa. Antes desse evento, não há nenhuma razão para constar na *Blockchain* um endereço Bitcoin que não possua crédito nenhum; mas depois que já fez parte da *Blockchain*, os endereços Bitcoins nunca mais saem, nem mesmo estando sem nenhum crédito. E, detalhe, não existe possibilidade de constar na *Blockchain* algum endereço Bitcoin (conta) com saldo negativo; vez que a rede Bitcoin não concede financiamento, empréstimo, limite de crédito ou cheque especial. Já em relação ao pagador, obrigatoriamente, ele deve ter seu endereço inscrito previamente na *Blockchain* e constar saldo suficiente para poder efetuar o pagamento; caso seja a primeira transação do pagador, ele deve antes providenciar um depósito inaugural em seu endereço.

Pelo fato de ser possível existirem endereços bitcoins sem qualquer vinculação ou associação de bitcoins a eles, até mesmo de forma eterna, é possível gerar os pares de chaves em dispositivos *off-line* (desconectados ou sem conexão à Internet). Esse procedimento de geração offline oferece maior segurança, pois as chaves privadas são criadas e armazenadas sem qualquer contato com um dispositivo online, que possa estar sujeito a ataques de *hackers*.

O site http://www.bitaddress.org é um gerador de endereços Bitcoin que permite criar e ver as chaves pública e privada.

Se a chave privada for perdida, a rede Bitcoin não irá fornecer nenhum método de recuperação de senha ou de acesso e nem reconhecer nenhuma outra evidência de propriedade, com o que as bitcoins vinculadas à dita chave privada ficarão bloqueadas (inacessíveis ou inutilizáveis) na *Blockchain* (cadeia de blocos). Por essa razão é recomendável a criação de *back-up* (cópia de segurança) da chave privada para ser salvo num pendrive exclusivo, de preferência virgem (sem nunca ter sido usado e que nunca tenha sido conectado a um computador com acesso à Internet) e/ou na nuvem (*cloud*).

Provavelmente, a forma mais segura de proteger os Bitcoins é armazenar as chaves num dispositivo *air gapped* (sem conexão com à Internet).

Algumas carteiras Bitcoin possuem o recurso de realização de *back-up* ou exportação da chave privada (normalmente localizada no arquivo "wallet.dat"); bem como de código mnemônico para evitar a perda do acesso à chave privada.

Para conseguir os primeiros satoshis ou bitcoins é através de compra em *exchange*, vendendo algo, efetuando algum serviço, recebendo em doação, comprando diretamente de outro particular, ganhando de sites da Internet ou através do processo de mineração.

A *wallet* (carteira) Bitcoin será como uma agência bancária virtual pela qual o usuário pode fazer transferências, saques, depósitos e consultar o extrato (resumo de transações) e o saldo.

É possível checar o saldo a qualquer momento, sem se expor a qualquer risco, simplesmente consultando o endereço púbico na *Blockchain* (que está reproduzido em vários sites clones).

- http://www.bitcoinpt.com/address-balance.

Pelo site http://www.bitcoinpt.com/valid-address é possível verifique se um endereço de bitcoin é real ou válido (*Valid Address Checker*).

Para criar uma carteira ("wallet") para recebimentos, vendas, compras ou trocas de bitcoins no Brasil, é recomendado utilizar um site brasileiro, como, por exemplo: https://www.mercadobitcoin.net. Criada a conta, você pode comprar Bitcoins com dinheiro ou transferir de suas minerações, utilizando o código de sua conta.

Para poder participar da comunidade Bitcoin (comprar, armazenar e usar o Bitcoin), é necessário ter uma carteira para guardar as chaves de acesso aos créditos. Na verdade, é preciso ter um endereço privado e outro público gerado a partir do primeiro. A carteira é simplesmente o local onde esse par de chaves é salvo, guardado, arquivado ou anotado.

Depois de criada a carteira Bitcoin, ela terá gerado um endereço de Bitcoin (chave pública), mas o usuário poderá criar quantos (ilimitadamente) endereços Bitcoins quiser ou sempre que precisar ou achar conveniente. Pode-se ter uma quantidade "ilimitada" de endereços.

Caso queira receber bitcoins e não possua uma carteira, é possível gerar um par de chaves em https://www.bitaddress.org e futuramente sincronizar em uma carteira qualquer.

Existem **cinco formas de carteiras Bitcoin**: *on-line* (*hot wallet*, *web wallet*, armazenamento quente ou através de sites), *desktop* (*software* em um computador ou *notebook*), móvel (de *smartphone* ou *tablet*), *hardware* (*offline*, *cold wallet*, armazenamento a frio ou física em dispositivos semelhantes a pendrives), em papel (imitando cédulas) e cerebral (*brain wallet*).

- https://bitcoin.org/pt_BR/escolha-sua-carteira;
- https://bitcoin.org/en/choose-your-wallet;
- http://btcfaucet.com/wallets/;
- https://www.bitcoin.com/choose-your-wallet;

- http://pt.wikihow.com/Criar-uma-Carteira-Bitcoin-Online.

Existem vários sites que oferecem **carteiras *online* ou "instawallets"** (carteiras instantâneas); tais como, por exemplos:

- Blockchain wallet (https://blockchain.info/wallet/#/ ou https://blockchain.info/pt/wallet/#/);
- CoinBase (https://coinbase.com/);
- Coinb (https://coinb.in/#wallet);
- Coinverse (https://coinverse.com.br/);
- InstaWallet (http://www.instawallet.org/);
- MyWallet (https://blockchain.info/wallet);
- Xapo (https://xapo.com/pt/);
- CoinJar (https://www.coinjar.com/);
- Coinpunk (https://github.com/kyledrake/coinpunk);
- Coinapult (https://www.coinbase.com/);
- Circle (https://www.circle.com/pt);
- BitGo (https://www.bitgo.com/);
- Bcoiner (https://bcoiner.com/pt/);
- GreenAddress (https://greenaddress.it/en/);
- StrongCoin (https://strongcoin.com/);
- Faucetbox (https://faucetbox.com/en/);
- Epay (https://epay.info/);
- Ripio (https://www.ripio.com/pt/);
- Criptopay (https://cryptopay.me/bitcoin-wallet);
- Ribbit (http://wallet.ribbit.me/);
- Bitbay (https://bitbay.net/).

Com esta opção não é necessário instalar nada no computador, mas a carteira é armazenada nos servidores da empresa; portanto estás a confiar no site a segurança da sua carteira. Por outras palavras, carteira web é a maneira mais fácil e conveniente de usar (pois pode ser utilizada através de qualquer computador, *notebook*, *tablet* ou *smartphone*); contudo, justamente por serem tão flexíveis, é potencialmente menos segura do que carteira de *software* rodada no computador.

Em suma, as *web wallets* costumam ter o inconveniente de o usuário não ser o dono das chaves privadas, com o que se têm o risco do dono do site sumir com as bitcoins.

Muitos sites não exigem CPF, RG, data de nascimento ou cartões de crédito. O cadastro básico apenas pede seu e-mail, uma senha e, na formalização dos termos de compromisso, apenas um nome. Contudo você pode alterar os dados cadastrais mais tarde se preferir.

Para conseguir uma carteira *online* e comprar o primeiro Bitcoin, siga estes passos. Tomando, como exemplo, a Blockchain wallet. Acesse https://blockchain.info/pt/ e clique em "Carteira" na barra de navegação superior. Depois clique no botão verde escrito: "Create A Free Bitcoin Wallet" ou "Criar Uma Carteira Gratuito Bitcoin". Ou, tentar ir diretamente em https://blockchain.info/pt/wallet/#/signup ou https://blockchain.info/wallet/new. Depois, clique em "Criar uma Nova Carteira". Forneça um endereço de e-mail seu e uma senha específica de acesso à carteira online. Selecione o "quadradinho" de aceitação dos termos do serviço ("I have read and agree to the Terms of Service") e clique em "Continue". Você já terá acesso imediato, mas lhe terá sido enviado um e-mail (de no-reply@blockchain.info com o assunto: “Welcome To My Wallet”) com instruções para concluir a instalação da carteira. Lhe será pedido para confirmar o e-mail e lhe terá sido informado o número identificador (ID) da sua carteira.

A partir daqui, usar a carteira é bastante intuitivo. É de extrema importância que ative medidas de proteção como a autenticação em 2 fatores, restrição de acesso pela rede TOR (https://www.torproject.org/) e extensão para o *browser* (navegador). Faça uma cópia de segurança da sua carteira para caso de acontecer alguma coisa ao site, desta forma garante que terá sempre acesso à sua carteira e as suas moedas estarão sempre disponíveis.

A vantagem do portfólio web é que você pode usar a mesma conta em vários dispositivos carteira. Algumas pessoas também se sentir menos ansioso quando a segurança do seu dinheiro é gerida por outra pessoa, e quando você não tem que se preocupar em perder suas moedas se algo

acontecer com seu telefone. A desvantagem é que alguém está segurando o seu dinheiro para você com um portfólio web, o que significa que você tem que confiar neles para manter a segurança e disponibilizá-lo sempre que quiser, e se você tiver um aplicativo armazenado localmente você tem controle total sobre suas finanças de você.

Na carteira híbrida (exemplos: StrongCoin e *Blockchain*), a chave privada é encriptada no *browser* (navegador da Internet) antes de atingir o servidor da carteira online, com o que ele apenas possui a chave privada criptografada e, assim, não tem como manusear os bitcoins da conta do usuário. Já se a carteira não for híbrida, não será segura, porque o servidor terá acesso à chave privada do usuário; com isso qualquer funcionário ou um *hacker* pode ter acesso à chave privada desprotegida e furtar os Bitcoins vinculados a ela.

Quem controla as chaves, controlar o bitcoin. A posse das chaves é a propriedade do bitcoin.

A carteira on-line fornecida pela Xapo (https://xapo.com/) é uma das mais usadas no Brasil muito provavelmente porque alguns *faucets* dobram os ganhos do usuário que encaminhar seus satoshis para uma carteira deles, ou seja, uma quantidade grande de novos usuários conseguem suas primeiras frações de bitcoin através desse tipo de site e acabam usando os serviços da Xapo.

De forma semelhante, existem as **carteiras móveis**. Detalhe, muitas carteiras móveis também são online ou para desktops.

- Breadwallet (https://breadwallet.com/);
- Greenaddress (https://greenaddress.it/en/);
- Bitcoinwallet (https://bitcoinwallet.com/);
- Circle (https://www.circle.com/pt);
- Uberpay (http://uberpay.io/);
- BX Wallet (https://bx.in.th/wallet/);
- Micélio (https://wallet.mycelium.com/)
- Airbitz (https://airbitz.co/);
- Xapo (https://xapo.com/pt/wallet/);

- Copay (https://copay.io/);
- Bither (https://bither.net/);
- Wirex (https://wirexapp.com/pt/);
- Coinverse (https://coinverse.com.br/);
- Coinjar (https://www.coinjar.com/).

Existem aplicativos disponíveis para dispositivos com Android e aparelhos iPhone. Entre as carteiras para Android, as mais tradicionais são Blockchain Wallet, Mycelium, Xapo e Bitcoin Wallet. Já para celulares com iOS, as mais famosas são a Blockchain Wallet, Mycelium e Xapo. E as escolhas mais populares são Airbitz (Android, iPhone), Breadwallet (iPhone) e Andreas Bitcoin Wallet (Android).

- http://pt.oggiline.com/tecnologia/a-melhor-wallet-bitcoin-para-celulares-e-tablets-android.php;

- https://www.bitcoinnews.com.br/bitcoinbrasil/review-das-carteiras-bitcoin-para-iphone/.

Para facilitar uma pesquisa de carteiras bitcoins para *smartphones* (celulares) e/ou *tablets*, se o sistema operacional do dispositivo for Android, ao invés de procurar pelo Play Store no próprio *smartphone* ou *tablet*, basta acessar pelo computador o site do Google Play, clicar na aba/guia Apps e digitar os termos de pesquisa; tais como, por exemplos: carteira bitcoin, carteira multicoin, carteira altcoin, bitcoin wallet, wallet multicoin e wallet altcoin.

- https://play.google.com/store/apps.

Executar o cliente Bitcoin tem algumas vantagens em relação a uma *instawallet*. Em primeiro lugar, ao executar o cliente Bitcoin, essencialmente, a pessoa terá seu próprio banco e não irá depender de terceiros para ter acesso aos seu Bitcoins. O cliente Bitcoin, quando totalmente criptografado, é muito mais seguro do que confiar na segurança de um site ou indivíduo. Além disso, executando o cliente Bitcoin estar-se-á colaborando no funcionamento da rede ao fortalecer, tanto a sua velocidade e, até certo grau, a sua segurança. A grande desvantagem de executar o cliente Bitcoin é que com o tamanho atual da *Blockchain*, dependendo da conexão à Internet, irá demorar horas e, até mesmo, dias para fazer o

download completo da cadeia de blocos (*Blockchain*) do Bitcoin; vez que a *full Blockchain* conta com, no mínimo, 447,522 blocos (*last block* [último bloco] ou *total blocks* [blocos totais]), totalizando mais de 90 GB (noventa gigabytes) de dados. Explica-se. Quando consultamos eram 97.492 MB. Recorda-se que como cada gigabyte possui 1.000 (mil) megabytes, são, na verdade, 97,492GB.

- https://blockchain.info/charts/blocks-size;
- https://www.smartbit.com.au/charts/blocks-total.

Uma forma de agilizar o *download* da *Blockchain* completa é, em vez de sincronizá-la bloco por bloco, fazer o *download* da *Blockchain* de uma só vez e importá-la separadamente sob o diretório de dados do Bitcoin Core. Para isso deve-se baixar e instalar o Bitcoin Core (https://bitcoin.org/pt_BR/download). Depois deve-se abri-lo e deixá-lo funcionando por alguns segundos e fechá-lo. Após isso, deve-se fazer o *download*, via Torrent, do arquivo *blockchain* ou do Bootstrap Bitcoin (pesquise no Google). Depois abre-se o Explorer do Windows e vai até a pasta localizada em C:\Users\SEUNOME\AppData\Roaming\Bitcoin ou C:\Usuários\SEUNOME\AppData\Roaming\Bitcoin. Essa pasta pode estar em uma partição diferente caso o usuário tenha instalado o Windows em uma partição diferente do drive C. Por óbvio a pasta “SEUNOME” trata-se do nome de usuário de quem utiliza o referido computador. Na pasta Bitcoin deve-se deletar (apagar) o arquivo de log existente dentro da subpasta "database"; talvez o nome dele seja "log.0000000001", mas pode-se apagar tudo que tem nessa pasta "database". Então seleciona e copia o arquivo "bootstrap.dat" que foi baixado e o cola dentro da pasta "Bitcoin" (ou seja, "C:\Users\SEUNOME\AppData\Roaming\Bitcoin"). Por último abre-se o Bitcoin Core e ele irá começar a sincronizar a carteira. No rodapé da carteira vai aparecer "Sincronizando com arquivos do disco local" ou algo assim. Isso não irá proporcionar uma sincronização offline de 100% porque a *Blockchain* não para de crescer, mas irá adiantar cerca de 97% de seu tamanho. Depois de importar (puxar) os dados do arquivo do computador, o programa Bitcoin Core irá terminar a sincronização através da rede própria do Bitcoin.

Ainda há a opção do "FastCoin BlockChain" que promete tornar a sincronização da *blockchain* mais rápida (http://www.fastcoin.ca/downloads.html).

Existem também aplicações que funcionam de forma semelhante ao cliente Bitcoin de referência, mas não exigem o *download* da *Blockchain*. Assim, é possível usar uma carteira leve como o Multibit (https://multibit.org/) ou o Electrum (https://electrum.org/#home). Por outras palavras, um longo período de sincronização só é necessário quando se utiliza clientes de nó completo como o Bitcoin Core. Tecnicamente falando, sincronização é o processo de *download* e verificação de todas as transações que já passaram pela rede Bitcoin.

Detalhe, utilizar a versão mais recente do *software* ou aplicativo Bitcoin permite o recebimento e a instalação de eventuais correções estáveis e seguras; as quais podem prevenir problemas de várias severidades e, ainda, disponibilizar novas funcionalidades e manter a carteira segura.

A https://btcflex.com/ é uma espécie de poupança de Bitcoin.

Carteiras *software* são baixadas e rodadas a partir de um computador. Elas são consideradas mais seguras, porque os usuários têm mais controle e não depende de serviços de terceiros. O método tradicional é conhecido como "execução de um nó completo" e consiste em executar um programa no computador que mantém um registo de todas as transações Bitcoin que já ocorreram (a *Blockchain*); o que leva várias horas e, até mesmo, dias para a conclusão, antes de poder efetuar qualquer transação.

Existem, também, aplicações que funcionam de forma semelhante ao cliente Bitcoin de referência, mas não exigem o *download* da *Blockchain*. Assim, é possível usar uma carteira leve como o Multibit (https://multibit.org/) ou o Electrum (https://electrum.org/#home).

Para alguns clientes de Bitcoin, para poder calcular o saldo da carteira de Bitcoin e realizar novas transações, é necessário que a cópia da *Blockchain* seja atualizada antes.

Portanto, existem dois tipos de **carteiras *desktop***: 1) core (cliente Bitcoin, nó completo ou *full node*) que fazem o *download* completo do teor da *Blockchain* (arquivo gigantesco) e mantêm essa cópia sempre atualizada e sincronizada; e, 2) simples (SPV - *Simplified Payment Verification*, *thin clientes* ou leves), que usam uma versão mais leve da *Blockchain* e não verifica a cadeia de blocos, mas somente usa os cabeçalhos dos blocos.

- MultiBit (https://multibit.org/);
- Bitcoin Core (https://bitcoin.org/pt_BR/download);
- Electrum (https://electrum.org/);
- mSIGNA (https://ciphrex.com/products/);
- Wirex (https://wirexapp.com/pt/);
- Armory (https://www.bitcoinarmory.com/);
- Bither (https://bither.net/).

Bitcoin Core ou BitcoinQT (Bitcoin-Qt foi rebatizada para Bitcoin Core desde a versão 0.9.0), é um *software* para carteiras que funciona nos sistemas operacionais Windows, Mac e Linux. Foi o primeiro aplicativo de carteira criado e, além disso, é um dos mais seguros. Ele também é um dos que possui uma das memórias mais intensivas. Ele, ainda, usa sempre um novo endereço a partir de um *pool* (piscina) de chaves para uma melhorar a privacidade. Confira os verbetes BitcoinQT e Bitcoin Core no glossário.

- http://www.bitcoin-en.com/install-bitcoin-qt-faster.html;
- https://bitcoin.org/pt_BR/download.

O Multibit (https://multibit.org/) é dos *softwares* de carteira mais fáceis de se utilizar. Além disso, suporta vários idiomas e, assim como o Bitcoin Core (https://bitcoin.org/pt_BR/download), roda em Windows, Mac e Linux.

O Electrum (https://electrum.org/) foi desenvolvido para funcionar de forma rápida e com bastante facilidade. Assim como o Multibit, ele também roda no Windows, Mac e Linux. Porém, apresenta um diferencial: ele também funciona em dispositivos que possuem o Android como sistema operacional.

A Bitcoin Wallet (https://bitcoinwallet.com/) foi desenvolvida para funcionar em dispositivos móveis que utilizem a tecnologia Android ou Blackberry como sistemas operacionais.

Já o Armory (https://www.bitcoinarmory.com/) é um *software* que é voltado para usuários bem sérios. Ele apresenta várias formas de realizar o *backup*, o encriptamento das transações e, ainda, armazena os registros de transação no modo *offline*. Funciona apenas no Windows, MacOSX, Ubuntu e Raspberry Pi.

Existem carteiras bitcoin com uma única assinatura e as de **multi-assinatura** (*multisig*, *multi-signature*, determinística (ou seja, não aleatória), *HD Wallet* ou P2SH - *pay-toscripthash*), que funcionam de forma semelhante às contas correntes conjuntas (usadas por casais, sócios, diretores de uma pessoa jurídica, comissões de formatura, etc.) que exigem mais de uma assinatura. Desse modo, nas carteiras multi-assinatura são necessárias duas ou mais chaves privadas que, comumente, estão em poder de pessoas diferentes. Os endereços (chave) públicos criados por uma carteira *multi-signature* começam sempre com o número 3.

- BitGo (https://www.bitgo.com/);
- Copay (https://copay.io/);
- GreenAddress (https://greenaddress.it/en/);
- Arsenal (https://www.bitcoinarmory.com/);
- Blocktrail (https://www.blocktrail.com/);
- Coinbase (https://support.coinbase.com/customer/portal/articles/1743782-what-is-the-multisig-vault-).

O procedimento de uma carteira multi-assinatura é o seguinte. Qualquer um dos co-titulares dos bitcoins (integrante da carteira *multisig*) efetua o procedimento normal de uma transação e a assina, só que ao invés dessa requisição de pagamento ser enviada à rede Bitcoin para processamento (como ocorre numa carteira simples), essa ordem (requisição) é interpretada como sendo uma mera proposta que deve ser enviada a todos os demais co-proprietários (sócios ou co-titulares). Desse modo, assim que algum co-

titular faz uma requisição de pagamento, uma notificação será emitida para todos os outros integrantes da referida multi-assinatura, constando nela todos os dados referentes à transação proposta (quem propôs a transação, quantidade de bitcoins envolvida, qual é o endereço público favorecido [beneficiado ou recebedor], quais sócios ou co-diretores já aprovaram e/ou rejeitaram, etc.). Diante dessa votação, se for atingido o *quórum* (quantidade) mínimo de aprovações pré-configuradas (100%, 2 de 3, 3 de 5, 4 de 8 ou x de x), automaticamente, a mera proposta passa a ser considerada uma transação e será efetivamente transmitida à rede Bitcoin para ser processada (validada por um minerador e adicionada a um novo bloco na *Blockchain*). Caso contrário (se não for atingido o *quórum* mínimo de aprovação), a proposta é rejeitada, arquivada com esse *status* (condição, situação) e não será enviada à rede Bitcoin.

Outro uso interessante da multi-assinatura é o próprio titular ser as 3 das 2 aprovações necessárias. Explica-se. O próprio titular pode-se ter uma das assinaturas no computador, outra no *smartphone* e uma terceira num tablete ou em outro dispositivo. Assim estar-se-á dificultando que alguém acesse indevidamente uma de suas assinaturas em um de seus dispositivos ou lhe coaja (obrigue) a efetuar uma transação contra a sua vontade num desses aparelhos. Lembre-se que o procedimento de transferência na carteira multi-assinatura é interpretado como mera proposta de pagamento a ser aprovada pelos demais.

Uma excelente utilidade para a carteira multi-assinatura, na configuração 2 de 3, é no serviço de *escrow* (terceiro garantidor, terceiro depositário, ente fiduciário, juízo arbitral, conta controlada ou conta de garantia); ou seja, quando duas partes contratantes querem se prevenir de desentendimentos, divergências, pendências, atritos, conflitos ou má fé, elegem um terceiro de confiança comum de ambos para ser o julgador de eventual divergência, desavença, disputa ou lide. Procedimento similar é adotado no site do Mercado Livre (ou Mercado Pago) onde este intermediador de vendas pergunta ao comprador se ele recebeu o produto e se este está de acordo com o divulgado, contratado ou esperado e, assim, se pode ser liberado o pagamento ao vendedor.

- https://www.mercadopago.com.br/ajuda/compra-garantida_521.

As carteiras determinísticas (não aleatórias) são a versão mais leve (espaço em disco), pois nelas a *Blockchain* não é baixada; elas mantêm somente os registros das transações e acessam a rede através de um servidor. Outra vantagem desse tipo de carteira é que as chaves privadas podem ser restauradas em outro dispositivo tento somente a "semente" (*seed*). Todas as chaves privadas são derivadas da semente, manter a semente segura (*backup*) é fundamental.

Uma ***wallet offline***, também conhecida como *cold storage* (armazenamento frio), provê alto nível de segurança; vez que armazena a carteira em local protegido desconectado da rede (Internet). Quando feito corretamente, pode oferecer uma boa proteção contra vulnerabilidades de computadores. É possível assinar uma transação *offline*. Este processo envolve dois computadores compartilhando algumas partes da mesma carteira. O primeiro deve estar desconectado da Internet. É o único que contém a carteira completa e é capaz de assinar transações. O segundo computador fica conectado à internet, mas só tem a função de criar transações não assinadas. As etapas são criar e assinar a transação no computador que está *online* e salvar no USB. Depois enviar a transação assinada com o computador online. Como o computador que está conectado à Internet não pode assinar transações, fica impossível transferir Bitcoins por ele, mesmo que esteja infectado.

- https://bitcoinarmory.com/tutorials/armory-advanced-features/offline-wallets/.

Um computador que não está conectado à Internet não pode assinar transações; sendo impossível transferir Bitcoins por ele, mesmo que esteja infectado. O serviço Armory pode ser usado para assinar transações *offline* (https://bitcoinarmory.com/tutorials/armory-advanced-features/offline-wallets/).

As **carteiras *hardware*** são mais seguras porque não expõem as chaves privadas para a rede. Estes pequenos dispositivos (semelhantes a pendrive USB ou cartão de memória) foram projetados para serem somente uma carteira de moeda criptográfica, nada mais que isso. Como não são pendrives ou HDs externos, nenhum *software* pode ser instalado nelas,

fazendo com que sejam altamente seguras contra vulnerabilidades de computadores e ladrões *on-line*. Elas permitem *backups* e, assim, é possível recuperar os fundos caso ocorra a perda do dispositivo.

- Pi Wallet (http://www.pi-wallet.com/);
- BitSafe (http://www.butterflylabs.com/bitcoin-hardware-wallet/);
- Trezor (http://bitcointrezor.com/ ou https://www.buytrezor.com/);
- Mycelium (https://mycelium.com/);
- Keepkey (https://www.keepkey.com/);
- Opendime (http://www.opendime.com/);
- CoolWallet (https://coolbitx.com/coolwallet/);
- Digital Bitbox (https://digitalbitbox.com/);
- Bitlox (https://www.bitlox.com/);
- BlochsTech (http://www.blochstech.com/);
- Case (https://choosecase.com/);
- EliptiBox (http://www.eliptibox.com/);
- Bitseed (https://bitseed.org/);
- Bitsafe (http://www.butterflylabs.com/bitcoin-hardware-wallet/);
- Walltime (https://cold.walltime.info/);
- Ledger (https://www.hardwarewallet.com/, https://www.ledgerwallet.com/ E http://www.ledger.co/#products).

A empresa BTChip (http://btchip.com/), depois de desenvolver e lançar uma carteira *hardware* USB de Bitcoin, nomeada de HW.1 e baseada em cartões inteligentes (*smart cards*), se fundiu com a empresa GreenAddress (https://greenaddress.it/en/), que conta a funcionalidade de multi-assinatura (https://www.hardwarewallet.com/).

Detalhe, muitas das carteiras online e das moveis (para *smartphones* e *tablets*), fornecem cartões Bitcoin (*Bitcoin cards*) de débito e até de crédito.

- https://cryptopay.me/bitcoin-debit-card;
- https://www.bitcoin.com/bitcoin-card;

- https://bitplastic.com/;
- https://www.e-coin.io/;
- https://xapo.com/pt/card/;
- https://wirexapp.com/pt/;
- http://advcash.com/en/;
- https://anxpro.com/pages/card.

O Cryo Cartão Cold Storage (https://www.cryobit.co/pt/cold-storage-products/cryo-card/) é uma espécie de carteira de papel (*paper wallet*), mas no formato de cartão bancário e feito de material rígido (ao invés de papel). Também existia o Versocard que era feito de plástico (https://versocards.com/).

- https://letstalkbitcoin.com/review-verso-cards;
- https://bitcoinmagazine.com/articles/verso-unboxing-usage-1395713243.

Os cartões físicos Prypto (https://prypto.com/?pg=qLS1s6rPyeLp5g), apesar do formato de cartão de bancário, é uma mistura de carteira de papel (*paper wallet*) com raspadinha. Através do site http://cryptoscratchcards.com/payment.php é possível resgatar os códigos Prypto para qualquer carteira de destino ou usar o código Prypto diretamente em um *Merchant web site* (https://prypto.com/merchants/?pg=qLS1s6rPyeLp5g).

A **carteira de papel** (*paper wallet*) é um documento impresso que contém cópias das chaves públicas e privadas que compõem a carteira. Normalmente possui código QR para facilitar o adicionamento das chaves em uma carteira de *software* para fazer uma transação. O benefício de uma carteira de papel é que as chaves não são armazenadas digitalmente em qualquer lugar e não estão, portanto, sujeitas a ataques cibernéticos ou falhas de *hardware* ou de *software*. A desvantagem de uma carteira de papel é que o papel é relativamente frágil e a tinta pode desbotar; além do que se deve mantê-la bem longe do fogo e da água. E, por óbvio, se perder a carteira de papel, não será possível acessar mais os Bitcoins.

- BitcoinPaperWallet (https://bitcoinpaperwallet.com/);
- Bitadress (https://www.bitaddress.org/);
- WalletGenerator (https://walletgenerator.net/).

O site https://walletgenerator.net/ suporta 117 moedas: 42coin, Acoin, Alphacoin, Animecoin, Anoncoin, Apexcoin, Auroracoin, BBQcoin, Bitcoin, BitcoinDark, Birdcoin, Blackcoin, BlackJack, BunnyCoin, CanadaeCoin, CannabisCoin, Capricoin, CassubianDetk, CashCoin, Catcoin, Corgicoin, CryptoBullion, CryptoClub, Cryptoescudo, Dash, DeafDollars, Devcoin, Digitalcoin, Dogecoin, DogecoinDark, eGulden, eKrona, Emercoin, EnergyCoin, Fastcoin, Feathercoin, Fibre, Fluttercoin, Freicoin, FUDcoin, Fuelcoin, Fujicoin, GabenCoin, GlobalBoost, Goodcoin, GridcoinResearch, Gulden, Guncoin, HamRadioCoin, HTML5Coin, HyperStake, ImperiumCoin, IncognitoCoin, Influxcoin, IridiumCoin, iCash, iXcoin, Judgecoin, Jumbucks, Latium, Litecoin, LiteDoge, MagicInternetMoney, Magicoin, Marscoin, MarteXcoin, MasterDoge, Mazacoin, Megacoin, MobiusCoin, MonetaryUnit, Monocle, MoonCoin, Myriadcoin, NameCoin, Neoscoin, Novacoin, Nubits, Ocupy, Omnicoin, Onyxcoin, Paycoin, Pandacoin, ParkByte, Pesetacoin, PHCoin, PhoenixCoin, Peercoin, Potcoin, Primecoin, Quark, Reddcoin, Riecoin, Rimbit, Rubycoin, Sambacoin, SecKCoin, SibCoin, SongCoin, SpreadCoin, StealthCoin, Syscoin, Titcoin, TittieCoin, Topcoin, TransferCoin, TreasureHuntCoin, Unobtanium, USDe, Vertcoin, Viacoin, VikingCoin, W2Coin, WankCoin, WeAreSatoshiCoin, WorldCoin, Zetacoin, etc.

Para guardar em segurança os Bitcoins, sugere-se gerar e guardar um endereço totalmente *offline*. Vanitygen é um gerador de endereço Bitcoin personalizado. Alternativamente, Vanitygen pode ser usado para gerar endereços aleatórios *off-line*. Trata-se de um programa simples, *open source*, que roda no *prompt* de comando do Windows ("C:\Windows\system32\cmd.exe") ou pode ser usado online (https://vante.me/#!/order/start). Para gerar endereços bitcoin *off-line*, deve-se fazer o *download* do Vanitygen e salvar o vanitygen.exe num pendrive.

- https://github.com/search?q=Vanitygen;
- https://github.com/samr7/vanitygen;

- https://github.com/klynastor/supervanitygen.

Depois deve-se copiar o vanitygen.exe do pendrive para o computador que nunca irá se conectar à Internet. No *prompt* de comando do Windows deste computador, deve-se executar o Vanitygen mediante a seguinte linha de comando: "C:/vanitygen/vanitygen.exe 1NOME". Para acelerar o programa, pode-se configurá-lo para não fazer diferenciação de letras maiúsculas e minúsculas apenas acrescentando –i no final (exemplo: vanitygen.exe NOME –i). O resultado poderia ser 1nOMe, por exemplo. O programa vai gerar várias chaves privadas por segundo até que uma delas corresponda a algum endereço que comece com 1NOME. A resposta vem, semelhante ao exemplo abaixo:

```
$ ./vanitygen 1NOME
Difficulty: 5679145
[48165 K/s][total 2080000][Prob 43.1%][50% in 21.2s]
Pattern: 1NOME
Address: 1NOMETh7z3NCDDUSZi4Q9ixy23M9YGVcXbN
Privkey:
5KLUmjZoirgzaDmWbNpyPeNx7DYmfodUNk7FQMmDOaiKZ24fX9o
```

Prosseguindo, deve-se selecionar os dados da janela do *prompt* de comando, copiar e depois teclar Enter. Depois, deve-se colar os dados em algum editor de texto (Notepad, Word, etc.) e imprimir quantas cópias quiser (de preferência, usar a fonte Arial para não confundir o número 1 com a letra l). Assim, quando for gastar ou transferir os Bitcoins, basta importar a chave privada (*privkey*) em alguma carteira online. Após enviar a quantia desejada, sugere-se repassar o restante para outra *paperwallet*; pois na operação realizada foi fornecida a chave privada num computador conectado.

Outra opção é usar o site BitAddress.org (ou LiteAddress.org para a moeda Litecoin). Como a segurança é primordial na criação de uma paper wallet, recomenda-se a criação da carteira totalmente *off-line*. Para deve-se salvar a página do bitaddress.org no computador, clicar com o botão direito do mouse sobre a página e selecione a opção “Salvar como…”. Quando for exibida a janela com a opção de onde salvar o arquivo, selecionar a área de

trabalho e, então, clicar no botão “Salvar”. Em seguida, deve-se desconectar o computador da Internet. Depois disso, deve-se abrir o arquivo “bitaddress.org.html”, que está dentro da pasta salva na área de trabalho, mediante dois cliques sobre ele. A página usa um algoritmo que usa o movimento do mouse e/ou a inclusão de letras, números e caracteres especiais para que os endereços criados sejam o mais randômico possível. Em razão disso, a página espera que o usuário faça alguma aleatoriedade, seja digitando a esmo caracteres no formulário (campo “OR type some random characters into this textbox”) ou movendo o cursor de qualquer jeito pela tela. Será feita uma contagem regressiva do 345 até o zero. Quando a contagem atingir zero, serão mostradas as chaves públicas e privadas e seus respectivos códigos QR (*Quick Response*). Não se deve verificá-los. Existe a opção “BIP38 Encrypt” para proteger a paper wallet com uma senha que deve ser preenchida no campo “Passphrase”; mas algumas carteiras não suportam esse recurso, vez que cada carteira Bitcoin possui um método próprio para importar chaves privadas. Ambos, BitAddress e LiteAddress, dão suporte a chaves privadas através do algoritmo BIP38, mas terá que usar o mesmo site para depois descriptografar a chave privada. Em seguida, deve-se clicar na guia “Paper Wallet” e, no campo “Addresses to generate:” (Endereços para gerar), deve informar a quantidade de endereços a gerar. No campo "Addresses per page" deve-se informar quantos "Endereços por página" serão. Para ser mais simples, informe tudo 1. Se quiser mudar a arte gráfica (aparência, *layout* ou formato), deve-se clicar em “Hide art”. Após a escolha das opções dos formulários, deve-se clicar em “Generate” (Gerar). Por último é só clicar no botão "Imprimir"; de preferência a partir de uma impressora que não esteja conectada a uma rede. Depois que uma *Paper Wallet* foi criada através de um site, é possível ao código do *website* funcionar *offline*. Para carregar (depositar ou colocar saldo) na paper wallet, basta efetuar uma transferência de uma quantidade desejada de Bitcoins (ou satoshis) para o endereço Bitcoin (chave pública) da paper wallet. Após cerca de 30 minutos, pode-se acessar a *Blockchain* e pesquisar o endereço Bitcoin da referida paper para confirmar o depósito realizado. Nas carteiras software, as transações possuem um endereço para "troco" (*change address*), mas no *paper wallet* não. Desse modo, no *Paper Wallet* deve-se informar manualmente o endereço de troco, senão esses créditos ficam perdidos e serão de quem os encontrar; ou seja, de quem achar o bloco.

- http://bestbitcoin.com.br/bitcoin-white-paper-artigo-original-traduzido-para-o-portugues/.

"Load & Verify" é o endereço público da carteira; já "Redeem" é a chave privada.

A *paper wallet* é de uso único; uma vez que importou a chave para alguma carteira online, deve-se descartar e usar uma nova *paper wallet*.

Para os usuários do site da Blockchain.info, na URL https://blockchain.info/wallet/paper-tutorial consta um tutorial.

Para **importar as chaves da paper wallet** para a carteira *software*, no caso a carteira BitcoinCore, no menu superior dele, deve-se clicar em "Ajuda" e selecionar a opção "Janela de depuração". Após a "Janela de debug" abrir, clicar na aba "Console". Se a carteira Bitcoin Core estiver criptografada, será preciso informar a senha dela usando o comando: walletpassphrase "sua senha" 600. Se a senha da carteira possuir espaço(s) é necessário o uso das aspas. O 600 é o período em segundos em que a autenticação será mantida. Depois inserir a linha de comando: importprivkey *ChavePrivada* "Resgate da paper wallet". Substitua a *ChavePrivada* pelos caracteres específicos da chave privada constante da *paper wallet* e substitua "Resgate da paper wallet" pela descrição para a transação na *wallet* (carteira). O comando verificará se a chave privada já foi usada alguma vez na *Blockchain*, isso pode levar aproximadamente 30 minutos. É possível, mas não é recomendável, desativar essa verificação (comando: importprivkey ChavePrivada "Resgate da paper wallet" rescan=false). Se desativar a verificação a informação será fornecida na próxima vez que iniciar o Bitcoin Core através do saldo informado. Após a verificação da chave privada, a transação com o recebimento do saldo da paper wallet constará na carteira.

Armazenado em um lugar seguro, um *backup* completo e atualizado da *wallet* (carteira) pode ser uma proteção contra falhas humanas e dos computadores. Ele também permitirá a recuperação da carteira após ter o dispositivo (*smartphone*, *tablet*, computador, notebook, etc.) furtado, roubado ou inutilizado. Os *backups* devem criptografados e serem feitos

regularmente para constar todas as recentes mudanças e inclusões de endereços Bitcoin; bem como devem ser salvos em locais seguros, em mais de um lugar e em diferentes mídias e formas (*pendrive*, CD, HD externo, nuvem, e-mail, impresso, etc.) para se prevenir de algum infortúnio.

A BrainWallet (https://brainwallet.io/) é uma carteira que usa a **memória humana** para guardar a chave privada; ou seja, a própria pessoa cria uma super senha misturando números, letras e até símbolos. A sua utilização é bastante simples: utiliza-se uma "frase-chave", expoente secreto ou chave privada para gerar um endereço. Se um *brainwallet* não tiver sido revelado a outrem ou anotado em algum lugar e acabar sendo esquecido ou o seu titular morrer, os Bitcoins estarão inacessíveis ante a perda da senha necessária. Por outras palavras, enquanto a senha não é gravada em qualquer lugar e nem revelada a terceiro, ela só existirá na mente de seu titular.

Em relação às altcoins, normalmente nos próprios sites delas existem as indicações das carteiras existentes. Outra forma é pesquisar por aplicativos no Google Play pelo fato da pesquisa ser muito mais fácil, prática, eficiente e rápida do que pelo Google normal. Assim, por exemplo, em relação ao Ethereum, alguma das opções existentes de carteiras são: MIST (https://github.com/ethereum/mist), MyEtherWallet (https://www.myetherwallet.com/) e Jaxx (https://jaxx.io/). Já em relação a moeda Dash (https://www.dash.org/), as melhores carteiras são: Jaxx (https://jaxx.io/), Electrum (https://electrum-dash.org/), Dash Core (https://www.dash.org/downloads/), Dash Wallet para Android e Coinomi (https://coinomi.com/).

Carteira *multi currency*, *multi-coin* ou *multi-cryptocurrency* é aquela que funciona com mais de uma moeda virtual ou criptográfica. Recorda-se que *altcoins*, abreviatura de *Alternative Cryptocurrencies*, são criptomoedas alternativas ao Bitcoin.

Êxodo (https://www.exodus.io/) é carteira desktop multi-ativos com Shapeshift (troca) embutido (http://pt.shapeshift.io/#/coins).

A FrozenBit (http://frozenb.it/) é uma *wallet* multi-coin e multi-assinatura que dá suporte ao Litecoin, Quarkcoin, Bitcoin e Blackcoin.

- https://onename.com/frozenbit;
- https://github.com/frozenbit.

Cryptonator (https://www.cryptonator.com/) é uma carteira on-line Bitcoin tudo-em-um (all-in-one) que suporta múltiplas criptomoedas (cryptocurrencies) como Bitcoin (BTC), Litecoin (LTC), Dogecoin (DOGE), Blackcoin (BLK), DASH, Emercoin (EMC), Paycoin (XPY), Peercoin (PPC), Primecoin (XPM), Reddcoin (RDD) e Vertcoin (VTC).

HolyTransaction (https://holytransaction.com/) é uma carteira criptomoeda universal que trabalha com Bitcoin, Litecoin, Dogecoin, Peercoin, Dash, Ethereum, Gridcoin, Blackcoin e Omni Layer.

BIT.AC (https://bit.ac/) é uma carteira que acomoda e permite a troca instantânea de 14 moedas criptográficas diferentes: Bitcoin, Ethereum, Dash, The DAO, Lisk, Monero, Factom, Dogecoin, Litecoin, Peercoin, Vericoin, Namecoin, Clams, Vertcoin e Novacoin.

Muitas carteiras possuem versão para smartphones e tabletes.

A Coinomi (https://coinomi.com/) é uma carteira multi-coin que suporta Bitcoin, Asiacoin, Auroracoin, Batacoin, Blackcoin, Cannacoin, Canadá ECOIN, Mexilhão, Clubcoin, Traço, Digibyte, Digitalcoin, Dogecoin, EDRCoin, EGulden, Ethereum, Feathercoin, GCRcoin, Gridcoin, Gulden, IXCoin, Jumbucks, Litecoin, Monacoin, Namecoin, Neoscoin, Novacoin, NuBits, NuShares, OKCash, ParkByte, Peercoin, Potcoin, Reddcoin, Richcoin, Rubycoin, ShadowCash, Smileycoin, Solarcoin, Syscoin, Unobtanium, Beira, Vertcoin, Vpncoin, etc.

O aplicativo para smartphone, Coinomi Bitcoin Altcoin Wallet (https://play.google.com/store/apps/details?id=com.coinomi.wallet) é uma multi carteira que suporta as moedas Bitcoin, Asiacoin, Auroracoin, Bata, Blackcoin, Canada eCoin, Cannacoin, Clams, Clubcoin, Dash, Digibyte, Digitalcoin, Dogecoin, EDRCoin, e-Gulden, Ethereum, Feathercoin, GCRCoin, Gulden, IXCoin, Jumbucks, Litecoin, Monacoin, Namecoin, Neoscoin, NovaCoin, NuBits, NuShares, OKCash, ParkByte, Peercoin,

Potcoin, Reddcoin, Richcoin, Rubycoin, Shadocash, Solarcoin, Syscoin, Verge, Vertcoin, Vpncoin, etc. Já a CoinPayments (https://play.google.com/store/apps/details?id=net.coinpayments.coinpaymentsapp) é outra carteira que trabalha com mais de 55 Moedas.

Por fim a recomendação de cautela. Antes de se inscrever em alguma carteira, deve-se consultar as referências para saber se não é um golpe ou se é uma imitação de uma carteira renomada. Diante disso, é recomendável que se confira os comentários das carteiras de *smartphones* antes de instalá-las. Por exemplo, as seguintes carteiras foram denunciadas de serem falsas: OceanCoin desenvolvida por Thuy Nguyen; FastWallet desenvolvida por Cu Pham Van; Cosmo desenvolvida por Hoang Long; TorWal desenvolvida por Chao Ngo; SilverBox desenvolvida por Phong Nguyen Thanh; Silverbox desenvolvida por Thuy Nguyen; etc.

COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?

As transações são registros criptograficamente assinados que reatribuem a propriedade de bitcoins a novos endereços públicos. As transações têm entradas (registros que fazem referência aos mesmos fundos [unidades, créditos ou valores] em outras operações anteriores) e saídas (registros que determinam o novo proprietário das bitcoins transferidas e que serão referenciadas como novas entradas em transações futuras com estes mesmos fundos). Cada entrada deve ter uma assinatura digital criptográfica que desbloqueia os fundos da operação anterior. Somente a pessoa que possui a apropriada chave privada é capaz de desbloquear os respectivos fundos.

Conforme visto no capítulo anterior, através de uma carteira (*wallet*), que pode ser *on-line* (*hot* ou *web*), *desktop* (*software*), móvel, *hardware* (*offline*, *cold*, a frio ou física), em papel ou cerebral (*brain*), se guarda um par de chaves criptográficas (privada e pública), que são utilizadas no manuseio (movimentação) das moedas virtuais.

Ressalta-se que a chave pública é criada a partir da chave privada e, para cada chave pública existe uma única chave privada associada a ela.

A **chave pública (*public key*)**, é o endereço Bitcoin ("Bitcoin address") e serve como identificação da conta (onde os Bitcoins estão armazenados) na *Blockchain* e, assim, é utilizada para receber (onde serão depositados ou creditados os valores) ou para debitar pagamentos efetuados (de onde serão feitas as deduções, abatimentos ou descontos; ou seja, de onde os valores sairão). Portanto, o endereço Bitcoin é utilizado tanto para receber como para realizar pagamentos. Quando o usuário está efetuando um pagamento, ele será o remetente; já quando ele for o recebedor, será o destinatário.

Já a **chave privada (*private key*)**, é como a senha ou assinatura para a movimentação (saques, transferências, pagamentos, etc.) dos créditos, fundos, saldo ou valores existentes em referida conta. Desse modo, portanto, é impossível efetuar uma transação (gastar ou transferir os bitcoins) sem que se saiba e forneça a respectiva e exclusiva chave privada vinculada ao endereço bitcoin (chave pública ou conta). Diante disso, somente pode ser de conhecimento do titular da conta.

Para receber Bitcoins, o beneficiário (destinatário) só precisa fornecer sua chave pública (endereço Bitcoin); já para poder efetuar pagamentos, além de precisar identificar de onde sairão os valores (seu endereço Bitcoin) e para onde serão enviados (endereço Bitcoin do destinatário ou beneficiário), o pagador (remetente) precisará utilizar a sua chave privada (que funciona como uma senha bancária ou uma assinatura digital) para poder concretizar a operação.

- http://tecnogeek.com.br/jornalista-mostra-chave-de-bitcoin-na-televisao-e-e-roubado/;
- http://codigofonte.uol.com.br/noticias/jornalista-mostra-chave-de-bitcoin-na-televisao-e-e-roubado.

O procedimento para efetuar uma movimentação de Bitcoin é através da carteira, onde será dada a respectiva ordem, de modo semelhante ao enviar um e-mail; ou seja, através de uma senha de acesso, serão informados e enviados os seguintes dados: remetente, destinatário e teor (valor). O procedimento é muito semelhante ao envio de um TED (Transferência Eletrônica Disponível) ou DOC (Documento de Ordem de Crédito) e, até mesmo, de um depósito ou transferência bancária convencional.

Uma **transação de bitcoin** é iniciada através do processo de solicitação de transferência de créditos de um endereço (remetente), na carteira do "ordenante", para um endereço beneficiário (destinatário).

No protocolo Bitcoin, portanto, cada transação exige no mínimo três chaves criptográficas:

- Um endereço remetente (chave pública);
- A chave privada do endereço remetente (chave secreta);
- Um endereço destinatário (chave pública).

Em síntese, a transação é iniciada pelo usuário pagador, que, após acessar uma carteira bitcoin onde constam suas chaves de acesso aos blocos

constantes da *Blockchain*, irá informar a quantia de bitcoins que quer enviar e qual é o endereço bitcoin de destino, como se fosse o número de uma conta bancária do destinatário. Para transmitir a transação à rede bitcoin, o usuário precisa apenas conectar-se brevemente à Internet.

- http://g1.globo.com/tecnologia/noticia/2014/02/entenda-como-e-uma-transacao-feita-com-moeda-virtual-bitcoin.html

Os endereços bitcoins, tal como os códigos de barras, podem ser representados por códigos de barra ou QR codes para facilitar a leitura e manuseio.

QR (*Quick Response*) Code é um código de barras em 2D (bidimensional ou duas dimensões), escaneável, no formato de um quadrado cheio de "quadradinhos" pretos e brancos, que pode ser escaneado pela maioria dos aparelhos celulares que têm câmera fotográfica. Esse código, após a decodificação, passa a ser um texto (interativo), um endereço URL, um link, o endereço de um site, um número de telefone, uma localização georreferenciada, um e-mail, um contato ou um SMS. É como um código de barras com outro formato (*layout*).

É possível, ainda, enviar os mesmos bitcoins para mais de uma pessoa ao mesmo tempo, exigindo que elas forneçam autorização conjunta poderem gastarem esses bitcoins no futuro. Assim, o bitcoins são dessas pessoas, mas nenhuma delas tem o direito de usá-los sozinha.

Após o usuário clicar em enviar (ou outro ícone semelhante), a ordem de pagamento (transação) será enviada (*upload*) para a rede Bitcoin para ser acomodada em um bloco. Quando esse bloco for finalizado após a loteria de mineração, a transferência estará finalizada.

Uma transação Bitcoin é uma peça assinada de dados que são transmitidos para a rede e, se válido, acaba em um bloco na *Blockchain*. A finalidade da transação é transferir a propriedade de uma quantidade de Bitcoin para um endereço Bitcoin.

Nos **blocos** existentes na *Blockchain* (cadeia de blocos), constam a identificação dos proprietários atuais dos valores ou créditos. Portanto, além dos Bitcoins possuírem uma numeração identificadora exclusiva (tal como um número serial de um produto ou o número de série de uma cédula), eles contêm a chave pública (como se fosse um cadeado) do atual titular. O protocolo Bitcoin, portanto, processa quantos créditos (bitcoins) cada endereço público (chave pública) possui. Assim, somente quem possui a, respectiva e exclusiva, chave privada pode desbloquear ("abrir o cadeado") e utilizar esses valores. Portanto a posse da chave privada determina a propriedade do bitcoin. Se a chave privada for perdida, a rede bitcoin não irá reconhecer nenhuma outra evidência de posse e, assim, as bitcoins vinculadas àquela chave pública tornar-se-ão inacessíveis eternamente. Desse modo, quando alguém efetua uma transferência de bitcoins, está na verdade transferindo a propriedade deles e, por essa razão, é necessária a lavratura ou averbação dessa transferência de propriedade no currículo (registro) desses bitcoins. Recorda-se que, de modo similar a um casamento civil, o ato envolve publicidade e a possibilidade de qualquer um manifestar algo que impeça o ato. Trata-se da verificação e conferência pelos demais nós da rede P2P (*peer-to-peer*) do Bitcoin, que funcionam como um grupo de tabeliães para fins de validação das transações. Outro detalhe, quando se fala em Bitcoins, não se pode esquecer, mas deve-se ter em mente sempre, que pode se referir a qualquer valor, até mesmo centavos (satoshis) e que Bitcoin é o nome dado aos meros registros de valores (créditos) existentes dentro dos blocos que estão na cadeia de blocos (*Blockchain*). Portanto, um bloco não possui uma quantidade definida de créditos, valores ou bitcoins; vez que os blocos são como meras páginas, cronologicamente sequenciais, de um livro contábil (*Blockchain*) onde se registram entradas e saídas de quaisquer valores. Outro ponto importante, os bitcoins não existem, o que existem são os registros das transações dos bitcoins.

As quantias recebidas (entradas ou depositadas) de bitcoin não se juntam, mas permanecem separadas exatamente como quando foram enviadas para o endereço bitcoin (chave pública). Explica-se. Como os valores depositados na conta são provenientes de um registro em um bloco e como esse bloco permanece intacto até que ocorra alguma transação que envolva algum desses registros; com o que o registro envolvido na nova transação será retificado (anotação de uso em nova transação) e, assim, substituído por um

novo registro em um novo bloco, tal como alguém que recebeu cheques em pagamento e está usando estes cheques de terceiros para fazer seus pagamentos, muitas vezes é preciso pegar mais de um cheque para poder efetuar um pagamento. Em resumo, os valores constam das transações anteriores, as quais estão registradas em bloco(s) anterior(es). E cada nova transação envolve fazer uma referência à uma transação anterior onde existe o crédito necessário para a operação e a inserção dessa nova transação num novo bloco, com o que constará no bloco anterior em questão que aqueles créditos foram utilizados nesta nova transação.

O mecanismo pelo qual as saídas (débito de uma conta em favor de outra conta) de transações anteriores são reutilizadas como entradas para novas transações é semelhante ao depósito bancário de um cheque endossado. Explica-se. O pagador originário emitiu o cheque nominalmente em favor de fulano, mas este, por sua vez, endossou este cheque e o deu em pagamento a beltrano, o qual, por sua vez, também, endossou e deu em pagamento a sicrano e assim sucessivamente. E quando o valor do cheque é maior do que o valor do pagamento, o recebedor dá o troco em cheque em favor do pagador, que em vez de descontar ou depositar, endossa e passa para frente.

Uma **saída** é um montante que foi enviado (via transação padrão) para um endereço Bitcoin, junto com um conjunto de regras para desbloquear o valor de saída. No linguajar (dialeto) do meio Bitcoin, uma saída é chamada de "saída de transação não gasta" ou **UTXO** (*Unspent Transaction Output*). Não deve ser confundida com *Output* (qualquer saída, se passou ou não).

UTXO são créditos enviados (transação) a um usuário, e este beneficiário ainda não os gastou (não efetuou nova transação) com os mesmos créditos.

O procedimento que confere a diferença entre os valores disponíveis em conta (saldo) e os constantes da ordem de pagamento (saída) se denomina "change" (troco). Isso se deve ao fato de que o sistema precisou efetuar uma operação semelhante ao pagar com uma nota de valor maior do que o do débito e, por esse motivo, existe troco (*change*) a receber. Portanto, em havendo troco, o sistema realiza duas saídas: uma para o receptor (beneficiário da ordem de pagamento) e outra para pagar o troco de volta à

carteira do emitente da ordem de pagamento e, para isso, utiliza um endereço de troco (*change address*).

Quando se emite uma **ordem de pagamento** na rede Bitcoin, é como se estivesse preenchendo um cheque, mas antes de ser cumprida a ordem de pagamento, o sistema confere os cheques anteriores que o emitente recebeu para saber se ele tem saldo (fundos) suficientes. Portanto, **UTXO** é simplesmente uma entrada que ainda não foi objeto em uma nova transação (operação) e para poder usar bitcoins em uma nova transação, o sistema precisa localizar uma transação anterior onde existe Bitcoins em favor do atual emitente da ordem de pagamento. Detalhe o sistema pode somar transações anteriores para atingir o montante necessário. É como estivesse usando cheques recebidos de terceiro para efetuar um pagamento. Detalhe, o sistema possui a preferência de usar os registros mais antigos primeiro e de preferir os registros cuja soma mais se aproxime (não ultrapasse muito) do valor necessário. Isso é necessário porque o sistema zera todos os créditos existentes nesses registros anteriores que ele utilizou para cumprir essa ordem de pagamento; ou seja, o sistema não retira desses registros anteriores somente o valor necessário, mas sim retira todos os valores constantes neles e, assim, na enorme maioria das vezes existe troco. Por outras palavras, o Bitcoin "destrói" as moedas velhas e cria uma nova só para pagar o troco. Portanto, após o uso de uma *paper wallet*, em havendo troco, o correto é enviar esse troco para uma nova *paper wallet*, considerando inutilizada a *paper wallet* anterior. Algumas carteiras alteram automaticamente o endereço público após cada transação para proteger a privacidade do usuário. Portanto, quando a saída de uma transação é usada como a entrada de uma outra operação, o valor, preferencialmente, deve ser gasto na sua totalidade. Ou seja, quando for gastar os bitcoins (criar uma transação), deve-se usar todo o valor de uma operação anterior não utilizada e torná-lo a entrada da nova transação. Desse modo, junto com a ordem de pagamento (transação), são enviadas referências, IDs (identificações) ou comprovantes (recibos) das transações anteriores do atual emitente provando-se que ele tem saldo suficiente para a operação e que já não gastou os bitcoins de sua conta. Caso os créditos recebidos (depósitos) já não tenham sido gastos, a transação (ordem de pagamento ou transferência) será efetuada. Se o valor de uma transação de saída exceder o valor das entradas (depósitos) realizadas, a transação será rejeitada; mas se as entradas excederem o valor

das saídas, qualquer diferença de valor pode ser considerada como uma taxa de transação pelo mineiro Bitcoin, que cria o bloco que contém essa transação. Por outras palavras, o minerador fica com o troco de todas as transações do bloco, caso esse troco não tenha sido devolvido ao pagador na transação. E somente é devolvido se o usuário assim previamente exigir. O troco devolvido se torna uma nova UTXO na carteira.

Para calcular de forma convencional o **saldo de uma chave pública**, seria preciso somar todos os blocos da corrente e, para isso, o sistema teria que processar todo o banco de dados (*Blockchain*), que é imenso; por essa razão, ele calcula o "saldo" analisando as transações anteriores. Desse modo, o sistema através da especificação da origem dos créditos efetua uma verificação mais simples, ágil e rápida: procura as transações em que aquela mesma moeda já foi utilizada. Se houver uma transação mais nova do que a especificada e que não dá o direito de uso da moeda para quem a está usando, então ela já foi gasta e não pode ser usada. Portanto, os montantes recebidos (UTXOs) são usados individualmente ou em combinação, mas sempre de forma integral e sem deixar nenhum valor ou crédito no(s) registro(s) anterior(es). Eventual troco (quando não creditado para o minerador) se torna uma nova UTXO na conta ou carteira, seja a mesma ou outra indicada (exemplo, uma recém-criada *paper wallet*). Pode-se, até, numa mesma transação pagar duas pessoas diferentes; ou seja, no endereço do beneficiário ou destinatário informa-se o endereço bitcoin de um credor; já no endereço de troco, coloca-se o endereço de outro credor. Mas desse segundo pagamento não haverá troco, pois se trata do troco do primeiro pagamento.

Quando algum endereço bitcoin (chave pública) recebe um crédito, esse valor passa a ser uma UTXO e estará bloqueado na *Blockchain* até que seu favorecido a desbloqueie (através da chave privada correlata ao endereço público beneficiado em questão) para ser usada em outra transação. Assim que a UTXO é desbloqueada e usada em alguma transação, ela passa a constar como usada e não poderá mais ser gasta. É como se tivesse sido destruída para sempre.

Quando um participante do protocolo (minerador) recebe uma mensagem digital contento uma transação de Bitcoin, ele verifica se a transação é

válida. Isso é feito através da conferência da chave privada (assinatura digital) informada para ver se corresponde à exclusiva (senha) do endereço público (chave pública) onde constam os créditos (bitcoins) que se quer movimentar. A conferência não se limita a verificar a assinatura, a conta e a propriedade dos Bitcoins; mas, também, se existe saldo suficiente e se o usuário já não utilizou os créditos que tinha. Apenas se o resultado for favorável, é que esse nó da rede P2P transmitirá a informação para seus pares (demais nós) e, assim, sucessivamente, em sequência ou em cascata, até a sincronização do banco de dados. Desse modo, em poucos minutos, todos os participantes da rede Bitcoin ficam sabendo que a transação aconteceu.

Em regra, as transações bitcoin são gratuitas. Mas, o usuário, opcionalmente, pode pagar uma pequena **taxa ("fee" ou "rates") em cada transação**. Caso assim faça, sua transação seja processada com maior prioridade pelos mineradores (pois estão recebendo), aumentando a probabilidade de ela ser incluída mais rapidamente na *Blockchain*. Explica-se. Os mineradores podem escolher quais transações eles irão processar e, geralmente, priorizam aquelas que pagam as maiores taxas. Em regra, a cada transação é atribuída uma prioridade, determinada pela idade, tamanho e o número de *inputs*. As taxas de transação, também, servem como forma de proteção contra usuários que enviam transações excessivas para sobrecarregar a rede ("dust spam"). Além disso, as transações com *inputs* não-gastos mais antigos também recebem prioridade. As taxas são baseadas no tamanho de armazenamento da transação gerada, que depende do número de *inputs* (entradas) usados para criar a transação; não tendo nenhuma correlação com o valor que está sendo transmitido. A taxa padrão, depende de carteira para carteira, varia de 0,00001 a 0,0005 bitcoin (BTC) para as transações de baixa prioridade (por cada 1000 bytes da transação; uma transação média é de cerca de 500 bytes) e, ainda, oscila, para mais ou para menos, de acordo com a quantidade de dados que a transação tem. Quanto maior a quantidade de dados, maior será o valor da taxa padrão para manter o mesmo tempo de espera para o processamento da transação. E, de outro modo, se menor a quantidade de dados, menor será a taxa.

- https://en.bitcoin.it/wiki/Transaction_fees;
- https://multibit.org/help/v0.5/help_whatIsTheTransactionFee.html;

- Tutorial sobre a taxa de transferência do Bitcoin - https://www.youtube.com/watch?v=Zoa1WRePHp8.

As taxas de transação são um dos incentivos para que os mineradores continuem executando os "nós" mineradores quando a dificuldade de gerar moedas crescer ou o tamanho da recompensa por resolver um bloco diminuir com o tempo. Os mineradores coletam as taxas de transação associadas a todas as transações incluídas em seu bloco candidato.

Portanto, deve-se lembrar que tal como ocorre com as TEDs e DOCs, além do valor do pagamento em si, há de se acrescer e especificar algum valor de pagamento (taxa) pelo trabalho do minerador que irá processar a operação.

Pagamentos com bitcoin são irreversíveis. Não é possível cancelar ou reverter uma transação, após ela ter sido enviada pela rede. Elas só podem ser reembolsadas voluntariamente pela pessoa que recebeu os créditos.

Os pagamentos Bitcoins são, necessariamente, feitos através da Internet, de forma semelhante as conhecidas transferências *on line* de *home banking*; mas ao invés de ser através de um banco, é por uma carteira (*wallet*) e, no lugar da identificação de banco, agência, conta e identificação do beneficiário, apenas se informa o número Bitcoin onde serão creditados os valores. Para tanto basta digitar manualmente, clicar num link próprio, escanear um QR Code ("Quick Response Code") ou utilizar o NFC ("Near Field Communication"), mediante a simples aproximação física de dois equipamentos (tal como nos procedimentos de infravermelho), informar o valor e apertar "enviar" ou "pagar".

- http://coinbrasil.blogspot.com.br/2015/03/veja-como-funciona-uma-transacao-bitcoin.html;
- http://g1.globo.com/tecnologia/noticia/2014/02/entenda-como-e-uma-transacao-feita-com-moeda-virtual-bitcoin.html;
- http://www.qrcode.com/en/;
- https://pt.wikipedia.org/wiki/Código_QR;
- http://www.nearfieldcommunication.org/;

- https://pt.wikipedia.org/wiki/Near_Field_Communication.

Entretanto, para receber pagamentos o beneficiário não precisa fazer nada além de ter informado o seu endereço bitcoin; muito menos, ter um dispositivo conectado à Internet ou confirmar a transação.

Todas as transações em Bitcoin são públicas e podem ser vistas por qualquer pessoa do mundo na *Blockchain*, a qual pode ser acessada por algum *software* ou algum site que contenha uma réplica sincronizada dela. Recorda-se, ainda, que a *Blockchain* original existe somente dentro da rede P2P (*peer-to-peer*) do Bitcoin e, tal como um arquivo em nuvem (*cloud*) com múltiplos usuários e seguranças, é impossível ser adulterada ou manipulada sem ser prontamente percebido e sem conseguir comprometer as informações e arquivos autênticos.

Entretanto, essa verificação da transação não é invasiva, pois ninguém consegue saber facilmente quem são os usuários envolvidos ou quais são os produtos e serviços comprados.

Se um dos nós da rede tentar alterar uma transação, por exemplo, colocando o seu endereço no lugar do beneficiário, a assinatura digital deixará de ser válida no mesmo instante. Explica-se. Qualquer caractere ou bit alterado da mensagem ou arquivo original, implica na corrupção ou deterioração da assinatura digital, fazendo com ela deixe de ser válida. Se tentar transmitir à rede essa adulteração, todos os outros participantes (nós), de forma automática irão descartar essa transação por identificarem prontamente a adulteração.

SIGILO DOS PAGAMENTOS ELETRÔNICOS

Os pagamentos eletrônicos podem ser de forma identificada, anônima ou semianônima; ou seja, podem conter, ou não, informações que revelem ambas ou uma das partes envolvidas. Por outras palavras, existem pagamentos que são anônimos em relação ao negociante ou recebedor, mas não ao banco ou ao pagador. Entretanto, em alguns casos, até na forma anônima, apesar de não identificar todos os envolvidos, é possível a qualquer um ver os demais dados da transação.

Sigilo é a condição de algo que é mantido como oculto e secreto, fazendo com que poucas pessoas saibam da sua existência. É segredo (reservada exclusivamente para aquela que a está recebendo).

Privacidade é a reserva de informações pessoais e da própria vida privada. É a capacidade de existir na sociedade de forma anônima e da vida íntima não sofrer exposição pública. É, portanto, o direito: de controlar a exposição e a disponibilidade de informações acerca de si; de não ser monitorado, entendido como direito de não ser visto, ouvido, etc.; de não ser registrado, entendido como direito de não ter imagens gravadas, conversas gravadas, etc.; e, de não ser reconhecido, entendido como direito de não ter imagens e conversas anteriormente gravadas publicadas na Internet em outros meios de comunicação. Em resumo, é a vedação dos outros saberem (verem, ouvirem, lerem, etc.) o que a pessoa fez, faz, fará ou está fazendo. Podem até saber quem é, mas não sabem nada da sua intimidade e vida privada.

Anonimato, por sua vez, é ausência de identificação; ou seja, é ocultação. Muitos países permitem aos cidadãos ocultar a identidade como parte do direito à privacidade, desde que os atos cometidos não sejam ilegais. Portanto, é quando as pessoas sabem o que alguém fez ou está fazendo, mas não sabem quem é e nem conseguem ver essa pessoa sem identificação.

Nas culturas ocidentais, a esfera privada é um direito inalienável do indivíduo. Na Alemanha, por exemplo, é considerada o espaço onde a pessoa pode se comportar à vontade, sem ser observada nem escutada por

outros. Nos Estados Unidos, a privacidade é o "right to be let alone"; ou seja, o direito de ser deixado em paz.

As transações eletrônicas ainda podem ser de forma *online* (conectado, logado ou plugado) ou *offline*. *Online* impõe a necessidade de comunicação em tempo real para efetuar uma transação; já *offline* não há essa necessidade por poder trocar os dados diretamente com a outra parte ou pelo fato dos dados serem confirmados posteriormente quando estiver online.

Em regra, as carteiras e os endereços bitcoins não possuem qualquer informação pessoal sobre seus proprietários e, por isso, o bitcoin é considerado anônimo para o mundo exterior; vez que cada usuário de Bitcoin é identificado apenas pelo número da sua carteira, cuja senha é uma chave criptográfica. A exceção fica por conta de endereços personalizados onde o usuário prefere constar alguma identificação no seu endereço Bitcoin; bem como se divulga voluntariamente que dito endereço é seu.

Apesar de os participantes da rede serem anônimos, todas as trocas ficam abertas ao público como medida de segurança para impedir fraudes no sistema (como, por exemplo, a mesma pessoa usar mais de uma vez as mesmas unidades) e reduzir o uso em compras de produtos ilegais pela Internet. Desse modo, o Bitcoin não é totalmente anônimo. Todas as transações Bitcoin são armazenadas, publica e permanentemente, na rede, o que significa que qualquer um pode ver o balanço e as transações de qualquer endereço Bitcoin. Entretanto, a identidade do usuário por trás de um endereço permanece desconhecida até que a informação seja revelada durante uma compra ou em outras circunstâncias.

O endereço Bitcoin é a única informação usada para definir onde as bitcoins serão alocadas e onde serão enviadas. Estes endereços são criados privadamente pelas carteiras de cada usuário. No entanto, uma vez utilizado o endereço, este torna-se marcado pela história de todas as operações em que estão envolvidos. Qualquer um pode ver o saldo e todas as transações de qualquer endereço. Como os usuários geralmente têm de revelar a sua identidade, a fim de receber bens ou serviços, os endereços Bitcoin não podem ficar totalmente anônimos. Por estas razões, os endereços Bitcoin

devem ser utilizados apenas uma vez e os usuários devem ter cuidado para não revelar seus endereços.

Por exemplo, qualquer pessoa consegue saber qual é o endereço Bitcoin do “The Pirate Bay” (https://thepiratebay.org/): 129TQVAroeehD9fZpzK51NdZGQT4TqifbG; porque eles divulgam publicamente no site deles.

Portanto, toda transação feita via Bitcoins é pública, rastreável e armazenada permanentemente na rede Bitcoin. Ao acompanhar um arquivo público chamado *Blockchain* (registro público de transações Bitcoin em ordem cronológica), é possível saber, hipoteticamente, que o endereço Bitcoin (chave pública) "X" fez uma transferência para o endereço Bitcoin (chave pública) "Y", tornando possível rastrear onde estão as bitcoins, mas sem saber diretamente quem é o proprietário delas; ou seja, quem é o titular do endereço Bitcoin (chave pública) em questão. Entretanto, quando o usuário for converter as bitcoins em moeda convencional (tradicional, estatal ou dinheiro do mundo físico), normalmente irá ser preciso fazer um cadastro e é exatamente nesse momento em que perde o anonimato. Qualquer criminoso que queira converter uma grande quantidade de dinheiro em bitcoins teria que, em algum momento, fazer uso das casas de câmbio (*exchange*) de bitcoins e estas podem identificar o usuário. O ciberladrão terá problemas ao tentar lavar as bitcoins ilícitas; pois os serviços que se propõem a fazer esse serviço, como o Bitcoin Laundry ou o Bitmix, no geral não fazem o que prometem ou, pior, se apropriam para si das bitcoins que deveriam ser lavadas.

O Bitcoin envia unidades a partir do endereço “A” para o endereço “B”, o que significa que as transações podem ser rastreadas do final para o começo. Portanto, todas as bitcoins em circulação podem ser rastreadas retrogradamente até as suas respectivas transações iniciais.

Qualquer usuário pode verificar diretamente a *Blockchain* (cadeia de blocos) e observar as transações quase em tempo real; existem vários sites que facilitam esse monitoramento, incluindo variáveis agregadas como o número de bitcoins em circulação, número de transações por hora e taxas de transação a cada momento e representações gráficas para auditorias.

Um exemplo disso, é que o FBI conseguiu, com sucesso, rastrear transações da moeda (bitcoin) e acabar com a Silk Road e seus idealizadores, o que demonstra como o anonimato no Bitcoin, de modo geral, não é absoluto.

Devido ao sistema Bitcoin ser uma rede ponto a ponto (P2P), é possível ouvir os relés das transações e registrar os endereços IP (*Internet Protocol* ou Protocolo de Internet). Clientes de intersecções completas retransmitem as transações de todos os usuários, assim como as suas próprias. Isso significa que encontrar a fonte de qualquer operação específica pode ser difícil e qualquer interseção Bitcoin (IP de um dos nós da rede P2P) pode ser confundida como sendo a fonte de uma transação, quando na verdade não é. Isso é semelhante a falsa identificação da origem de um ataque *hacker*, quando é atribuída equivocadamente ao IP da máquina infectada ao invés de quem realizou o ataque por meio de acesso remoto de um computador zumbi.

Pelo fato de que o envio de bitcoin pode ser rastreado por seu montante, IP de propagação, nó da rede... se um usuário quiser operar de forma anônima na rede, é essencial que tome medidas preventivas para esconder o seu endereço IP para obter privacidade máxima enquanto navega na Internet e não tornar público a sua identidade real e seus endereços Bitcoins. Desse modo, sugere-se o uso do *browser* (navegador) Tor (https://www.torproject.org/) cumulado com um aplicativo de VPN (*Virtual Private Network* ou rede virtual privada) para desvincular o endereço IP das ações *online*; por exemplo, o Steganos Online Shield (http://www.segurisoft.com.br/steganos-online-shield-vpn/).

Ainda mais. Recentemente, nos Estados Unidos, a exchange Coinbase (https://www.coinbase.com/) foi obrigada (forçada) pela justiça a fornecer os dados de usuários de bitcoins.

- https://www.tecmundo.com.br/bitcoin/112255-tribunal-eua-pede-servico-bitcoin-entregue-dados-usuarios.htm;
- https://guiadobitcoin.com.br/coinbase-e-forcada-pela-justica-dos-eua-a-entregar-dados-de-usuarios-de-bitcoin/;

- http://www.criptomoedasfacil.com/2016/11/irs-vs-coinbase-enormes-implicacoes-para-bitcoin-e-demais-moedas-digital.html.

Whonix (https://www.whonix.org/) é um sistema operacional baseado no Debian focado em anonimato, privacidade e segurança através do isolamento. Whonix consiste em duas partes: uma exclusivamente roda o browser Tor chamada de Gateway. A outra, a Workstation, está em uma rede completamente isolada. Somente conexões através do Tor são possíveis.

Uma maneira de tentar dificultar o rastreio é através da utilização de diferentes endereços Bitcoins. Desse modo, a criação de endereços para um único uso pode ajudar com a proteção da privacidade; vez que o usuário não precisará expor seus endereços antigos e transações associadas para poder proceder com a transação.

Portanto, uma forma de aumentar a privacidade é através da utilização de um endereço Bitcoin novo e exclusivo para cada novo recebimento e/ou pagamento; bem como de múltiplas carteiras para propósitos diferentes. Em assim fazendo, estar-se-á isolando cada uma das transações, dificultando que sejam associadas (sejam relacionadas à mesma pessoa). Por outras palavras, há de se dificultar que as pessoas consigam consultar facilmente a quantidade, frequência, valores e com quem realiza transações em Bitcoins. Desse modo, em tendo vários endereços, cada uma das pessoas que conhece apenas um deles, não terá ciência dos vários outros.

BitcoinQT ou Bitcoin Core (Bitcoin-Qt foi rebatizada para Bitcoin Core desde a versão 0.9.0), sempre usa um novo endereço a partir de um *pool* de chave para uma melhorar a privacidade.

- http://www.bitcoin-en.com/install-bitcoin-qt-faster.html;
- https://bitcoin.org/pt_BR/download.

LocalBitcoins (https://localbitcoins.com/pt-br/) é famosa por sua natureza anônima. Seu slogan é: "Instantâneo. Discreto. Seguro.".

O que a Synereo (https://www.synereo.com/) quer fazer é criar uma rede social, descentralizada, inspirada na tecnologia Bitcoin, onde o foco

primeiro tem a ver com a reserva da privacidade e centrado no utilizador. Este projeto é uma rede social da nova geração que coloca a segurança, identidade e gestão da comunidade diretamente sob a alçada do utilizador, respeitando a sua atenção e recompensando-o pelas suas atividades na rede social.

A menos que a intenção seja receber doações públicas ou pagamentos com total e plena transparência, publicar um endereço Bitcoin em qualquer espaço público (como um site ou uma rede social) é não só abrir mão da privacidade, mas expor, continuamente, a movimentação financeira em Bitcoins para sempre e a qualquer pessoa do mundo.

Enquanto que num banco tradicional, a privacidade do cliente é protegida escondendo as transações de todas as partes, na rede Bitcoin qualquer comerciante pode fazer uma análise estatística do histórico inteiro de pagamentos e recebimentos; inclusive, estimar quantas bitcoins a pessoa tem. Em razão disso, alguns serviços online realizam uma mistura (*mixing*) de informações (embaralha as *input* [entradas] e *output* [saídas] de transações) para confundir e dificultar eventual rastreabilidade entre os usuários. O procedimento é feito, por exemplos, mediante a separação e restrição das informações de histórico para cada contraparte e, ainda, o recebimento e o envio usando endereços Bitcoin independentes. A legalidade desse tipo de procedimento pode ser questionável (e associado com lavagem de dinheiro) e exige-se a confiança nas pessoas que os executam para não perderem ou roubarem os valores e, inclusive, para não manter um registro das transações efetuadas.

Moedas mais sofisticadas usam misturadores que direcionam as moedas de endereço Um através de endereços X, Y, Z para abordar B. Com um misturador, embora mais difícil para um terceiro rastrear, ainda existe uma ligação entre as moedas enviadas e recebidas.

Outra opção é usar intermediários entre o emitente e o destinatário; assim, por exemplo, o emitente paga através de qualquer moeda à uma *exchange*, para que esta converta em outra moeda e envie para outra carteira e desta, enviasse o pagamento a outra *exchange* para que credite a moeda desejada na conta do credor ou destinatário final. Entretanto, envolve não só muito

trabalho, mas o conhecimento do câmbio do dia e das taxas das *exchanges* (casas de câmbio). Entretanto, sites de câmbio bitcoin e comércios em geral podem associar a identidade real com endereços bitcoin para fornecer serviços. Por razões como essa, o correto é classificar o Bitcoin como pseudoanônimo em vez de anônimo.

A Dark Wallet (https://github.com/darkwallet/darkwallet/releases/tag/0.2.0 e https://www.darkwallet.is/) é um conjunto de ferramentas (*plug-in*, *add-in* ou *add-on*: módulo de extensão que adiciona recursos ou funções a um software) para armazenar, enviar e receber bitcoins de forma totalmente anônima.

Moedas verdadeiramente anônimas são Monero (XMR), NAVcoin (NAV), ShadowCash (SDC), Darkcoin (DRK), etc. Cada uma delas tem seu protocolo de mineração próprio e prometem, à sua maneira, proteger seus dados de forma absoluta.

Dash (https://www.dash.org/), anteriormente denominada Darkcoin, é "a primeira moeda anónima". Isso gerou muitos clones, em especial pela sua tecnologia darksend para ocultar as transações. Há muitos clones de Dash/Darkcoin, mas nenhum tem conseguido ter o nível e o seu prestígio. A mudança de nome de Darkcoin para Dash corresponde à tentativa de retirar à moeda a carga negativa que lhes estava associada, como moeda utilizada em negócios ilícitos e pouco claros, que aproveitavam o seu anonimato para crescer.

- http://www.mercadodash.com/2015/03/a-darkcoin-agora-e-dash.html.

Monero (http://monero.org/ e https://getmonero.org/home) é uma criptomoeda que promete deixar as transações mais anônimas do que nunca, com o que rapidamente ganhou fama na *deep web*. Inclusive é o método de pagamento aceito no AlphaBay (um mercado on-line operado na *Darknet*).

A NAVcoin (http://www.navcoin.org/), por exemplo, para concretizar a promessa de ser uma rede totalmente anônima, utiliza duas *blockchains* distintas para efetuar o processo, fazendo as transferências serem realizadas

com acumulador de entrada e saída de fundos. Por outras palavras, o uso de duas *blockchains* visa a quebra (divisão, separação ou desmembramento) da cadeia de transações entre emissor e receptor; ou seja, os endereços do emissor e receptor da mesma transação não aparecem na mesma cadeia de operação ou registro.

As unidades da moeda Nav são, assim, enviadas pelo emissor ou pagador para a *blockchain* secundária, que as arquivará no seu saldo e enviará outras unidades para o destinatário ou recebedor; portanto, como não são as mesmas unidades que o pagador enviou e que o destinatário recebeu, não há qualquer ligação entre eles. Desse modo, as unidades de Nav enviadas pelo emitente ou pagador são utilizadas pela *blockchain* secundária apenas como reposição de caixa (saldo) para compensar (restituir ou reembolsar) o pagamento que será feito ao destinatário da ordem de pagamento expedida pelo emitente. Depois, em futura operação, essas unidades da moeda que ficaram retidas serão aplicadas em uma transação totalmente diferente. Detalhe, a *blockchain* secundária nem precisa esperar pela chegada de outras unidades de Nav para poder aplicar as unidades anteriormente retidas em alguma transação. E, em breve, os próprios usuários da Nav poderão executar seus próprios servidores de processamento (*blockchain* secundária ou subcadeia). Tudo isso significa que não é possível traçar as moedas recebidas de volta aos seus remetentes.

As cadeias laterais (*sidechains* ou *Blockchain* 2.0) são extensões para *blockchains* existentes que, além de aperfeiçoar a funcionalidade e adicionar recursos como contratos inteligentes, também melhoram a privacidade, possibilitando a realização de transações confidenciais. Em suma, a *blockchain* secundária ou subcadeia é usado para dirigir e gerir como as operações anônimas são criptografadas, randomizada e encaminhadas através da rede.

Zerocash (http://zerocash-project.org/) e Zerocoin (http://zerocoin.org/), através de conexões providas por sidechains, fornecem "Confidential Transactions" (Transações Confidenciais).

Zcash (https://z.cash/pt_br/buzz.html) também promete privacidade.

Anoncoin (https://anoncoin.net/) é uma criptomoeda baseada na I2P (*Projeto Internet Invisible*), a internet invisível; que foi originalmente concebida como uma maneira de ser capaz de usar IRC (*Internet Relay Chat*) anonimamente, mas tornou-se uma das redes mais populares anônimas. Embora semelhante ao Tor, as principais diferenças incluem o fato de que I2P se concentra em obter acesso a sites dentro da rede (e não para a Internet em geral). Este serviço é muito popular na Rússia. Cerca de metade dos roteadores parecem estar localizados lá. Detalhes podem ser encontrados em https://geti2p.net/pt-br/.

A moeda Quark (http://www.quarkcoins.com/) usa nove rodadas de criptografia para garantir a segurança e o anonimato em suas operações.

Nxt (https://nxt.org/) oferece uma opção para criar moedas shuffleable; ou seja, embaralhar para obscurecer a origem e os destinos das moedas para aumentar o anonimato.

Muitas melhorias podem ser esperadas no futuro para melhorar a privacidade. Por exemplo, vários trabalhos e pesquisas também estão sendo feitos para desenvolver outros potenciais recursos de privacidade prolongados como ser capaz de unir as operações aleatórias dos usuários juntas.

Uma das opções para aumentar a proteção dos usuários foi proposta com o uso de "Confidential Transactions". Esse recurso foi apresentado pelos desenvolvedores do Blockstream, uma ferramenta para integrar sidechains ao Bitcoin e adicionar/modificar funcionalidades. A ideia geral é esconder os valores das transações, dessa forma rastrear um usuário se torna mais complicado, pois é difícil saber quem seria um usuário em potencial para ser atacado.

POSSIBILIDADE DE PENHORA E DE DEPÓSITO JUDICIAL DE BITCOINS

A única forma de conseguir penhorar (apreensão judicial) bitcoins é conhecendo o par de chaves (a privada e a respectiva pública vinculada); as quais, em regra, somente são de conhecimento do seu titular. E, se está sendo necessária a realização de penhora, é porque o titular está relutante ou está querendo esconder as bitcoins que possui. Portanto, o titular não vai querer fornecer voluntariamente.

Desse modo, será preciso apreender os dispositivos (computadores, notebooks, tablets e smartphones) do Requerido, tanto de sua residência como de seu local de trabalho, para que sejam submetidos à perícia policial e/ou judicial com a finalidade de se descobrir as tais chaves necessárias. Se o requerido não tiver colocado senha em sua carteira bitcoin desktop, o trabalho será mais fácil.

Além da apreensão dos dispositivos supra, urge a realização de diligência de busca e apreensão para localizar eventuais anotações (lembretes), *back-ups* ou, até mesmo, eventuais *paper wallets* (carteiras bitcoin em papel).

Uma vez descoberto o par de chaves, basta o magistrado criar um endereço bitcoin específico, transferir as bitcoins do requerido para esse endereço e as deixar bloqueadas sob seu cuidado. Procedimento similar deve ser feito para que algum interessado possa efetuar depósito judicial de bitcoins; ou seja, o requerente solicita ao juiz a criação de um endereço bitcoin exclusivo para esse fim, o qual, depois de criado e informado ao requerente, este efetua o depósito judicial aos cuidados do magistrado.

Outra possibilidade de poder penhorar bitcoins é através de carteiras *online* que possuem acesso e conhecimento do par de chaves do usuário. Neste caso, basta o juiz oficiar ao site requisitando a transferência das bitcoins para um endereço bitcoin previamente criado pelo magistrado para esse fim. Na dúvida se o site tem acesso, ou não, ao par de chaves do requerido, o magistrado oficia assim mesmo. Entretanto, por óbvio, exige

saber previamente em qual site o requerido possui sua carteira online e qual é o endereço bitcoin (chave pública) do requerido.

E modo similar, em 30/11/2016, um juiz federal do Tribunal de Distrito do Norte da Califórnia, nos Estados Unidos, exigiu que o serviço de carteira Bitcoin Coinbase entregasse os registros de todas as transações que ocorreram de 2013 a 2015, como parte de uma investigação maior sobre possíveis fraudes fiscais por parte dos usuários da Coinbase.

- http://www.theverge.com/2016/11/30/13799638/coinbase-bitcoin-tax-fraud-investigation-irs.

Entretanto, existe a opção de o magistrado oficiar às *exchanges* (casas de câmbio) e demais locais que vendem bitcoins sob cadastro prévio de seus clientes, para o fim de requerer eventuais endereços bitcoins (chaves públicas) do requerido. De igual forma, se o magistrado souber de algum estabelecimento onde o requerido efetuou alguma compra ou pagou por algum serviço com bitcoin, pode-se oficiar solicitando o endereço bitcoin utilizado pelo requerido.

ONDE E COMO COMPRAR BITCOINS E ALTCOINS

Pode-se comprar bitcoins em vários sites:

- https://www.mercadobitcoin.com.br/;
- https://foxbit.com.br/;
- https://www.coinbr.net/;
- http://bitcointoyou.com/;
- http://basebit.com.br/;
- https://www.snapcard.io/;
- https://bitcambio.com.br/;
- https://foxbit.exchange/;
- https://www.coinbase.com/;
- https://localbitcoins.com/;
- https://www.carteirabitcoin.com.br/;
- https://www.coinbase.com/;
- http://www.negociecoins.com.br/;
- https://trader.flowbtc.com/;
- https://www.bitstamp.net/;
- https://bitbargain.co.uk/buy;
- https://www.kraken.com/;
- https://www.bitstamp.net/;
- https://btcdirect.eu/es-es;
- https://anycoindirect.eu/es;
- https://www.bitcoin.de/es;
- https://www.ripio.com/pt/;
- http://lista.mercadolivre.com.br/bitcoin#D[A:bitcoin];
- https://bter.com/trade/btc_cny;
- https://www.bitinka.pe/bitinka/home;
- https://www.virwox.com/;
- https://indacoin.com/change;
- https://cex.io/;
- https://www.coinmama.com/;
- http://www.avatradeportuguese.com/lp/bitcoin-trading;
- https://exchangewar.info/;
- https://www.bestchange.com/;
- https://bitfinex.com;

- https://bitmarket.pl;
- https://btc-e.com;
- https://www.btcc.com/;
- https://lakebtc.com;
- https://www.crxzone.com/;
- https://cryptonit.net;
- https://www.mistermoneybrasil.com/.

Change significa trocar ou mudar; portanto, câmbio. *Exchange* significa intercâmbio, trocar e vender. Outros significados de *exchange*: bolsa, letra, centro, permuta, corresponder, intercâmbio, mudar, divisa, correspondência, casa, cotação, descontar, câmbio ou corretor. *Trade* é trocar um item por outro (permuta). *Trader* é comerciante ou negociante. *Swap* é trocar, troca, barganhar, trocar-se, permuta ou barganha. *Swap* tem o sentido muito parecido com *exchange*. O papel da *exchange* é trazer compradores e vendedores todos juntos e aumentar a liquidez do Mercado. Por outras palavras, apenas aproxima vendedores e compradores e cobra uma comissão a cada transação.

Existem sites com calculadora de taxas de *exchanges*, como, por exemplo: http://freecurrencyrates.com/pt/BTC-exchange-rate-calculator.

As *exchanges* (casas de câmbio) ou *trading* (comércio ou negociação) bitcoin são como bolsas de bitcoins que facilitam as transações entre particulares, sem que o comprador saiba quem é o vendedor e vice-versa. Nas *exchanges* é visível a disposição do preço segundo a oferta e a demanda; pois as pessoas colocam as chamadas ordens de compra ou de venda com um preço que elas acham justo. Se tiver alguém disposto a fazer a transação por essa quantia, a ordem é executada e se transferem os valores através da *exchange*. São como o site Mercado Livre intermediando o negócio entre vendedor e comprador. Também a *exchange* mostra o valor médio para comprar ou vender diretamente, executando as ordens automaticamente.

O site https://www.bestbitcoinexchange.io/ lista várias exchanges de criptomoedas e as avaliações das mesmas. Confira, ainda, as listas de

exchanges existentes em http://saldigi.info/exchange/ e http://cryptocoin.cc/ccres.php?resource=exchanges.

Os sites Local Bitcoins (https://localbitcoins.com/pt-br/) e Carteira Bitcoin (https://www.carteirabitcoin.com.br/quero_comprar) permitem procurar pessoas próximas (na mesma localidade ou comunidade) que queiram vender ou comprar bitcoins diretamente.

O procedimento de comprar bitcoin é bastante simples e intuito, mas no site http://pt.wikihow.com/Comprar-Bitcoins existe um manual ilustrativo, passo a passo.

O site https://www.virwox.com/ negocia bitcoins e aceita Paypal (https://www.paypal.com/), Skrill (https://www.skrill.com/), Paysafecard (https://www.paysafecard.com/pt-pt/), OK Pay (https://www.okpay.com/pt/), Sofort banking (https://www.sofort.com/) e cartões de crédito.

- https://www.buybitcoinworldwide.com/pt-br/compre-bitcoins-com-paypal/.

O site https://www.havebitcoin.com/buy-bitcoins/ permite comprar bitcoin através do Paypal, Payza (https://www.payza.com/), Perfet Money (https://perfectmoney.is/), *Bank Wire* e cartões de débito e crédito.

Também é possível comprar bitcoins com cartão de crédito ou débito em https://indacoin.com/change.

Do mesmo modo que existem *exchanges* que trabalham com bitcoins, também existem outras que trabalham com uma, algumas ou várias altcoins.

O site https://shapeshift.io/, por exemplo, permite a troca de várias criptomoedas entre si (comprar uma usando outra): Bitcoin, Bitcrystals, Blackcoin, BitShares, Clams, Dash, Digibyte, DigixDAO, Dogecoin, Emercoin, Ether, Ether Classic, Factoids, LBRY, Lisk, Litecoin, MaidSafe, Mastercoin, Monacoin, Namecoin, Novacoin, Nubits, Nxt, Peercoin, Reddcoin, Augur, ShadowCash, Siacoin, StorjcoinX, SingularDTV,

Startcoin, Steem, TetherUSD, Vericoin, Vertcoin, Voxels, Counterparty, Monero, Ripple e Zcash.

O site Mercado Bitcoin emite nota fiscal dos seus serviços (https://www.bitcoinbrasil.com.br/s).

Coins2learn (http://coins2learn.com/) é um simulador para compra e venda de Bitcoin e Altcoins. Também é um jogo; existe um *ranking* onde os melhores jogadores vão se destacando e ganhando prêmios em Bitcoin. Cada jogador começa com $2000 dólares (*playmoney*). Cada torneio tem duração de uma semana.

Recorda-se que também existem vários aplicativos (Apps) de *smartphones* e *tablets* que permitem comprar e vender bitcoins. Para facilitar uma pesquisa, se o sistema operacional do dispositivo for Android, ao invés de procurar pelo Play Store no próprio *smartphone* ou *tablet*, basta acessar pelo computador o site do Google Play (https://play.google.com/store/apps), clicar na aba/guia Apps e digitar os termos de pesquisa.

E, inclusive, é possível realizar empréstimo em bitcoin no site https://btcjam.com.br/.

As bitcoins, também, podem ser recebidas em troca de disponibilizar a capacidade de processamento computacional (mineração). Também é possível ganhar bitcoins em sites denominados *faucets* (torneiras).

COMO GANHAR BITCOINS E ALTCOINS?

Uma forma bem simples de adquirir bitcoins, é simplesmente aceitando-os como pagamento por produtos e serviços; ou seja, basta dar aos clientes essa opção de pagamento. Para divulgar isso na comunidade bitcoin, o interessado deve possuir, no mínimo, um endereço bitcoin para o recebimento.

Entretanto, uma das formas mais comuns de adquirir os primeiros bitcoins é através das "faucets" para ganhar pequenas quantidades de bitcoins. *Faucet*, na tradução do inglês, é torneira e, como tal, pinga de pouco em pouco.

Faucets são sites ou aplicativos que disponibilizam pequenas quantidades de bitcoins (satoshi) grátis. Os valores oferecidos variam de *faucet* para *faucet*; assim como o espaço de tempo em que se pode pedir novamente bitcoins. Normalmente o tempo de espera vai de alguns minutos a algumas horas. As *faucets* disponibilizam as bitcoins (satoshis no caso) de forma grátis porque ganham com a publicidade.

- https://en.wikipedia.org/wiki/Bitcoin_faucet

Os *faucets* normalmente são aplicativos ou sites malfeitos, confusos, instáveis e que nem sempre cumprem o que prometem; principalmente quando o assunto é o pagamento dos seus míseros satoshis. Isso acontece porque normalmente possuem vida curta, pois, quando eles deixam de ser economicamente viáveis, seus proprietários simplesmente os abandonam ou retiram do ar e, assim, os infelizes usuários que tinham pagamentos pendentes ficam a “ver navios”.

Existem duas coisas nas quais nunca se deve acreditar numa *faucet*: 1) aumento da quantidade ganha mediante o pagamento de qualquer quantia de bitcoins; e, 2) serviços de multiplicação de criptomoedas, onde o usuário deposita uma quantia em bitcoin e, depois de um determinado tempo, o site devolve uma quantia maior do que a que foi depositada. Os motivos para não se acreditar nesse tipo de promessa são simples, ninguém dá dinheiro de

graça e não faz sentido pagar valores para aumentar os ganhos sobre serviços que o usuário está prestando (acessar sites, links, vídeos, etc.).

Algumas *faucets* exigem um prévio cadastro simples. Assim deve-se clicar inicialmente em algum ícone ou link escrito algo, como por exemplo, “New user” ou “Novo usuário”. Fornecer um endereço de e-mail; não precisa ser o vinculado à carteira Bitcoin. Informar o endereço Bitcoin (*Bitcoin Address*). Criar uma senha (*Password*). Resolver um *Captcha* e clicar em algo como *Sign UP* (Inscrever-se).

Alguns sites de *faucets* precisam de autorização de "cookies" (https://pt.wikipedia.org/wiki/Cookie_HTTP). Normalmente mostram uma mensagem como: "This website uses cookies to ensure you get the best experience on our website." (Este site usa cookies para garantir que você obtenha a melhor experiência no nosso site.). Aí é só clicar em algo como "Got it!" (Entendi!).

Basicamente em todas os sites *faucets* deve-se fornecer o NB ou endereço Bitcoin ("Enter your Bitcoin address" ou "Your address"), clicar em "Log in", "Log Me In", "Submit", "Enter", "Go", "Play", "Start Earning" ou "Next". Depois em "Claim", "I Want My Bitcoin", "I'm a Human", "Roll", "Pay me", "Get a reward", "Request Bitcoin", "Give coins", "Get free bitcoins", "Catch Your Prize", "Toggle navigation", "Withdraml", "Submit", etc. Detalhe, os ícones ou links não são todos esses, não são exatamente nessa sequência/ordem e podem estar, cumulativamente, antes e depois da *captcha*. Depois, digita-se a *captcha* ("Human Verification", "I'm a Human" ou "Prove you are a human" = provar que é humano e não um robô). Os links e ícones ficam meio escondidos, misturados, discretos ou camuflados de propósito para forçar clicar no lugar errado e, assim, ler as propagandas ou visualizar eventuais janelas e/ou páginas que se abrem.

Em síntese, conforme supra explicado, o funcionando das *faucets* consiste, basicamente, em fornecer o endereço bitcoin (chave pública), preencher ou resolver um *captcha* e receber os satoshis.

Atualmente existem centenas de sites onde se pode ganhar Bitcoin (satoshis na verdade) de graça, seja clicando em anúncios (PTC - "paid to

click ads"), seja assistindo vídeos, ou jogando algum game (jogo) on line. O processo é bem simples, basta acessar um desses sites, informar o endereço Bitcoin (NB) e cumprir uma meta determinada, de acordo com a natureza do site.

Captcha é um acrônimo da expressão "Completely Automated Public Turing test to tell Computers and Humans Apart" (teste de Turing público completamente automatizado para diferenciação entre computadores e humanos). Trata-se de um teste de desafio cognitivo, utilizado como ferramenta anti*spam*. Em linhas gerais, os *captchas* servem como uma ferramenta auxiliar para evitar *spams* ou mensagens disparadas por outros computadores ou robôs ("robots" ou "bots"). A ideia é que a resposta aos testes de *captcha* seja de solução impossível para um computador, permitindo, assim, que somente seres humanos tenham acesso a determinados conteúdos ou possam enviar informações.

Dessa forma, os *captchas* são utilizados para impedir que *softwares* automatizados executem ações que degradam a qualidade do serviço de um sistema dado, devido à despesa do abuso ou do recurso. São também ativamente utilizados para limitar e controlar o acesso automatizado aos blogs ou a fóruns, em consequência de promoções comerciais, ou de vandalismo. *Captchas* servem também no controle da taxa limite de serviço automatizado (*robots*) em detrimento de usuários humanos. *Captcha* é, também, o mecanismo sugerido para impedir listas automatizadas em placares e em votações de discussão pública.

Normalmente o *captcha* é precedido da frase "Please confirm that you are a human" (Por favor, confirme que você é um ser humano).

Um *captcha* usual envolve um computador (um servidor), que pede que um usuário termine um teste. Como os computadores são incapazes de resolver o *captcha*, todo usuário que incorpora uma solução correta é presumidamente humano. Quando a resposta ou solução dada estiver errada aparece a mensagem "Invalid captcha code!" ("Captcha código inválido!") ou "CAPTCHA incorrect. Please try again." ("CAPTCHA incorreta. Por favor, tente novamente.").

Um tipo comum de *captcha* requer que o usuário identifique e digite as letras e/ou números ("Enter the following:" no campo "Your Answer") normais, distorcidos, borrados ou com a adição ou sobreposição de uma sequência obscurecida das letras ou dos dígitos que apareça na tela.

- http://googleonlinesecurity.blogspot.com.br/2014/12/are-you-robot-introducing-no-captcha.html;
- https://support.google.com/recaptcha/?hl=pt-BR;
- https://pt.wikipedia.org/wiki/ReCAPTCHA;
- https://www.google.com/recaptcha/intro/index.html;
- http://www.captcha.net/;
- https://www.oficinadanet.com.br/artigo/php/o-que-e-recaptcha-e-como-funciona.

Existem várias empresas e tipos de *captchas*. Alguns sites deixam escolher qual *captcha* usar.

O ReCaptcha pertence ao Google e inicia-se selecionando a opção "Não sou um robô" ("I'm not a robot") e, após, se abre uma janela onde se pede para selecionar/marcar determinados/específicos tipos de imagens (exemplos: carros, aviões, laranjas, comidas, bebidas, tortas, pizzas, placas de rua, etc.) dentro das apresentadas e finaliza com o clique em "Confirmar" ("Verify").

O *captcha* da Solvemedia (http://solvemedia.com/) costuma exigir uma interação iniciando-se com clique em "Revele" ou "Player", onde se abre uma janela de propaganda e se espera aparecer um código (exemplos: Gone Fishing, Flannel Shirt, Fish Tacos, Birdie Putt, Study Group, Team Player, Diving Board, etc.) para ser digitado no campo "Your answer" e depois clicar em "Return to page". Normalmente é para colocar alguns objetos no local apropriado ou relacionado.

- http://api.solvemedia.com/public/puzzle_more_info.

Quando é da Funcaptcha (https://www.funcaptcha.com/), clique na palavra "Player" ou "Verify" para decifrar uma charada em forma de jogo de

raciocínio lógico através de imagens utilizando o arrastar pelo mouse ou em clicar em setas para alinhar uma imagem e depois clicar em "Done". Outro tipo envolve girar um círculo com recorte/parte de uma imagem para alinhá-lo com o restante da imagem.

- http://support.funcaptcha.com/.

Outro *captcha* é bem simples; basta clicar em "Start", mover algumas imagens específicas para o local adequado e talvez clicar em "Continue" (http://blog.areyouahuman.com/help/english.html).

Normalmente em todos os *captcha* possui o ícone da função "New puzzle" ou "Refresh" para carregar uma nova imagem ou tarefa.

No site http://bitcoin-data.com/, por exemplo, consta a advertência: "AntiBot System: Please press the text that says "I'm Human" to activate the Claim" (AntiBot Sistema: Por favor, pressione o texto que diz " Eu sou humano " para ativar a Reivindicação); ou seja, tem que clicar em um punhado de escritos "I'm Human" para poder aparecer o botão "Claim" (reivindicação). Detalhe, não é para clicar nos escritos "I'm Robot".

Nos sites http://freebtcforalll.com/, http://www.freebitcoinsgolds.info/ e http://bazarofbitoins.com/ constam o aviso: “"Due to Abuse of bots, You must Click on the 8, "No bots" to Claim"” (Devido ao Abuso de bots, você deve clicar sobre as 8 "Não há bots" para reivindicar). Assim tem-se que clicar nos minúsculos escritos "No Bots" (em alguns sites são "unlock" [destravar] ou "Are you a human" [Você é humano]) espalhados e escondidos para somente depois aparecer o botão "Get Bitcoins" (obter Bitcoins); vez que o escrito "Claim" (reivindicação) nestes sites é falso.

No site http://www.bitcoinfree.es/faucet.php tem a mensagem: "DISCULPE LAS MOLESTIAS, Debido a muchos robos de Bitcoins, para activar el boton SOLICITE YA!, y verificar que Uste no usa Bots, por favor haga click a 4 botones ANTIBOT que ese encuentran escondidos, una vez completados, el boton aparecera automáticamente." (Lamentamos, devido a muitos de roubo de Bitcoins, para ativar o botão, INSCREVA-SE AGORA! E verificar se você deixar de usar Bots, por favor clique AntiBot 4 botões

que estão escondidos, uma vez concluído, o botão aparecerá automaticamente.).

Em outros sites constam o aviso: "Please choose the phrase "I'm Human" (4 times) on 4 different positions to reveal the captcha." (Por favor, escolha a frase "Eu sou humano" (4 vezes) em 4 posições diferentes para revelar o captcha.). No site http://www.dineromatic.net/faucet.php os 6 (seis) escritos escondidos são "I'm not a bot"; somente depois de digitar o NB, resolver o captcha e clicar nesses 6 escritos discretos, é que aparece o ícone "SOLICITA YA!" (depois dele, clique em "OK"). No site http://super-bitcoins.com/ segue o mesmo procedimento para poder aparecer o ícone "Claim Now". De igual forma o site http://faucetbtcs.com/ para poder aparecer o link "Bitcoin!".

Pode ocorrer de o site não ter fundos suficientes no momento para poder efetuar o pagamento ("Insufficient funds."). Essa situação pode ser momentânea, prolongada ou definitiva.

Algumas *faucets* pagam de imediato ("direct"), outros de forma semanal e, alguns efetuam os pagamentos através do site https://faucetbox.com/en/ ou http://epay.info/. Também há sites que pagam de forma imediata, mas através do Xapo (https://xapo.com/ ou https://xapo.com/pt/). Já outros pagam quando atingir determinado valor acumulado (exemplos, 5.000 ou 6.000 satoshis). Portanto, alguns sites podem enviar os créditos direto na hora ("satoshi was sent to" [FaucetBox, ePay ou Xapo] ou "You can withdraw coins on" [Faucetbox, ePay ou Xapo]), semanalmente (WEEKLY), após atingir um valor ("Satoshi has been added to your balance", "Current balance:", "Min. Cashout:" e/ou "Cash out amount") ou em sendo clicada a opção "Cash Out To" (Faucetbox, ePay ou Xapo), "Send My Bitcoin To" (Faucetbox, ePay ou Xapo) ou "Cash out all".

Alguns sites possuem a opção de “auto-withdraw enabled” (auto-saque habilitado); ou seja, assim que atingindo o valor mínimo necessário para a transferência, esta será efetuada automaticamente.

FaucetBox é um género de carteira online utilizada para receber todos os micros pagamentos feitos pelas *faucets*, desde que estes também utilizem o

FaucetBox como forma de pagamento. Desta forma pode-se acumular os satoshi e levantá-los para a carteira principal em um único pagamento.

O **EPAY** é um grande site de coleta gratuito de Satoshis (frações de Bitcoin) que reúne potentes torneiras (*faucets*), e, também é, um site seguro de micropagamento (*CyproCoins micropayment cache*); que apenas paga, não sendo possível fazer depósito.

Confira a lista das torneiras do FaucetBox (https://faucetbox.com/en/list e http://www.btcfaucetlist.net/) e do ePay (http://epay.info/rotator/free-bitcoin-faucets). Infra algumas *faucets* conveniadas à Xapo:

- http://xapo-faucets-list.com/pt/;
- http://cointasker.com/bitcoin-faucets/xapo-faucets/;
- https://cryptocointalk.com/topic/36147-top-5-free-bitcoins-with-xapo-faucets/.

Infra algumas das outras mini-carteiras ("Microwallet" ou "micropayment cache"):

- https://www.microwallet.org/;
- http://bitcoin-cloud.eu/index.php;
- https://paytoshi.org/;
- https://www.coinbucks.io/.

Quando se tenta receber mais satoshis antes do intervalo necessário pode aparecer a advertência: "You can get a reward again in", "You can claim a satoshi prize again in:", "You can claim again in" ou "It'll start again tomorrow!".

Algumas páginas necessitam serem recarregadas/atualizadas para poder pedir satoshis novamente e pode ser que possua a opção de atualização automática quando terminar o tempo de espera/intervalo entre um pedido e outro ("Auto refresh when finished").

Alguns sites possuem a opção "Play sound when finished", "Play sound when timer runs out" ou "Alert me when it's time to claim", que é tocar um som quando terminou o tempo de espera para pedir mais satoshis ou bitcoins.

Poucos sites salvam o endereço Bitcoin para não ser precisar digitar de novo; assim pode-se deixa-lo salvo num bloco de notas, para ficar copiando e colando.

Se não souber inglês ou outro idioma, basta navegar na Internet com o "browser" (navegador) Google Chrome (https://www.google.com.br/chrome/browser/desktop/); que ele tem a função de traduzir. Ou, se preferir, usar o site do Google Tradutor (https://translate.google.com.br/?hl=pt-BR).

Confira uma listagem de sites de *faucets* em http://moneyinpjs.com/faucet-list/freebitcoin.php e http://btc.re/faucetrotator.php e em http://coinbucks.io/coinwall/.

Mais sites de *faucets* podem ser encontrados nos próprios sites de *faucets*; ou seja, é comum um site de *faucet* fazer indicações ou propagandas de outros sites de *faucets*.

Os sites de *faucets* também possuem programas de referenciamento ("Referral link" ou simplesmente "Refer"); ou seja, através de indicação de novos usuários ao *faucet* se recebe um percentual ou comissão sobre o valor ganho por esse novo usuário. Tais indicações são feitas através de links/url (normalmente, indicado ou exemplificado, com a expressão "YOUR REFERRAL URL" ou simplesmente "Referral link") com o endereço do site *faucet* acrescido de algum código de identificação do divulgador (não é pirâmide).

Alguns divulgadores incrementam tais indicações através de sites rotativos ("Rotator") ou de revezamento de todos os sites de *faucets* que eles indicam. Assim, em tais sites de divulgação de *faucets*, existe um ícone (como "Next") onde você vai navegando de *faucet* em *faucet*. Exemplos:

- https://www.landofbitcoin.com/;
- http://www.faucetbtcs.com/rotator/;
- http://www.cryptoblox.com/Bitcoin/rotator.php;
- http://btc.re/faucetrotator.php;
- http://rotator.doublebitcoins.com/;
- http://freebtc.website/;
- http://ifaucet.net/bitcoin/browser/;
- http://bitcoinrotator.com/;
- http://allbtc.ru/rotator/;
- http://rotabit.com/;
- http://super-bitcoins.com/rotator/;
- http://boxclikz.com/rotator/;
- http://dogegalaxy.net/DogeGalaxy_LTCRotator.html;
- http://www.1stbitco.in/faucet/rotator/;
- http://crypto.uboxi.com/;
- http://rotator.doublebitcoins.com/r/BestBitcoinFaucetsGUARANTEED/;
- http://www.getfreebitcoins.eu/rotate/;
- https://freebitcointalk.org/bitcoin-faucet-rotators/;
- http://www.bestbitcoinsfaucet.com/sitios/faucet/xapo/01.php.

Mais explicações constam em http://vocemaisrico.com/2015/06/23/bitcoins-2/ e http://freecriptomoedas.blogspot.com.br/2015/03/ganhe-bitcoins-de-dez-em-dez-minutos.html.

LISTA DE *FAUCETS*

Infra uma lista de *faucets*. Ressalta-se que as condições e os valores dos prêmios podem mudar a qualquer momento; bem como os sites podem, a qualquer tempo, ficarem sem fundos ou serem desativados (*disabled*) e, até mesmo, serem abandonados, resultando em mensagens de erro, tais como: *Service Unavailable* (Serviço indisponível), “A página de não está funcionando”, “Não é possível acessar esse site”, etc. Apesar disso, os nomes e links foram mantidos em razão de que, nada impede que seus responsáveis resolvam recarregá-las, repará-las ou reativá-las; ou seja, a indisponibilidade pode ser apenas temporária, por exemplo, por excesso de visitações, por queda na rede, por quebra de link, por estar em manutenção (*maintenance*), por problemas no servidor ou por estar sendo reformulada ou atualizada (*updating*). Somente excluímos da lista original os sites que realmente não existem mais, mas, mesmo assim, podem ocorrer erros e não serem mais visualizados, estarem a URL disponível para compra ou terem tido o domínio adquirido por outra pessoa e, assim, o endereço ser de outra coisa agora. Portanto, apesar do que se possa parecer, todos os links foram testados e, vários foram deletados, antes da conclusão do livro.

Outro motivo de se manter alguns poucos links apesar da indisponibilidade, foi o fato de servirem de exemplo da modalidade e das explicações de uso que servem para outros sites semelhantes.

Recorda-se as *faucets* não existem somente em sites, mas também em aplicativos de *smartphones* e tablets.

Bitvisitor (http://www.bitvisitor.com/) – Ganha-se Bitcoin vendo anúncios. Digita-se o endereço Bitcoin (NB) e clica-se em "SUBMIT". Resolve-se o *captcha* e clica-se em "VISIT!". Ocorrerá o direcionado ao anúncio, onde deve-se esperar a contagem regressiva e só depois clicar em "NEXT". Para ganhar mais, basta continuar acessando as páginas; mas existe um limite de anúncios por dia.

Ads4btc (http://ads4btc.com/) - Ganhe Bitcoins por visualizar anúncios.

Bittoclick (http://bittoclick.com/) -Ganhe bitcoins para clicar anúncios.

Btcclicks (http://btcclicks.com/) - Ganhe bitcoins para clicar anúncios.

Field Bitcoins - Depois de uns cliques deixa o site aberto e os satoshis vão aumentando: http://fieldbitcoins.com/?ref=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

VIEWCLICKASH - 10.000 satoshis por tarefas diárias durante uma semana: http://www.viewclickcash.com/registro.php.

Free Bitcoin Lottery - Uma vez por dia: http://bitcoinlottery.club/en/.

EarnFreeBitcoins é um serviço em que se ganha pequenas quantidades de Bitcoins em troca de visitar sites, por um período de tempo designado: http://earnfreebitcoins.com/?r=eaef398b5.

Bitcoins Surveys – Ganha-se Bitcoins fazendo tarefas e testes: http://bitcoinsurvey.com/index.php.

Bitcoin Quiz - Entre 3.000 a 10.000 satoshis, a cada 24 horas (3 perguntas, responder: "Silk Road was an online black market", "21,000,000" e "XAPO is a Bitcoin Faucet site"): http://pinktussy.co/quiz-for-bitcoins-2/.

Turbobiti - 500 satoshis, via FaucetBox, a cada 1100 minutos: http://turbobiti.ru/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Faucet World - Até 7.500 satoshis a cada 418 minutos: http://faucetworld.info/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

MyFaucetBitcoin - 600, 2.500 ou 6.000 satoshis, via FaucetBox, a cada 400 minutes: http://myfaucetbitcoin.com/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Botva - 300, 500, 700, 1.000, 5.000 ou 10.000 satoshis, via FaucetBox, a cada 180 minutos: http://botva.net/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

CatsFaucet - 600, 800, 1.000 ou 5.000 satoshis a cada 120 (cento e vinte) minutos: http://catsfaucet.su/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

FreeBitcoin - 520, 620, 720 ou 3.100 satoshis, via FaucetBox, a cada 120 (cento e vinte) minutos: http://freebitcoinhome.com/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

BTC Drips - 200, 250 ou 1.200 satoshis, via FaucetBox, a cada 120 minutos: http://btcdrips.com/id=51317.

Altcoin Revolution - 300, 400, 500 ou 1.000 satoshis, via FaucetBox, a cada 90 minutos: http://altcoinrevolution.com/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

FrogBTC - 500, 550 ou 1.500 satoshis a cada 60 (sessenta) minutos: http://frogbtc.com/id=7559.

Destiny BTC - De 400 a 20.000 satoshis a cada 60 (sessenta) minutos: http://destinybtc.com/?id=816417.

MoneyInPJ's - 200, 800, 2.000 ou 100.000 satoshis, via FaucetBox, a cada 60 (sessenta) minutos: http://moneyinpjs.com/free-coin/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Bit Kranik - 215, 370, 450, 500 ou 1.000 satoshis a cada 60 minutos: http://bitkranik.ru/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

YouBit - 500, 800, 1.000 ou 5.000 satoshis, via FaucetBox, a cada 60 (sessenta) minutos: http://youbit.su/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Highest Paying - 200, 800, 2.000 ou 100.000 satoshis, via FaucetBox, a cada 1 (uma) hora: http://moneyinpjs.com/free-coin/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Daily Free Bits - De 100 a 1.200 satoshis, via Faucetbox, a cada 1 (uma) hora: http://dailyfreebits.com/faucet.

Bitcoin Newsday - 300 ou 500 satoshis, via FaucetBox, a cada 60 (sessenta) minutos: http://bitcoinnewsday.com/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA#sthash.nBzitNvL.dpuf/.

CM Monitor - Entre 200 e 2.500 satoshis, via FaucetBox, a cada 60 (sessenta) minutos: http://www.cmmonitor.com/btc/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

B-T-C FAUCET - 600 satoshis, via FaucetBox, a cada 60 (sessenta) minutos: http://b-t-c.tk/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Hourly Bitcoin - 200 ou 1.000 satoshis a cada 60 (sessenta) minutos: http://www.hourlybitcoin.com/.

Babyfreebtc - 700 satoshis, via FaucetBox, a cada 1 (uma) hora: https://www.babyfreebtc.com/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

GreenBitCo.in - Ganhe 300, 320, 340, 360, 400, 450, 2.000 ou 200.000 satoshis a cada hora: http://greenbitco.in/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Freebitcoin - Sorteio (valores variados) de satoshis a cada 1 (uma) hora: http://freebitco.in/?r=1590405.

Mezza Bank - 5.000, 1.250, 350 ou 175 satoshis, via FaucetBox, a cada 1 (uma) hora: http://faucet.mezzabank.com/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Elenafaucets - 501, 601, 701 ou 1501 Satoshis a cada 1 (uma) hora:

- http://elenafaucets.com/freebitcoin01/?id=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA;

- http://elenafaucets.com/freebitcoin02/?id=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA;
- http://elenafaucets.com/freebitcoin03/?id=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA;
- http://elenafaucets.com/freebitcoin04/?id=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

BTC Block - 100 satoshis a cada 1 (uma) hora: http://btcblok.org/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Bitcoin Showers - 200, 300, 400, 500, 600 ou 2.000 satoshis, via FaucetBOX, a cada 1 (uma) hora: http://bitcoinshowers.com/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Fast Bitcoin Faucet - 200 satoshis a cada 1 (uma) hora: http://moneyinpjs.com/fast-bitcoin/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Best Bitcoin Faucet - 50, 100, 250, 300, 350, 500 ou 700 satoshis via FaucetBOX a cada 1 (uma) hora: http://moneyinpjs.com/best-bitcoin/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Lucky Bit Faucet - Premiação variada a cada 1 (uma) hora: http://luckyb.it/faucet/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

DailyFaucet.com - Satoshis a cada 1 (uma) hora: http://dailyfaucet.com/.

We Love BitCoin - 500 satoshis a cada 1 (uma) hora: http://welovebtc.com/.

InFaucet - De 250 a 1.000 satoshis a cada 1 (uma) hora. Escolha uma caixa: http://infaucet.com/.

Free Satoshi Bit - Ganhe satoshis e números de sorte a cada 1 (uma) hora ("Free Satoshi", "Log in" ou "sign up", "login", captcha, "Get Satoshi!" e "I'm human"): http://freesatoshibit.com/.

Print Money - 505, 750 ou 1.000 satoshis, via FaucetBOX, a cada 1 (uma) hora ("To the printer!", digite o NB, captcha e "Print!"): http://printmoney.info/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Anchor Faucet - 500, 700, 1.000 ou 10.000 satoshis, via FaucetBOX, a cada 1 (uma) hora: http://www.anchorfaucet.tk/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Paidbooks - 3.000 satoshis por hora por ler livros: http://www.paidbooks.com/.

FreeBitcoinWin - Ganhe até US $ 200 (duzentos dólares americanos) em bitcoins a cada 1 (uma) hora por jogar: http://freebitcoinwin.com/signupin.

Busbitco.in - A cada 45 (quarenta e cinco) minutos: http://busbitco.in/?id=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Bitmachine - A cada 30 (trinta) minutos escolha uma imagem e veja quantos satoshis ganhou: http://bitmachine.org/mach1/finalpic.

Water Bitcoin - 800, 900, 1.000 ou 20.000 satoshis a cada 30 (trinta) minutos: http://waterbitco.in/.

P+P - Satoshis a cada 27 (vinte e sete) minutos: https://pppfaucet.com/bitcoin?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Red Faucet - 220, 300 ou 1000 satoshis, via FaucetBOX, a cada 16 (dezesseis) minutos: https://redfaucet.pw/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Bitcoin Inker - Escolher 250 ou tentar 100, 200 ou 450 satoshis, via FaucetBOX ou Xapo, a cada 15 (quinze) minutos: http://bitcoinker.com/faucet?ref=e68703be5c75.

StarFaucet.com - Entre 169 e 215190 Satoshis, via ePay, a cada 15 (quinze) minutos: http://www.starfaucet.com/?

r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

SurpriZes.org - Raspadinha com 127, 169, 211, 253, 295 ou 4.219 satoshis, via ePay, a cada 15 (quinze) minutos: http://surprizes.org/.

Coin Collecting - Raspadinha com 232, 253, 329, 388, 591, 1097 ou 1603, satoshis, via ePay, a cada 10 (dez) minutos: http://coincollecting.ws/ e http://coincollecting.ws/free-bitcoin/index.php.

Coin Gamez - Gire a roleta ("Spin") a cada 10 (dez) minutos. Recarregar a página para jogar ("Spin", "Next" e "Claim") novamente. De 150 a 1.000 satoshis e jackpot via ePay: http://goldsday.com/free-bitcoin/.

SpinandWinOnline - Igual ao Coin Gamez. Gire a roleta a cada 10 (dez) minutos: http://spinandwinonline.com/.

Crown Faucet - Entre 76 e 380 satoshis, via ePay, a cada 10 (dez) minutos: http://crownfaucet.com/.

Play Bitcoin - 300 Satoshi a cada 10 (dez) minutos ao votar no desenho mais bonito: http://playbitco.in/.

DreamFaucet.com - Raspadinha com 148, 295, 414, 473, 591, 675 ou 1181 satoshis, via ePay, a cada 10 (dez) minutos: http://dreamfaucet.com/.

Boxbit - A cada 10 (dez) minutos clique em Select box, Next e Get Reward (mais instruções em disponíveis em http://freecriptomoedas.blogspot.com.br/2015/03/ganhe-bitcoins-de-dez-em-dez-minutos.html): http://boxbit.co.in/?ref=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Coin Checkin - Faça o chekin, tente acertar o horário exato. Premiação variada a cada 5 (cinco) minutos, de 15 a 100.000 satoshis: http://coincheckin.com/Main/index.

QoinFaucet - 222 satoshis a cada 5 (cinco) minutos: http://qoinfaucet.com/?id=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

Alien Bitcoin - "Mate" alienígenas e ganhe 110, 192, 440, 715 ou 7.425 satoshis (o jogo para celular está em http://www.bitcoingameapps.com/track.php?ref=176514). Acesso a cada 5 (cinco) minutos: http://www.bitcoinaliens.com/faucet/.

Just Get Bit - 100, 200, 600, 3.000 ou 100.000 satoshis a cada 5 (cinco) minutos: http://jrswab.com/justgetbit/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

GlobalFaucet.com - Entre 76 a 12.658 satoshis, via ePay, a cada 5 (cinco) minutos: http://globalfaucet.com/.

Free-bitcoin - Gire a roleta e ganhe 99, 111, 222, 333, 555 ou 999 satoshis, via epay, a cada 5 (cinco) minutos: http://free-bitcoin.org/.

Moon Bitcoin - Satoshis a cada 5 (cinco) minutos. Pagamento direto semanal ou via Xapo: http://moonbit.co.in/.

GoldFaucet.com - Entre 160 a 210.970 satoshis, via ePay, a cada 5 (cinco) minutos: http://goldfaucet.com/.

Bitcoin-Free.net - Entre 96 a 4348 satoshis, via ePay, a cada 5 (cinco) minutos: http://bitcoin-free.net/.

Fast BTC - 250 satoshis, via FaucetBOX, a cada 4 (quatro) minutos: http://fastbtc.net/?r=1F697nwkkozRnuXN8CqfDRbtudYg3sYXAA.

FastBTC Club - 250 satoshis, via FaucetBOX, a cada 4 (quatro) minutos: https://fastbtc.club/?p=free_bitcoin.

QuickFaucet.com - Entre 93 a 42.194 satoshis, via ePay, a cada 3 (três) minutos: http://quickfaucet.com/.

NinjaFaucet.com - Entre 105 a 42.194 satoshis, via ePay, a cada 3 (três) minutos: http://ninjafaucet.com/.

Free CryptoCoin - Entre 105 a 422 satoshis, via ePay, a cada 1 (um) minuto: http://freecryptocoin.com/.

Land of Bitcoin - Cadastre e deixe a página carregada que os satoshis vão aparecendo. Necessário reclicar periodicamente: https://www.landofbitcoin.com/.

Wbit.co - Valores diversos e mantendo a página aberta vão acumulando. Paga quando atingir 6.000 satoshis: http://www.wbit.co/?id=381464.

Field Bitcoins - Valores diversos e mantendo a página aberta vão acumulando: http://fieldbitcoins.com/?ref=26zbd24z80779.

WeUseCoins Bitcoin Faucet (https://www.weusecoins.com/en/get-free-bitcoins/) – Consiga bitcoins grátis, que são disponibilizados por patrocinadores.

Coin Ad - Ganhe bitcoin por clicar em anúncios e visitar websites por 10 a 30 segundos: https://coinad.com/?r=D15CEIYNLFHYAGJ.

BTCClicks (https://btcclicks.com/) - Ganhe bitcoins para clicar em anúncios.

World of Bitcoin (http://www.world-of-bitcoin.com/) - Paga bitcoins pela visualização de anúncios.

BITCOINGET (http://www.bitcoinget.com/) - Ganhe bitcoins, completando tarefas, respondendo pesquisas e muito mais.

Coinchat (https://coinchat.org/) é uma comunidade onde se pode discutir sobre qualquer coisa interessante e ser recompensado com pequenos pedaços de Bitcoin.

YABTCL – Loteria (site de apostas) - https://yabtcl.com/userAccount.aspx?lng=pt.

JsiBitBot (http://jsibitbot.soft112.com/) é uma ferramenta desenhada para automatizar sites que pagam bitcoins por tarefas.

Infra vários links de listas de *faucets*:

- http://1000r.tk/;
- http://givemecoin.net/;
- http://bit.makejar.com/;
- http://bitcoin115.com/;
- http://cointasker.com/;
- http://bitcoiner.net/list;
- http://freebitcoins.eu/;
- http://coinsgratis.com/;
- http://bitcoinmonkey.org/;
- http://bitcoinfaucetrelay.com/;
- http://satoshi.bravesites.com/;
- http://www.bitcoingratis.com.br/;
- http://netcoinage.com/faucets.htm;
- http://www.freecrypto.co/directory;
- http://www.bitcoinsgratis.com.es/;
- http://www.fauceting.com/faucets;
- https://myfreebtc.wordpress.com/;
- http://www.dailycoins.net/bitcoin.html;
- http://bitcoinbarrel.com/free-bitcoins/;
- http://www.bitcoinrotators.com/u/fireblond;
- https://bitcoingratisparati.wordpress.com/;
- http://moneyinpjs.com/faucet-list/freebitcoin.php;

- https://sites.google.com/site/200000satoshvcas/;
- http://usebitcoins.info/index.php/bitcoin-related/32-bitcoin-free;
- http://topbitcoingratis.blogspot.com.br/ (menu à esquerda);
- http://www.coinbrasil.net.br/p/blog-page_5.html;
- http://fidanzatedinerd.altervista.org/bitcoin/#;
- http://mundoinfo.org/ganhar-bitcoins-gratis-lista-de-sites/;
- http://www.bitcoinaliens.com/top-10-free-bitcoin-faucets/;
- http://comefaresoldi.club/lista-migliori-bitcoin-faucet-gratis/;
- http://claimbitcoins.blogspot.com.br/p/free-bitcoins-websites.html;
- http://blog.clickgratis.com.br/seubitcoin/601262/ganhar-bitcoins.html;
- http://www.bitcoinnews.com.br/bitcoinbrasil/como-ganhar-bitcoin-gratis/;
- http://www.bitcoingratis.com.br/2013/12/mineirar-litecoin-e-bitcoin.html;
- http://bestbitcoin.com.br/bitcoin-gratis-saiba-como-ganhar-bitcoin-de-graca/;
- http://bitgolden.blogspot.com.br/p/bom-espero-que-tenha-gostado-dessas.html;
- http://musriady.blogspot.com.br/2014/12/daftar-situs-tambang-bitcoin-gratis.html;
- http://www.bitcoingratis.com.br/2015/07/bitcoin-gratis-melhores-faucets-BTC.html;
- http://dinheiropragelada.com/dinheiro/como-ganhar-bitcoins-de-graca-a-lista-absoluta/;
- http://ganhoextracomcliques.blogspot.com.br/p/g-bitcoin-e-moeda-que-mais-cresce-no.html.

E a listagem exemplificativa de *faucets* continua:

• http://bitcoiner.net/;	• http://btcclicks.com/;
• http://bitcoinfaucet.tk/;	• http://www.freebitoin4you.ga/;
• http://dailybitcoins.org/;	• http://bitcoiner.net/list;

• http://www.dailybitcoins.org/;	• http://coinreaper.com/;
• http://bitcoin-faucet.eu;	• http://bitcoinsblue.com/;
• http://777bitco.in/;	• http://www.bitcoin-gator.com/;
• http://goldsday.com/;	• http://coincheckin.com/Main/re;
• https://btc4you.com/;	• http://bitcoin-free-faucet.eu/;
• http://win-free-bitcoins.eu/;	•

Também existem faucets em forma de jogos, como, por exemplo, o **Wonderland Coin Game** (http://www.wonderlandco.in/); um jogo onde tem que alimentar os bichos a cada 5 minutos.

- http://www.robotcoingame.com/;
- http://www.spellsofgenesis.com/;
- http://pt.freegamesmax.com/acao/bitcoin-miner;
- http://1stcrypto.com/tag/bitcoin-mining-game/;
- https://www.coinbrawl.com/;
- http://bitplay.today/;
- https://primedice.com/welcome;
- http://www.bestbitcoingames.com/;
- http://www.baixaki.com.br/android/download/bitcoin-billionaire.htm;
- https://www.cryptocoinsnews.com/deckbound-competitive-card-game-based-bitcoin-blockchain/;
- http://insidebitcoins.com/news/sarutobi-drops-bitcoin-as-in-game-currency-integrates-breadwallet-support/33023;
- http://bitcoinchaser.com/bitcoin-apps;

- http://bitcoingamelist.com/;
- https://en.bitcoin.it/wiki/Category:Games;
- http://cryptomining-blog.com/tag/bitcoin-ios-game/;
- http://bitcoinbarrel.com/bitcoin-games/;
- http://cryptorials.io/earn-bitcoin-playing-fun-games-no-deposit-needed/;
- https://cryptogames.io/;
- http://1stcrypto.com/tag/play-game-for-bitcoin/;
- http://1stcrypto.com/category/bitcoin-games/;
- http://cryptomining-blog.com/tag/sarutobi-bitcoin/;
- http://www.bitcoinnews.com.br/bitcoinbrasil/games-ios-e-android-para-ganhar-bitcoins-ohcrop/.

O QUE É MINERAÇÃO DE BITCOIN?

A mineração do Bitcoin ("Bitcoin miner" ou “mining de Bitcoins”) é o processo de utilização de computadores para fazer cálculos matemáticos para a rede P2P do Bitcoin, a fim de confirmar transações (*transactions*), registrá-las na *Blockchain* (cadeia de blocos) e aumentar a segurança da rede Bitcoin através da confirmação da autenticidade das transações. Como recompensa pelos serviços, os mineiros (*miners*) do Bitcoin recebem taxas (*fees*) de transação (*transaction*) pelas operações que eles confirmam e, ainda, podem “levar a sorte grande” e serem contemplados com bitcoins pelo bloco recém-criado. A mineração é um mercado competitivo onde os rendimentos são divididos em função do número de cálculos efetuados. Nem todos os usuários do Bitcoin fazem mineração (*mining*) e não se trata de uma maneira fácil de ganhar dinheiro.

Mining é o processo de adição de registros de transações de contabilidade pública da Bitcoin de transações passadas. Esse livro-caixa (*Blockchain*) das operações passadas é chamada de cadeia de blocos. A cadeia de blocos serve para confirmar as transações para o resto da rede como tendo ocorrido. E, ainda, para distinguir as transações legítimas das tentativas de gasto duplo (reutilização de unidades já utilizadas pelo titular).

Recordemos que ocasionalmente, o sistema (rede Bitcoin) emite um “hash” (sequência de bits criptografados) para ser decodificado ("quebrado"); então, inicia-se uma corrida pelos mineradores para ver quem consegue decifrar o *hash* (encontrar o *nonce* certo) primeiro, pois o vencedor terá bitcoins como recompensa. O minerador, ainda, poderá ficar com o troco das transações do bloco (que pode armazenar 1 megabyte de dados), caso cada pagador não exija antecipadamente a sua devolução.

Para poder resgatar sua recompensa, uma transação especial chamada de coinbase é incluída pelo minerador junto com os pagamentos que ele processou. O montante da recompensa foi programado para cair pela metade a cada 210.000 blocos minerados ou a cada quatro anos, o que ocorrer primeiro. Em 2009, o minerador recebia 50 bitcoins por cada bloco (*block*) minerado. Em 28/11/2012, o bloco de número 210.000 foi minerado e, assim, a recompensa caiu para 25 bitcoins por bloco. Em 09/07/2016, o

bloco de número 420.000 foi concluído e, desse modo, o valor da recompensa passou a ser de 12,5 bitcoins por bloco. Essa regra é apelida de **redução para a metade ou *halvening***. Detalhe, quando o limite arbitrário de 21 milhões de bitcoins produzidos for atingido, não existirá mais recompensa porque não existirá mais a criação de novas unidades de bitcoins; a partir desse momento, os mineradores receberão apenas as taxas (*fees*) das transações do bloco como recompensa pelo trabalho. O site http://bitcoinclock.com/ possui um relógio calculando a *halvening*.

Se o poder de mineração tivesse permanecido constante desde que a primeira bitcoin foi gerada, a última bitcoin seria extraída em 08/10/2140. Entretanto, em razão do constante aumento do poder de mineração, essa data prevista está diminuindo cada vez mais.

Atualmente, cada usuário é livre para escolher o quanto quer pagar em taxas aos mineradores a fim de que sua transação seja tomada como prioridade por eles. Por sua vez, o minerador é quem determina em certa medida a configuração do seu próprio nó da rede, estabelecendo de forma livre e competitiva a quais valores e tamanhos de transação ele dará prioridade no processamento, durante a formação dos novos blocos que tenta minerar.

O *nonce* é usado para variar o *output* (saída ou resultado) de uma função criptográfica e o *nonce* correto é que torna um bloco candidato em válido. Se o *hash* obtido não for menor do que o alvo (*target*), o minerador ficará modificando o *nonce* (geralmente somando o número 1) e tentará novamente até conseguir o resultado correto. Caso dois mineradores encontrem um *nonce* juntos, ou quase juntos, a rede terá dois blocos válidos em circulação. Eventualmente, um novo bloco será gerado, mas a rede Bitcoin referenciará apenas o *hash* de um bloco anterior (bloco pai). O bloco que sobrou, chamado de "bloco órfão", é descartado. Se a transação foi incluída apenas no bloco órfão, ele terá que ser novamente incluída em um bloco futuro. Recorda-se que todas as transações Bitcoins são incluídas nos blocos.

O bloco candidato é conferido pelos outros nós da rede P2P através da prova de trabalho. O algoritmo (*hashcash*) de prova de trabalho (*PoW* - *proof-of-work*) é que define o grau de dificuldade (*difficulty*) de mineração

da criptomoeda, sendo constantemente ajustado para manter a velocidade (em média 10 minutos) de confirmação das transações. A confirmação do resultado (do *nonce*) é uma prova de trabalho, pois prova o trabalho tido pelo minerador para encontrar esse *nonce*. Desse modo, uma dificuldade de 90000 significa que, para poder gerar o bloco atual, foram necessárias 90000 vezes mais trabalho do que Satoshi Nakamoto teve para gerar o primeiro bloco. Todos os blocos liberados que não atendam aos requisitos, serão, automática e simplesmente, rejeitados por todos os demais nós na rede Bitcoin.

Enfim, a mineração de bitcoins nada mais é que do que concluir um bloco e registrá-lo na *Blockchain* (cadeia de blocos). Recorda-se que os blocos não são bitcoins, mas tão somente o lote onde constam as transações em bitcoins; vez que o bitcoin é tão somente o nome dado aos créditos ou valores utilizados nessas transações.

Para confeccionar um bloco, os mineiros pegam os dados das transações (que estão sendo propagadas na rede e que ainda não foram inclusas em um bloco), as agrupam para serem inseridas no seu bloco candidato e, ainda, as resumem através do *nonce* em um *hash* (transformar alguma coisa em algo menor), contendo apenas as informações mais importantes. Depois de concluído o bloco, o *hash* é finalizado fazendo uma referência vinculativa e integrativa com o bloco anteriormente registrado (bloco pai) na *Blockchain*, servindo de prova de integridade. Por outras palavras, os mineradores não usam apenas as transações constantes do seu bloco candidato para gerar um *hash*, mas, também, uma conexão com o *hash* do último bloco guardado na *Blockchain*. Este *hash* é então armazenado juntamente com o bloco, o qual será registrado na *Blockchain*. Desse modo, o *hash* é o elo de ligação (amarração) entre um bloco e outro, é como se fosse a argamassa que une os tijolos que estão sendo assentados na construção de um muro ou parede. Portanto o trabalho dos mineiros é gerar *hashes*.

Na linguagem da informática, um *hash* é o resultado de uma operação matemática complexa, que é fácil de reproduzir, mas impossível de reverter e difícil de prever. Conforme visto no capítulo próprio, o *hash* consegue resumir, simplificar e agilizar, tanto em tempo como em espaço, qualquer informação. O *hash* é representado de forma hexadecimal com números de 0

a 9 e letras de A a F. Por exemplo, pelo site http://www.xorbin.com/tools/sha256-hash-calculator, as frases anteriores a esta foram convertidas em: b9f5c160fb723de6a7f79df424537d5c6bce6d582506b48d37930f0a3032baae.

Desse modo, a mineração Bitcoin é o processo de ficar fazendo *hashing* do cabeçalho do bloco (*block*), inúmeras e sucessivas vezes através do método de tentativa e erro, modificando aleatoriamente o *input* (entrada), até que o hash resultante (*output*, saída ou resultado) corresponda a um alvo específico (*nonce* correto). Para cada novo *hash* que é tentado, o *software* de mineração vai usar um número diferente, esse número é chamado de *nonce*. Com outras palavras, o objetivo da mineração é encontrar um valor para o *nonce* que resulte em um *hash* de cabeçalho de bloco menor do que a dificuldade alvo. O nodo (nó da rede Bitcoin) de mineração terá que testar bilhões ou trilhões de valores de *nonce* até encontrar um *nonce* que satisfaça as exigências.

Em síntese, o procedimento é similar à resolução de fórmulas matemáticas onde se pretende descobrir o valor do resultado x.

O engenheiro Ken Shirriff divulgou esse procedimento através de cálculos manuais com um lápis escrevendo numa folha de papel (https://www.youtube.com/embed/y3dqhixzGVo).

Diante dessas explicações, pode-se, enfim, dizer que não existe isso de bloco ser descoberto ou encontrado, mas tão somente ser gerado e reconhecido como válido. Em razão dessa exigência de o bloco ser autenticado e aprovado pelos pares (demais nós) da rede P2P do Bitcoin, é que se fala em bloco candidato. Por outras palavras, até que o bloco seja autenticado como válido pela rede Bitcoin, ele será apenas um bloco candidato. E se o bloco não for aprovado para ser registrado na *Blockchain* (cadeia de blocos), ele será um bloco órfão. Pelas mesmas razões acima, já podemos dizer que a rede Bitcoin não solta ou esconde bitcoins pela rede P2P para serem encontrados; muito menos existem pepitas de ouro virtuais para serem descobertas. Tais expressões não passam de força de linguagem para fins didáticos. Enfim, as “pepitas de ouro” ou bitcoins “lançadas”

constantemente na rede Bitcoin para serem mineradas são os blocos de transações. Em conclusão, bitcoins são criadas cada vez que um minerador registra um novo bloco recém-criado na *Blockchain*.

Para entender melhor, ou se profundar, sobre o que são as bitcoins e como elas são feitas, confira os capítulos: "*HASH*", "CERTIFICADOS DIGITAIS", "*PEER-TO-PEER* (P2P)", "BITCOIN", "COMO A BITCOIN É FEITA?", "*BLOCKCHAIN*" e "COMO MINERAR BITCOINS E ALTCOINS".

COMO MINERAR BITCOINS E ALTCOINS

Antes de decidir a minerar alguma altcoin deve-se conferir se a mesma permite mineração, vez que algumas são totalmente pré-minadas (*100% premined* ou *full premined*); ou seja, não se pode minerá-las. Além disso, deve conferir se existe uma limitação de quantidade de moedas a serem emitidas e se já atingiu esse limite ou se falta pouco para atingir. Outros detalhes são os graus de dificuldade para a emissão e a respectiva recompensa pela geração da moeda. Essas informações mudam com muita frequência; com o que não é possível ter todo um trabalho de pesquisa, organização e divulgação para correr o enorme risco de divulgar algo desatualizado ou modificado. Existe uma dica comumente dada para os iniciantes; qual seja, toda informação com mais de 6 (seis) deve ser totalmente desprezada e, as que tiverem mais de 3 (três) meses, devem ser vistas com desconfiança. Desse modo, nos canais próprios de comunicação, anúncios, divulgações e atualizações das respectivas moedas é que se deve procurar tais informações.

- *Mining difficulty* (dificuldade de mineração) na rede Bitcoin em https://tradeblock.com/bitcoin/historical/1d-f-diff_avg-01071-blksize_per_avg-01071;

- *Hash rate* (taxa de hash) - https://tradeblock.com/bitcoin/historical/1d-f-hashr_avg-01071-blksize_per_avg-01071;

- *Bitcoin issued total* (total de bitcoins emitidas) - https://tradeblock.com/bitcoin/historical/1d-f-xbtiss_per_tot-01071-blksize_per_avg-01071;

- *Blocks mined total* (total de blocos minados) https://tradeblock.com/bitcoin/historical/1d-f-blk_per_tot-01071-blksize_per_avg-01071;

- Piscinas de mineração Bitcoin: https://bitcoinchain.com/pools.

A mineração de uma moeda digital é algo diferente para cada criptomoeda e em constantes mudança e evolução. Muda-se periodicamente a dificuldade de mineração e novos e modernos *hardwares* são lançados frequentemente.

Para minerar o Bitcoin ou outra moeda virtual (altcoin) gratuitamente, há a opção de fazer isso direto através de computador, notebook (com excelente placa de vídeo e/ou processador), *tablet*, *smartphone* e, até mesmo, com eletrodomésticos inteligentes (exige conhecimento avançado de informática) que se conectam à Internet. Em ambos aparelhos é necessário instalar um *software* (programa) ou aplicativo (em caso de *tablet* ou *smartphone*) de mineração, e/ou utilizar-se de mineração em nuvem (seja através de conta gratuita e/ou pagando com Bitcoins ganhados da Internet).

- http://www.tecmundo.com.br/bitcoin/66169-eletrodomesticos-alvos-ataques-hackers-mineracao-bitcoins.htm;
- http://canaltech.com.br/noticia/seguranca/Hackers-estao-usando-eletrodomesticos-inteligentes-para-minerar-bitcoins/;
- http://info.abril.com.br/noticias/seguranca/2014/11/hackers-estao-usando-torradeiras-e-geladeiras-para-minerar-bitcoins.shtml;
- http://olhardigital.uol.com.br/noticia/aparelhos-com-android-fabricam-bitcoin-sem-usuarios-saberem/41078;
- http://www.linhadefensiva.org/2013/04/praga-brasileira-garimpa-bitcoins-com-maquina-infectada/;
- http://gizmodo.uol.com.br/funcionario-de-liga-de-jogos-online-transformou-14-000-usuarios-em-zumbis-que-mineravam-bitcoins/.

Conforme exposto nos capítulos "COMO A BITCOIN É FEITA?" e "O QUE É MINERAÇÃO DE BITCOIN?" para minerar bitcoin exige-se a instalação de um *software* (programa de computador) específico, tal como se fosse uma carteira *software* ou *desktop*, trata-se do *software* cliente, na versão nó completo (*full node*).

- https://bitcoin.org/pt_BR/download;
- https://bitcoin.org/en/full-node#linux-instructions;
- https://bitcoin.org/en/full-node#windows-8x;

- https://bitcoin.org/en/full-node#mac-os-x-instructions.

A versão nó completo é aquela que efetua o *download* completo da *Blockchain* (*datacenter* ou banco de dados do Bitcoin) e a mantém atualizada e sincronizada; bem como valida as transações e blocos e depois os retransmite para os outros nós completos da rede P2P do Bitcoin. Recorda-se que para que as transações sejam confirmadas, elas precisam ser incluídas em um bloco juntamente com uma prova matemática de trabalho. Isso é a mineração.

- http://pt.wikihow.com/Minerar-Bitcoins.

A mineração solo consiste em uma pessoa usar somente o seu poder de processamento local, via CPU - *Central Processing Unit* (Unidade Central de Processamento ou processador) ou GPU - *Graphics Processing Unit* (Unidade de Processamento Gráfico ou placa de vídeo), para tentar sozinho decifrar e criar um novo bloco na *Blockchain*. Essa modalidade de mineração é totalmente inviável no Bitcoin; pois usará mais energia elétrica do que a máquina terá capacidade de gerar em bitcoin, então ter-se-á apenas prejuízo. Essa modalidade de mineração só é rentável em operações de larga escala e com preços baixos de energia, como no Paraguai, por exemplo. Também é viável em altcoins novas, que ainda não tenham equipamentos específicos de mineração em uso, que somente permitam mineração via GPU ou que impossibilitem o uso de equipamentos específicos de mineração. Sugere-se pesquisar a respeito, as criptomoedas Ethereum (https://www.ethereum.org/), Litecoin (https://litecoin.org/pt/) e Feathercoin (https://www.feathercoin.com/).

- http://www.criptomoedasfacil.com/2016/07/guia-basico-como-minerar-ethereum.html.

O quanto de *hash* uma CPU ou uma GPU pode gerar não é fixo, pois varia de moeda para moeda. Entretanto quanto melhor for a CPU ou a GPU, mais hash ela gerará e mais cara também será.

Uma dica para a mineração solo, portanto, é evitar as criptomoedas que usam algoritmos de hash que possibilitam ASIC: SHA-256, Scrypt, X11,

Quark, Qubit, etc.

Monero é uma moeda CPU, cujo algoritmo de *hash* é projetado para tornar difícil a mineração em GPU e, muito mais ainda, em ASIC.

Cada criptomoeda possui seu software (programa de computador) de mineração, cada qual com suas próprias vantagens e desvantagens diante das especificações da respectiva criptomoeda (algoritmo de hash, método de consenso, etc.). Explica-se. O software de mineração analisa as transações transmitidas através da rede ponto a ponto da respectiva moeda digital e executa as tarefas apropriadas para processar e confirmar essas transações. As pessoas que realizam esse trabalho (na verdade os computadores dessas pessoas) são denominadas de mineiros.

Normalmente após baixar o arquivo de instalação, que costuma ser compactado (Winrar, por exemplo), costuma ser necessário criar uma pasta com o nome dele (exemplos: Guiminer ou Bfgminer) dentro da pasta "Arquivos de programas" (ou “Program Files”) ou onde o minerador bem quiser. Antes de abrir o arquivo, deve-se fazer uma varredura com antivírus e anti-*malware* nele (exemplo, o software minerador "50miner" foi conhecido por conter *trojan*). E, em não sendo encontrado nenhum código, algoritmo ou programa malicioso ou após eliminá-lo(s), descompactasse o programa para dentro da pasta recém-criada para ele. Depois deve-se dar dois cliques no arquivo com a terminação ".exe". Vai ser aberta a tela inicial do programa. Em caso de software de mineração em *pool* (piscina) costuma ser aberta a janela do prompt de comando do DOS pedindo o endereço de URL, TCP, "hostname", "server host name" e até mesmo o endereço IP da *pool* (piscina) onde o minerador deve estar previamente cadastrado. Todos os dados de configurações específicas são fornecidos no anúncio e no site da própria moeda, bem como no site da piscina. Por óbvio deve-se tratar de uma piscina sobre a moeda digital desejada ou, no caso de uma piscina de várias moedas, da configuração específica da moeda escolhida. No site do YouTube existem vários videotutoriais de como instalar e configurar referidos programas.

Para que as novas transações sejam confirmadas, elas precisam ser incluídas num bloco candidato juntamente com uma prova matemática de

trabalho (*PoW* - *Proof of Work*). Tais provas são muito difíceis de gerar porque não há uma fórmula ou receita para criá-las, a não ser através de sucessivas tentativas, realizando milhões de cálculos por segundo. Isso requer que os mineradores realizem tais cálculos antes que os seus blocos sejam aceitos pela rede e antes de serem recompensados. A prova de trabalho também é projetada para depender do bloco anterior para forçar uma ordem cronológica na cadeia de blocos. Isso torna exponencialmente difícil reverter operações anteriores, já que isso exigiria o recálculo das provas de trabalho de todos os blocos subsequentes. Quando dois blocos se encontram ao mesmo tempo, os mineiros trabalham sobre o primeiro bloco que receber e exibem a cadeia mais longa de blocos logo que o bloco seguinte é encontrado. Isso permite que a mineração garanta e mantenha um consenso global com base no poder de processamento.

Existem muitos programas que podem ser utilizados, mas os mais populares são o CGminer (https://bitcointalk.org/index.php?topic=28402.0) e o BFGminer (http://bfgminer.org/), que são programas de linhas de comandos. Já quem prefere uma interface mais fácil, pode experimentar o EasyMiner (http://www.easyminer.eu/).

Os programas de mineração Bitcoin ("software mining bitcoin") mais populares são:

- CGminer (https://guiminer.org/ e http://ck.kolivas.org/apps/cgminer/);
- BFGminer (http://bfgminer.org/);
- EasyMiner (http://www.butterflylabs.com/drivers/);
- Phoenix (https://github.com/phoenix2/phoenix);
- DiabloMiner (https://github.com/Diablo-D3/DiabloMiner);
- Minergate (https://br.minergate.com/downloads/gui);
- Awesome Miner (http://www.awesomeminer.com/download.aspx).

CGminer (https://github.com/ckolivas/cgminer) é o software de mineração mais popular. Este software inclui *overclocking*, monitoramento, controle de velocidade e capacidade de interface remota. Suas outras

características incluem autodetecção de novos blocos com um mini-banco de dados, carregamento binário de kernels e suporte multi GPU e CPU.

GUIMiner (http://guiminer.org/) é essencialmente uma interface gráfica que pode controlar múltiplas aplicações de mineração diferentes ao mesmo tempo. Ele suporta tanto GPUs AMD e NVIDIA; bem como mineração CPU. Também pode-se escolher entre mineração reunida ou mineração solo. O software, ainda, incorpora uma lista de *pools* (piscinas) de mineração para escolher.

BitMinter (https://bitminter.com/). Podemos dizer que, embora BitMinter pode não ser o software de mineração mais popular, é certamente um dos melhores quando se trata de se conectar com os usuários e potenciais "clientes". O site oficial do software é bastante completa e clara: para os criadores do programa, é tudo sobre como fazer mineração Bitcoin "fácil" e ganhar "pagamentos elevados". BitMinter é diferente porque é um software que pertence a um pool de mineração, para que o seu primeiro passo é registrar e preencher o formulário de inscrição grupo. Então, é uma ótima opção se você está procurando uma instalação simples. Além de estar disponível para os sistemas operacionais como Windows, Linux e Mac OS X, BitMinter garante uma boa velocidade de mineração e longa votação, a fim de reduzir o trabalho obsoleto. Ele também permite que você a mina em GPUs ou ASICs OpenCL compatíveis / FPGAs (BFL, Bloco Erupter e outros Icarus-compatíveis).

BTCMiner (http://www.ztex.de/btcminer/#download). Esta fonte Bitcoin software de mineração aberto para ZTEX USB-FPGA Módulos 1,15 roda em sistemas operacionais Linux e Windows. No entanto, os usuários do Windows precisam instalar o driver libusb primeiro. As placas FPGA apoiados por BTCMiner (USB-FPGA Módulos 1,15bi e 1.15d, USB-FPGA Módulos 1.15x e USB-FPGA Módulos 1.15y). Tem uma interface USB, que pode ser usada para comunicação e programação, permitindo que o usuário construa clusters de baixo custo FPGA com componentes padrão (como hubs USB, por exemplo). Em termos práticos, isso significa que nenhum programador JTAG é necessário e o programa permite executar grandes equipamentos de mineração a partir de apenas uma instância de software. O software possui um ready-to-Bitstream, que não requer qualquer software

Xilinx ou uma licença, então isso é uma vantagem. No entanto, sua escala de frequência dinâmica é baseada na medição de erro: assim, BTCMiner escolhe automaticamente a frequência com a maior taxa de hashes válidos.

O algoritmo de *hash* mais popular foi o que começou tudo, SHA-256, que originalmente estreou como algoritmo de *hash* de Bitcoin. Com a introdução do Litecoin, o Scrypt entrou em cena e veio com seu próprio conjunto de prós e contras, mas é de longe um dos algoritmos mais populares na existência. Desde então, muitos outros algoritmos tomaram cena no palco das criptomoedas: X11, X12, X13, X14, X15, x17, Scrypt-N, Scrypt-ChaCha, Groestl, Keccak, NIST5 e muitos outros.

O Groestl é utilizado pela GRS - Groestlcoin (http://www.groestlcoin.org/) e pela DMD - Diamond (http://bit.diamonds/).

O site http://www.coinwarz.com/cryptocurrency mostra diferentes tipos de algoritmos de mineração de criptomoedas.

Por óbvio, pelo fato de que o minerador irá receberá bitcoins pelo trabalho realizado, será necessário possuir uma carteira (par de chaves). Porém, o próprio *software* cliente, também é um *software* carteira. Portanto, pode-se usar o Bitcoin Core simplesmente como carteira ou pode-se simplesmente deixá-lo ligado, conectado e trabalhando em benefício da rede Bitcoin.

Entretanto, já fazem anos que produzir sozinho bitcoins (*solo mining*, *solo miner*, mineração solo ou minerador sozinho) pelo computador (seja usando a CPU ou a placa de vídeo) implica em uma conta energética maior do que se consegue ganhar com a mineração. Mesmo que seja através de um *hardware* customizado para mineração (ASICs - *Application-specific integrated circuit chips* ou chips de circuitos integrados de aplicação específica); vez que quanto mais potente o equipamento, maior será o consumo de energia elétrica. Isso sem levar em consideração do custo do equipamento, da energia elétrica para refrigerar o mesmo e da conta de Internet. Já se a mineradora estiver instalada onde a energia elétrica é barata (exemplo, Paraguai) ou, até mesmo, gratuita (exemplo, Chile, onde o governo

capta e fornece energia solar), a questão passa a envolver apenas os custos do equipamento e da conta de Internet.

- http://brasil.elpais.com/brasil/2015/09/10/politica/1441837292_242802.html;
- http://exame.abril.com.br/economia/chile-tem-tanta-energia-solar-que-agora-e-de-graca/.

Outra observação, é que ao contrário do Bitcoin, outros sistemas ainda são viáveis para a mineração solo e, até mesmo, através de um computador doméstico simples. Inclusive, existem moedas digitais que bloqueiam a possibilidade de mineração por equipamentos muito potentes.

Uma recomendação para a mineração solo é, em regra, evitar moedas digitais que usem o método de consenso PoW - *Proof of Work* (prova de obra ou de trabalho); vez que ele exige poder computacional e, portanto, normalmente são ideais para equipamentos ASIC. Não confundir com código ou tabela ASCII. As exceções constam das considerações acima. Alguns outros algoritmos de *hashing*, que são utilizados para a PoW incluem SHA-256, Scrypt, Blake-256, CryptoNight, HEFTY1, Quark, SHA-3, Scrypt-Jane, Scrypt-N, etc. Desse modo SHA-256 é PoW, mas nem todo PoW é SHA-256. Confira uma listagem exemplificativa de criptomoedas PoW em https://minkiz.co/coin/cmcap-pow. Saiba mais no capítulo "MÉTODOS DE CONSENSO".

Burst (https://www.burst-team.us/) é um clone da Nxt (https://nxt.org/), mas não usa a prova de jogo. Seu algoritmo de prova de capacidade permite que as pessoas minerem em casa, vez que se concentra no espaço em disco rígido ao invés de em processadores rápidos.

MarteXcoin (http://martexcoin.org/), uma criptomoeda brasileira, é a primeira criptomoeda x13 hibrida; ou seja, que minera PoW e PoS simultaneamente. Ainda mais, não possibilita a mineração por ASIC e grandes centros de mineração.

Lista exemplificativa de algumas altcoins para mineração através de CPU (***CPU mining***):

- Primecoin (http://primecoin.io/);
- MemoryCoin (https://bitcointalk.org/index.php?topic=370806.0);
- Skeincoin (http://www.skein-hash.info/);
- Aeon (http://www.aeoncoin.org/);
- Boolberry (http://boolberry.org/);
- Bytecoin (https://bytecoin.org/);
- Dash (https://www.dash.org/);
- DigitalNote (http://digitalnote.org/);
- Fantomcoin (http://fantomcoin.org/);
- Givecoin (http://2givecoin.info/);
- Global Denomination (https://bitcointalk.org/index.php?topic=578574.0);
- GroestlCoin (http://www.groestlcoin.org/);
- Hirocoin (https://bitcointalk.org/index.php?topic=516349.0);
- JackpotCoin (https://bitcointalk.org/index.php?topic=584481.0);
- Logicoin (https://bitcointalk.org/index.php?topic=567114.0);
- MemoryCoin (https://bitcointalk.org/index.php?topic=370806.0);
- Monero (https://getmonero.org/);
- Moneta Verde (https://bitcointalk.org/index.php?topic=653141.0);
- New Universal Dollar (https://bitcointalk.org/index.php?topic=640933.0);
- QuazarCoin (https://bitcointalk.org/index.php?topic=615732.0);
- Riecoin (http://riecoin.org/);
- Slimcoin (https://bitcointalk.org/index.php?topic=1141676.0);
- QubitCoin (http://www.qubitcoin.com/);
- Datacoin (http://datacoin.info/);
- Chaincoin (http://www.chaincoin.org/);
- FairQuark (https://github.com/jdgdredd/FairQuark);
- Frozen (https://bitcointalk.org/index.php?topic=366762.0);
- BitShares [anteriormente ProtoShares] (https://bitshares.org/);
- SecureCoin (http://securecoin.org/);
- YACoin - Your alternative currency (https://www.yacoin.org/);
- Vertcoin (https://vertcoin.org/);
- C-Note (https://bitcointalk.org/index.php?topic=397916.0);
- Ducats (https://cryptocointalk.com/topic/3321-ducats-duc-information/);
- Offerings to Cthulhu (https://bitcointalk.org/index.php?topic=294383.0);
- Quarkcoin (http://www.quarkcoins.com/);
- Skeincoin (https://github.com/skeincoin/skeincoin-cpuminer).

Existem sites com **calculadoras de rentabilidade da mineração** Bitcoin (*Bitcoin mining calculator*) e de outras criptomoedas:

- http://www.coinwarz.com/calculators/bitcoin-mining-calculator;
- https://btcserv.net/bitcoin-mining-calculator;
- https://alloscomp.com/bitcoin/calculator;
- https://bitcoinwisdom.com/bitcoin/calculator;
- http://www.coinwarz.com/cryptocurrency;

- https://whattomine.com/calculators;
- https://whattomine.com/coins;
- http://www.bitcoinx.com/profit/;
- http://bitcoin.web-share.nl/;
- http://beta.ivc.no/bitcoin/calc/;
- http://coinish.com/bitcoin-mining-calculator/;
- https://www.cryptocompare.com/mining/calculator/btc;
- http://www.vnbitcoin.org/bitcoincalculator.php;
- http://bitcoin.web-share.nl/#;
- http://bitcoinminingcalculator.org/;
- https://bitjohny.com/MiningCalc/Bitcoin/;
- http://www.alcula.com/calculators/finance/bitcoin-mining/;
- https://99bitcoins.com/bitcoin-mining-calculator/;
- http://btcinvest.net/en/bitcoin-mining-profit-calculator.php;
- https://bitcoinchain.com/mining-calculator;
- https://mining-profit.com/;
- http://tpbitcalc.appspot.com/;
- http://blockchained.com/profit/;
- https://en.bitcoin.it/wiki/Profitability_Calculator;
- https://www.litecoinpool.org/calc;
- https://bitmakler.net/Litecoin mining;
- http://www.litecoinminingcalculator.com/;
- https://99bitcoins.com/c/ltc/mining.

O NeoScrypt é utilizado pela FTC - Feathercoin (https://www.feathercoin.com/), UFO - UFOcoin (http://ufocoin.co/), ORB -

Orbitcoin (http://www.orbitcoin.org/) e PXC - Phoenixcoin (http://phoenixcoin.org/).

Bytecoin (https://bytecoin.org/) foi a primeira criptomoeda que usa um algoritmo de mineração chamado **CryptoNight**; que é um algoritmo de prova de obra (PoW). Ele é projetado para ser adequado para CPUs (PCs comuns). Portanto, qualquer criptomoeda que usa o algoritmo CryptoNight pode ser eficazmente extraída com uma CPU. Desse modo, o Bytecoin diz bloquear a mineração através da GPU. **CryptoNote** (https://cryptonote.org/ e https://en.wikipedia.org/wiki/CryptoNote) é uma tecnologia para criação de criptomoedas, que dá suporte a várias moedas digitais. **Monero** (https://getmonero.org/), anteriormente conhecido como Bitmonero, é uma das primeiras moedas CryptoNote. Já a AEON - *Anonymous Eletrônico On-line* (https://bitcointalk.org/index.php?topic=641696.0) é um *fork* da Monero. **Dash** (https://www.dash.org/), por sua vez, é um *fork* do Bytecoin e, desse modo, também utiliza o algoritmo CryptoNote. A **Boolberry** (http://boolberry.org/) é um experimento CryptoNote. A DarkNetSpace (http://www.darknetspace.org/) é baseada na Boolberry, mas usa função hash Keccak vez de CryptoNight. DigitalNote (http://digitalnote.org/), conhecido anteriormente como DarkNote e duckNote, também utiliza a tecnologia CryptoNote. Pebblecoin (https://bitcointalk.org/index.php?topic=909624.0) é uma moeda baseada em CryptoNote com certos ajustes. Quazarcoin (https://bitcointalk.org/index.php?topic=615732.0) é outra moeda baseada em CryptoNote.

Fantomcoin (http://fantomcoin.org/) é a primeira moeda CryptoNote com o apoio de mineração resultante da fusão. Desse modo, além da própria, é possível minerar Bytecoin (BCN), Monero (MRO) ou QuazarCoin (QCN).

Outras moedas CryptoNotes são:

- DoctorByte (https://bitcointalk.org/index.php?topic=901685.0);
- Infinium-8 (https://bitcointalk.org/index.php?topic=698727.0);

- MonetaVerde (https://bitcointalk.org/index.php?topic=657820.0);
- Dosh (https://cryptocointalk.com/topic/14220-dosh-information/);
- Magnatoj (https://bitcointalk.org/index.php?topic=1270755.0);
- RedWind (https://bitcointalk.org/index.php?topic=904485.0);
- Tavos, que virou NX-Tavos (https://bitcointalk.org/index.php?topic=1126558.0).

A maneira mais simples de extrair moedas Cryptonote é usando o Minergate (https://br.minergate.com/).

No Ethereum (https://www.ethereum.org/), com seu Ethash, não é possível minerar usando AISC e Antminers. Apenas CPU ou GPU (*Graphical Processing Unity*), porém CPU *mining* não é mais rentável devido à dificuldade atual. O Ethash usa o algoritmo Dagger-Hashimoto, que consome bastante memória do *hardware* para carregar o DAG file, um arquivo que calcula previamente a dificuldade de acordo com a época; ou seja, quanto mais distante do bloco gênesis, maior será a dificuldade.

A mineração via GPU pode ser feita nos algoritmos de hash: Ethash, Groestl, Chacha (Nf14), CryptoNight, Equihash, Lyra2Rev2, NeoScrypt, LBRY, Blake (2b), Blake (14r), Blake (XVC), etc. Saiba mais no capítulo "ALGORITMO DE HASH".

O X11 era uma ótima escolha para os mineiros que usam GPU (*Graphical Processing Unity*), pois o desempenho do X11 é melhor na GPU. O DASH (https://www.dash.org/mining/) usa o algoritmo X11. Entretanto, como já existem ASIC para o X11, talvez essa disputa se já não está perdida, logo estará. O vencedor dependerá de qual hardware vai ficando mais eficaz durante a corrida armamentista.

- http://cryptomining-blog.com/8266-first-impressions-from-the-baikal-mini-miner-asic/.

Em http://bitcoin-brasil.com/comparacao-de-placas-de-video/ existe uma listagem comparativa de placas de vídeo. Já o ASIC funciona em *hashing algorithm* como: SHA-256, Scrypt, X11, Quark, Qubit, etc. Portanto, onde o ASIC opera, a mineração solo tende a se tornar ineficaz.

O algoritmo Scrypt funciona em GPU e as moedas Litecoin e Dogecoin usam o Scrypt. O Scrypt exige muita memória e as GPUs são projetadas para esse tipo de dificuldade enquanto que as máquinas ASICs não são. Entretanto, a mineração Scrypt exigem muita energia elétrica e, eventualmente, as maquinas ASIC - Scrypt são projetadas para resolver este problema.

As placas de vídeo AMD possuem uma arquitetura melhor que a NVIDIA o que as torna a melhor opção para mineração GPU. Entretanto, apesar de que a placa de vídeo Nvidia GeForce GTX 1050 Ti (chip Pascal GP107, GPU clock 1290, GPU turbo 1392, 4 GB de memória GDDR5 e 7 Gbps de velocidade de memória) pode não ser a solução mais poderosa para a mineração, o interessante dela é seu menor consumo de energia elétrica (limite de TDP de 75W).

- http://www.clubedohardware.com.br/artigos/video/teste-da-placa-de-vídeo-zotac-geforce-gtx-1050-ti-mini-r36635/.

Confira uma lista de GPUs e suas características em http://mininghwcomparison.com/list/index.php?brand=both; bem como no site: https://www.whattomine.com/coins.

Infra alguns exemplos de mineração via GPU (***GPU mining***); bem como de como são feitos os anúncios (ANN - *announcement*) de lançamento (*launch*) das moedas na comunidade virtual:

- Animecoin (https://bitcointalk.org/index.php?topic=423339.0);
- Atomo (https://github.com/moleculecoin/atom);

- Badgercoin (https://bitcointalk.org/index.php?topic=585796.0);
- Bitquark (http://www.bitquark.info/);
- C-Note (https://bitcointalk.org/index.php?topic=397916.0;all);
- Chaincoin (http://www.chaincoin.org/);
- Dash (https://www.dash.org/);
- Datacoin (http://datacoin.info/);
- Dougcoin (https://bitcointalk.org/index.php?topic=464267.0);
- FairQuark (https://github.com/jdgdredd/FairQuark);
- Fatecoin (https://bitcointalk.org/index.php?topic=468889.0);
- Frozen (https://bitcointalk.org/index.php?topic=366762.0);
- Hashcoin (https://bitcointalk.org/index.php?topic=568453.0);
- HighFiveCoin (https://bitcointalk.org/index.php?topic=558286.0);
- Heavycoin (http://heavycoin.github.io/);
- Juggalocoin (https://bitcointalk.org/index.php?topic=555896.0);
- Kryptonite (https://bitcointalk.org/index.php?topic=606682.0);
- LimeCoin (https://bitcointalk.org/index.php?topic=579604.0);
- Marucoin (https://bitcointalk.org/index.php?topic=570744.0);
- Megcoin (https://bitcointalk.org/index.php?topic=594886.0);
- Metacoin (https://bitcointalk.org/index.php?topic=454848.0);
- Metiscoin (https://bitcointalk.org/index.php?topic=424517.0);
- Minicoin (https://bitcointalk.org/index.php?topic=429105.0);

- Molecule (https://bitcointalk.org/index.php?topic=371576.0);
- MountCoin (https://bitcointalk.org/index.php?topic=658072.0);
- Muniti (https://bitcointalk.org/index.php?topic=545886.0);
- Myriadcoin (http://myriadcoin.org/en/home);
- Netll Coin (https://bitcointalk.org/index.php?topic=425267.0);
- NoirShares (https://bitcointalk.org/index.php?topic=565623.0);
- Offerings to Cthulhu (https://bitcointalk.org/index.php?topic=294383.0);
- Particle (https://bitcointalk.org/index.php?topic=392804.0);
- PinkCoin (https://bitcointalk.org/index.php?topic=591666.0);
- PNut (https://bitcointalk.org/index.php?topic=435232.0);
- Primecoin (http://primecoin.io/);
- BitShares [anteriormente ProtoShares] (https://bitshares.org/);
- QubitCoin (http://www.qubitcoin.com/);
- Quarkcoin (http://www.quarkcoins.com/);
- Rhinohorns (https://bitcointalk.org/index.php?topic=515285.0);
- Roulettecoin (https://bitcointalk.org/index.php?topic=592251.0);
- Siamese Coin (https://bitcointalk.org/index.php?topic=651594.0);
- Soma (https://bitcointalk.org/index.php?topic=444273.0);
- SecureCoin (http://securecoin.org/);
- Twecoin (https://bitcointalk.org/index.php?topic=553593.0);
- TJCoin (https://bitcointalk.org/index.php?topic=610807.0);
- Tlascoin (https://bitcointalk.org/index.php?topic=576107.0);

- TwilightCoin (https://bitcointalk.org/index.php?topic=576107.0);
- Unioncoin (https://bitcointalk.org/index.php?topic=365399.0);
- Vertcoin (https://vertcoin.org/);
- VirtualCoin (https://bitcointalk.org/index.php?topic=557946).

O poder de processamento de um chip criado para minerar, chega a ser 300 x (trezentas vezes) maior que os das GPUs. Uma ASIC criada para gerar bitcoins, somente gerará bitcoins, diferente da FPGA que poderá ser reconfigurada. FPGA - *Field-Programmable Gate Array* (campo programável de ordem de entrada ou chips reprogramáveis de imediato) é um circuito integrado projetado para ser configurado e reconfigurado pelo usuário ou pelo projetista após a fabricação.

Uma dica. Sempre se deve, primeiramente, conferir se a moeda virtual não foi extinta (encerradas as atividades), se não encerrou a geração de novas unidades, se possui cotação ou negociação no comércio, qual é o valor e/ou aceitação dessa moeda, se não acabou sendo provado ser golpe, se alguém se aproveitou do nome ou endereço para outra atividade, se existe *exchange* que negocia essa moeda, etc. Ressalta-se, assim, que o ícone da moeda e sua sigla servem para distinguir a moeda em questão de outra com nome semelhante ou, até mesmo, idêntico. É comum as moedas mudarem o endereço do site ou nem terem site, mas apenas a página onde divulgaram seu lançamento. Também é algo comum as moedas mudarem de nome, lançarem novas versões e/ou os integrantes se dividirem em outras moedas.

Com BurstCoin não existe alto gasto de energia elétrica e nem com aquisição e manutenção de hardwares. A distribuição e a competitividade são mais justas; vez que qualquer pessoa pode minerar Burst, desde que tenha espaço livre no HD (disco rígido). Por outras palavras, **o espaço do HD é o fator que define o poder de mineração**; assim quanto mais espaço em HD, maior a capacidade de mineração.

- https://bitcointalk.org/index.php?topic=731923.0;
- https://bitcointalk.org/index.php?topic=1541310;

- http://bitwatcher.github.io/burstcoin/;
- http://burstcoin.biz/stats/;
- http://web.burst-team.us/;
- https://www.burst-team.us/;
- https://forums.burst-team.us/;
- http://burstcoin.biz/calculator;
- http://pool.burstcoin.eu/;
- http://www.burstcoin.online/;
- https://www.facebook.com/groups/373420826334452/.

A mineração solo, portanto, é quando se minera sozinho e por conta própria, o que proporciona o prêmio total pelo eventual bloco gerado; já a mineração em piscina (*pool*) é um lugar (site, URL, hiperlink, etc.) onde mineradores compartilham seus recursos com outros facilitando assim a mineração, mas quando um bloco é gerado pela piscina, o prêmio é dividido proporcionalmente aos participantes, conforme a contribuição dada, o que é calculada pelo programa de gerenciamento da piscina. Normalmente, a mineração solo só compensa quando a moeda é nova, o sistema possibilite real chance para computadores simples, o custo do equipamento e da energia elétrica sejam baratos e/ou não existem piscinas disponíveis ainda.

Em razão dessa dificuldade de minerar sozinho, os mineradores passaram a unir esforços. Uma *pool* (piscina) é um servidor onde os mineradores se conectam e recebem uma parte do trabalho conjunto de descriptografar o código do mesmo bloco; ao final, cada um envia seu trabalho à *pool* e caso aquele bloco tenha sido minerado com sucesso por algum deles, todos os envolvidos recebem uma recompensa equivalente ao seu trabalho. Diferente da mineração solo, minerar através de uma piscina não necessita ter a carteira instalada no computador, mas continua exigindo possuir uma carteira. Entretanto, mesmo sendo através de uma piscina, exige-se a instalação de um *software* para realizar o trabalho de mineração.

- https://slushpool.com/home/.

A mineração agrupada (*pooled mining*) é uma mineração conjunta onde vários mineiros contribuem para a geração de um bloco e depois dividem a recompensa de acordo com o poder de processamento que cada um contribuiu. A BPM - *Bitcoin Mining Pooled* (mineração agrupada de Bitcoin), apelidada de “piscina de lama" (*mud pool*), baseia-se em pontuação. Quem entrou desde o início da rodada têm peso maior do que as ações mais recentes, o que impede a trapaça de ficar alternando entre piscinas dentro de uma rodada.

A mineração coletiva dá aos membros um pagamento mais frequente e constante (redução de variância), mas o pagamento pode ser diminuído por qualquer taxa que a piscina (*pool*) pode cobrar. Já a mineração solo, paga muito bem (pois o prêmio é só de um minerador), mas tais pagamentos não são frequentes em oposição à mineração coletiva que dá pequenos pagamentos frequentes.

Por fim existe as opções onde não se usa equipamento próprio, mas aluga-se poder computacional de terceiro ou *rigs* (equipamentos ou mineradores). Desse modo, não há despesa com energia elétrica. Algumas empresas em vez de simplesmente alugar, vendem o equipamento para ser operado em suas instalações.

Outro detalhe, moedas novas ou ainda não populares, provavelmente são muito mais fáceis de minerar; inclusive com qualquer computador pessoal. Recorde-se da história da mineração do Bitcoin, como qualquer pessoa, com o computador simples que tinha em casa, conseguia minerar e receber, fácil e rapidamente, grandes quantidades da moeda. O mesmo padrão inicial tende a se repetir com as altcoins novas, desconhecidas ou, ainda, não populares.

Nos sites e/ou nas divulgações ou anúncios (ANN - *announcement*) de lançamento (*launch*) das criptomoedas, normalmente, constam, além da descrição da mesma (história, características, detalhes, diferenciais, filosofias, objetivos, regras, etc.), também possuem as informações técnicas (como é gerada, como se minera, como se compra, etc.). Detalhe, os anúncios de divulgação do lançamento da moeda costumam ser atualizados.

HODL - HOdlcoin (http://hodlcoin.com/), por exemplo, é uma altcoin relativamente nova que só pode ser extraída com a CPU; pelo menos, por enquanto.

- https://bitcointalk.org/index.php?topic=1317918.0;
- https://github.com/HOdlcoin/HOdlcoin;
- https://yobit.net/en/trade/HODL/BTC.

Bon PeKaO (http://bonpekao.org/) é uma nova moeda digital que se guarda em uma determinada carteira online (https://poswallet.com/login.php) e se ganha bonificações (https://coinexchange.io/).

Outra moeda relativamente nova é a Decred (https://www.decred.org/); confira suas orientações em https://wiki.decred.org/. Outro exemplo, não tão recente, é a Gridcoin (http://gridcoin.us/) com sua wiki (páginas interligadas): http://wiki.gridcoin.us/.

Conforme demonstrado, muitas das moedas novas são divulgadas (ANN - *announcement*), dentre outros sites, em https://bitcointalk.org/, https://cryptocointalk.com, https://allcryptotalk.com/ e https://github.com/. Por isso, é aconselhável acompanhá-los; vez que no início, além das condições serem melhores, costumam ser dadas moedas gratuitamente aos interessados.

LISTA DE ALTCOINS: CONSENSO E *HASH*

A lista infra é apenas um complemento sucinto e prático dos capítulos "MÉTODOS DE CONSENSO" e "ALGORITMO DE *HASH*".

Confira uma listagem exemplificativa de criptomoedas PoW em https://minkiz.co/coin/cmcap-pow e de criptomoedas PoS em https://minkiz.co/coin/cmcap-pos.

- 007Coin (007): PoS – scrypt;
- 020Londoncoin (O2O): PoS – quark;
- 10kcoin (10k): PoS – SHA2-256;
- 110coin (IIO): PoW – SHA2-256;
- 1337 (1337): PoS – x13;
- 13 Coin (13): PoS – scrypt-j;
- 16Bit (BIT16): PoS – nist5;
- 1Coin (ONE): PoW – 3s;
- 1Credit (1CR): PoW – scrypt;
- 1Paisacoin (PAISA): PoW – SHA2-256;
- 1Satoshi (1S): PoW – x11;
- 2112coin (YYZ): PoW – SHA2-256;
- 21 Coin (21): PoW – SHA2-256;
- 23skidoo (CHAO): PoW – SHA2-256;
- 24x7coin (TFS): PoW – scrypt;
- 256Coin (256): PoW – SHA2-256;
- 2bacco (BACCO): PoW – scrypt;
- 2CHcoin (2CH): PoW – quark;
- 2ndEUR (2NDEUR): PoW – SHA2-256;
- 32bit (32BIT): PoS – x11;
- 365Coin (365): PoW – SHA3-256;
- 419coin (SCAM): PoW – scrypt;
- 42Coin (42C): PoW – scrypt;
- 4chancoin (4CH): PoW – scrypt;
- 500Coin (FHC): PoW – scrypt;
- 502Coin (502): PoW – scrypt;
- 611coin (SIL): PoW – SHA2-256;
- 666Coin (666): PoW – scrypt;
- 66Coin (66): PoW – scrypt;
- 6Coin (6CN): PoW – scrypt;
- 7coin (7): PoW – scrypt;
- 81coin (BIG): PoW – SHA2-256;
- 84 Coin (84): PoW – scrypt;
- 8bit (8BIT): PoS – scrypt;
- 8coin (8): PoW – scrypt;
- #coin (#C): PoS – scrypt-j;
- A3 coin (A3C): PoS – scrypt;

- ABcoin (ABC): PoS – scrypt
- Abundancecoin (ABC): PoS – x11;
- Accelerate (ACLR): PoS – x11;
- Acecoin (ACE): PoS – x11;
- Achillescoin (ACH): PoW – x11;
- Acoin (ACOIN): PoW – SHA2-256;
- AcroCoin (ACRO): PoS – novel;
- Activecoin (ACT): PoW – scrypt;
- Activecoin (ACTIVE): PoW – scrypt;
- Adamantium (ADM): PoS – x11;
- Adamantiumcoin (ADMT): PoS – x11;
- Adcoin (XAD): PoW – scrypt;
- AdderalCoin (ADD): PoS – x13;
- Aditicoin (XAD): PoW – scrypt-j-n;
- AdzCoin (ADZ): PoW – x11;
- aEchoCoin (AECC): PoW – scrypt;
- Aeciocoin (AEC): PoW – scrypt;
- Aegiscoin (AGS): pow-pos – x15;
- ÆØÅcoin (AEOA): PoS – x13;
- Aeon (AEON): PoW – cryptonight;
- Aerocoin (AERO): PoS – x13;
- AeroME (AM): PoS – x13;
- Aevumcoin (AEVUM): PoW – scrypt;
- African Black Diamond (ABD): PoW – scrypt;
- AgileReserveCoin (ARC): PoS – scrypt-j;
- AHScoin (AHS): PoW – SHA2-256;
- Aidbitcoin (AID): pow-pos – Grøstl;
- Aidencoin (ADN): PoW – scrypt;
- Aimcoin (AIM): PoS – scrypt;
- Aircoin (AIR): PoW – scrypt;
- Aixincoin (AXC): PoW – scrypt;
- Alancoin (ALC): PoW – hefty1;
- Albatrosscoin (ATR): PoS – nist5;
- Albocoin (ALB): PoW – scrypt;
- AlchemistCoin (XAC): PoW – scrypt;
- Alcohoin (ALC): PoW – scrypt;
- Aleacoin (ALEA): PoS – x15;
- Alexiumcoin (AUM): PoW – scrypt;
- Alibacoin (ABC): PoW – scrypt;
- Aliencoin (ALN): PoW – scrypt;
- Alipaycoin (ALI): PoW – x14;
- Allagescoin (AAC): PoW – BLAKE;
- Alliancecoin (AAC): PoS – x13;
- AlliedCoin (ADN): PoW – scrypt;
- Allstars (ALLS): PoS – SHA2-256;
- AlpaCoin (APC): PoW – SHA2-256;
- Alphacoin (ALF): PoW – scrypt;
- Alphaomegacoin (AOC): PoW – scrypt;
- Altcoin (ATC): PoW – SHA2-256;
- Altcoin (ALT): PoW – scrypt-n;

- AltcoinReserve (ALT): PoS – x11;
- AltexIndustries (ALT): PoS – x13;
- AluminiumCoin (ALU): PoW – scrypt;
- AMAXCoin (AMAX): PoW – scrypt;
- Amazoniacoin (AMZ): PoW – scrypt;
- Ambercoin (AMBER): PoW – x13;
- Ambercoin (AMBER): pow-pos – x11;
- AmericanCoin (AMC): PoW – scrypt;
- Amerocoin (AMX): PoW – scrypt;
- AmeroX (AX): PoS – x11;
- Amigacoin (AGA): PoW – scrypt;
- AmKoin (AMK): PoW – SHA2-256;
- Amsterdamcoin (AMS): PoS – quark;
- AmsterdamCoin (AMS): PoW – scrypt;
- AnaLCoin (ANAL): PoS – SHA2-256;
- AnarchistPrime (ACP): PoW – SHA2-256;
- Android token (ADT): PoS – scrypt;
- AndromedaCoin (AND): PoS – x11;
- Angelcoin (ANG): PoS – x15;
- Angora (ANG): PoW – x11;
- AngryBirdCoin (ABC): PoW – x11;
- Angrybirdscoin (ABC): PoW – x11;
- Anherocoin (AHC): PoW – scrypt;
- Animecoin (ANI): PoW – quark;
- Anoncoin (ANC): PoW – scrypt;
- AnonDollar (DOLLAR): PoS – SHA2-256;
- Anonymouscoin (XAC): PoW – x11;
- Antarctic (ACC): PoW – x11;
- Antibeebacoin (ABC): PoW – SHA2-256;
- AntiBitcoin (ANTI): PoW – SHA2-256;
- Anti-Keisercoin (AKC): PoW – scrypt;
- AntiLitecoin (ALTC): PoW – scrypt;
- Antimatter (ANT): PoW – scrypt;
- Anti-TerroristicCoin (PEN): PoS – scrypt;
- AntwerpenCoin (JEWEL): PoS – x13;
- Apccoin (APC): PoW – scrypt;
- Apecoin (APE): PoW – scrypt;
- APEXcoin (APEX): PoS – x13;
- AphroditeCoin (APH): PoW – scrypt;
- APIcoin (XAP): PoS – SHA2-256;
- Apollocoin (APOLLO): PoW – scrypt;
- Appcoin (APP): PoW – scrypt;
- AppCreditCoin (ACC): PoS – scrypt;
- Applebyte (ABY): PoW – scrypt;
- Applecoin (MAC): PoW – SHA2-256;
- AppleCoin (APC): PoS – scrypt-j;
- April (XAP): PoS – SHA2-256;
- Aptcoin (APT): PoW – scrypt-n-m;
- AquariusCoin (ACR): PoS – scrypt;
- ARbit (ARB): PoS – SHA2-256;

- Archcoin (ARCH): PoS – scrypt;
- Architectcoin (ARCH): PoS – scrypt;
- Arcoin (AR): PoS – x13;
- Arcticcoin (ARC): PoS – scrypt;
- ArenaCoin (ARN): PoS – novel;
- Argcoin (ARGC): PoW – scrypt;
- Argentum (ARG): PoW – scrypt;
- Argon2 (AR2): PoW – salsarg;
- Aricoin (ARI): PoW – scrypt;
- Arkenstone (ARS): PoW – SHA2-256;
- Arkhash (ARK): PoW – SHA2-256;
- ArpaCoin (ARP): PoS – SHA2-256;
- Artifact (ART): PoW – SHA2-256;
- Aryacoin (ARYA): PoW – x11;
- ASAPcoin (ASAP): PoW – cryptonight;
- Ascensioncoin (ASN): PoS – qubit;
- Ascentcoin (ASCE): PoS – x11;
- ASDcoin (ASD): PoW – SHA2-256;
- Asiacoin (ASC): PoW – scrypt;
- AsiaCoin (AC): PoS – scrypt;
- Asiadigicoin (ADCN): PoW – scrypt;
- Asian Investmentment Bond (AIB): PoW – scrypt;
- ASICcoin (ASC): PoW – SHA2-256;
- Asspenny (ASS): PoW – scrypt;
- Astral (ASTRAL): PoS – x13;
- Astrocoin (ASR): PoW – scrypt;
- Atencoin (ATEN): PoW – quark;
- Atheistcoin (ATH): PoW – Grøstl;
- Atomcoin (ATO): PoW – quark;
- Audiocoin (ADC): PoS – scrypt;
- Augmentum (XAF): PoW – SHA2-256;
- Augur (REP): PoW – Dagger;
- AureusCoin (ARE): PoS – x11;
- Auroracoin (AUR): PoW – scrypt;
- AurumCoin (AU): PoW – SHA2-256;
- Aurumwaycoin (AURC): PoW – scrypt;
- AustraliaCoin (AUS): PoW – scrypt;
- AustroCoin (ATC): PoS – scrypt;
- AutismCoin (AUT): PoW – scrypt;
- Autocoin (AUT): PoW – scrypt;
- Autumncoin (ATM): PoS – x11;
- Avatar (AV): PoS – SHA2-256;
- Avcoin (AV): PoS – x11;
- Axiocoin (AXIO): pow-pos – scrypt;
- Axiom (AXH): PoS – Shabal;
- Axiscoin (AXIS): PoS – x13;
- Axroncoin (AXR): PoS – fresh;
- Azzacoin (AZC): PoS – x11;
- B1bl3Coin (B1BL3): PoS – scrypt;
- B2BCoin (B2B): PoS – x13;

- BabesandNerds (BAN): PoS – x11;
- Backpackercoin (BACK): PoS – x15;
- Baconbits (YUM): PoW – scrypt;
- Badcoin (BAD): PoW – SHA2-256;
- Badgercoin (BDG): PoW – x11;
- Bagelcoin (BGC): PoW – SHA2-256;
- Baihuicoin (BHC): PoW – SHA2-256;
- Bamboo (BAM): PoW – x11;
- Bamit (BAM): PoS – x11;
- BananaBits (NANAS): PoS – x11;
- Bananacoin (BANC): PoW – x11;
- Bancorcoin (BNCR): PoW – SHA2-256;
- Ban Hammer coin (BAN): PoS – x11;
- Bankcoin (BANK): PoW – x11;
- Banknote (BN): PoS – scrypt;
- Banksycoin (BSY): pow-pos – scrypt;
- Bantam (BNT): PoW – x11;
- Banxcoin (BANX): PoS – SHA2-256;
- Baobeicoin (BBC): PoW – scrypt;
- BarberBuck (CUT): PoS – x11;
- Barcoin (BAR): PoW – scrypt;
- BaseballCardcoin (BBCC): PoS – scrypt;
- Basecoin (BAC): PoS – scrypt;
- Bata (BTA): PoW – scrypt;
- BatCoin (BAT): PoW – scrypt;
- BattleCoin (BCX): PoS – SHA2-256;
- Battlestake (BSTK): PoS – x11;
- Bawbee (BAW): PoW – scrypt;
- BBQCoin (BQC): PoW – scrypt;
- Bcoin (BCOIN): PoW – SHA2-256;
- Bcttalkcoin (BCT): PoW – SHA3-256;
- BDSMcoin (BDSM): PoW – SHA2-256;
- BDSM-FETISH (WHIPPED): PoS – scrypt;
- BeaoCoin (BEC): PoW – scrypt;
- BeardDollars (BRDD): PoS – scrypt;
- BeastCoin (666): PoW – scrypt;
- Beatlecoin (BEA): PoW – scrypt;
- Beavercoin (BVC): PoW – scrypt;
- Beecoin (BEE): PoW – scrypt;
- Beecoinv2 (BEE2): PoS – x11;
- Beercoin (BEER): PoW – scrypt;
- BeezerCoin (BEEZ): PoS – scrypt;
- Belicoin (BELI): PoW – scrypt;
- Bellacoin (BELA): PoW – scrypt;
- Bells (BEL): PoW – scrypt;
- Benjamins (BEN): PoW – SHA2-256;
- Bernankoin (BEK): PoW – primechain;
- Berncash (BERN): pow-pos – x14;
- Bestcoin (BEST): PoW – scrypt;
- Bestericoin (BIC): PoW – x11;

- BetaCoin (BET): PoW – SHA2-256;
- BeyondAccess (BEY): PoS – myriad;
- Biebercoin (BRC): PoW – scrypt;
- BigBangcoin (BBC): PoS – x15;
- BigBullioncoin (BIG): PoW – SHA2-256;
- Bigcoin (HUGE): PoW – BLAKE;
- BigPicoin (BPI): PoW – scrypt;
- Billaume (BLL): PoW – scrypt;
- BillionCoin (BIL): PoW – scrypt;
- Bilshares (BILS): PoS – nxt;
- Binarycoin (BIN): PoW – scrypt;
- Binarycoin (BIC): PoW – scrypt;
- Biocoin (BIO): PoS – x13;
- BiosCrypto (BIOS): PoS – quark;
- Birdcoin (BRD): PoW – scrypt;
- Bitalpha (BA): PoS – scrypt;
- BitAltcoin (BAI): PoW – cryptonight;
- BitAltcoin2 (XBA): PoW – scrypt;
- BitBar (BTB): PoS – scrypt;
- Bitbay (BAY): PoS – scrypt;
- Bitbean (BITB): PoS – SHA2-256;
- BitBlockcoin (BBL): PoS – x15;
- BitBronze (BRONZ): PoW – scrypt;
- Bitburst (BTB): PoW – scrypt;
- Bitcash (BCSH): PoW – x14;
- BitCent (BCENT): PoS – x11;
- Bitcentavo (NBE): PoW – SHA2-256;
- Bitchcoin (BTCH): PoW – x11;
- BitChips (CHP): PoW – scrypt;
- Bitcoin (BTC): PoW – SHA2-256;
- Bitcoin12.5 (BTC12): PoS – quark;
- Bitcoin21 (XBTC21): PoS – SHA2-256;
- BitcoinClassic (BTC): PoW – SHA2-256;
- Bitcoindark (BTCD): PoS – SHA2-256;
- BitCoinFast (BCF): PoS – scrypt;
- BitcoinHashCore (BTCHC): PoW – scrypt;
- BitcoinLite (BTCL): PoS – x11;
- BitcoinNEW (BTN): PoW – SHA2-256;
- Bitcoinplus (XBC): PoS – SHA2-256;
- BitcoinScrypt (BTCS): PoW – scrypt;
- BitcoinT (BT): PoS – x11;
- Bitcointalknshop (BTCS): PoS – SHA2-256;
- BitcoinTX (BTCTX): PoW – x11;
- BitcoinUltra (BTCU): PoS – SHA2-256;
- Bitcoinx11 (BTCX): PoS – x11;
- Bitcredits (CREDITS): PoW – scrypt;
- Bitcredits (BCR): PoW – momentum;
- BitCrystal (BTCRY): PoW – quark;
- BitCurrency (BTCR): PoS – x11;
- Bitdolar (BTD): PoW – SHA2-256;

- BitDolar (BD): PoS – SHA2-256;
- Bitgem (BTG): PoS – scrypt;
- Bitgold (GOLD): PoS – scrypt;
- BitHIRE (HIRE): PoS – SHA2-256;
- Bitinum (BTN): PoW – SHA2-256;
- Bitleu (BTL): PoW – scrypt-j;
- BitLion (XBL): pow-pos – x13;
- BitLitS (BTLS): PoW – scrypt;
- Bitloon (BLN): PoS – SHA2-256;
- Bitlux (LUx): PoS – x11;
- Bitmark (BTM): PoW – scrypt;
- Bitmiles (BTMI): PoW – scrypt;
- BitMocoin (XBM): PoS – x13;
- BitMonero (BMR): PoW – cryptonight;
- Bitmoneycoin (BMY): PoW – scrypt;
- Bitnote (BNT): PoW – scrypt;
- BITOK (BOK): PoS – x11;
- Biton (BITON): PoW – scrypt;
- Bitorecoin (BTO): PoW – x11;
- BitPagar (BPC): PoW – scrypt;
- BitPeso (BTP): PoW – SHA2-256;
- Bitpopcoin (BPC): PoS – x11;
- Bitpound (BTP): PoS – SHA2-256;
- BitQuark (BTQ): PoW – quark;
- Bitraam (BRM): PoW – SHA2-256;
- BitReplica (BITR): PoW – x13;
- BitRush (BSH): PoS – x11;
- BitSeeds (BIT): pow-pos – SHA2-256;
- Bitsend (BSD): PoW – x11;
- BitSharesPTS (PTS): PoS – momentum;
- BitsharesX (BTSX): dpos – interest;
- Bitsis (BSS): PoW – SHA2-256;
- Bitslap (BS): PoW – x11;
- Bitstake (XBS): PoS – x11;
- Bitstar (BITS): PoS – scrypt;
- Bitstone (BST): PoS – x11;
- BitSwift (SWIFT): PoS – x15;
- BitToCcoin (BT): PoW – x13;
- Bitvegan (VEG): PoS – x11;
- BitXcoin (BIT-X): pow-pos – x11;
- Bitz (BITZ): PoS – x11;
- Bitzcoin (BTZ): PoS – x11;
- BitZeny (ZNY): PoW – yescrypt;
- Bizcoin (BIZ): PoS – x11;
- Blackblackblackcoin (BBB): PoW – SHA2-256;
- BlackBlackcoin (BBC): PoW – SHA3-256;
- Blackcatcoin (BCAT): PoS – x11;
- BlackCoin (BC): PoS – scrypt;
- Blackdiamondcoin (BDC): PoW – scrypt;
- BlackDogCoin (BDC): PoS – x11;

- BlackDogecoin (XBD): PoS – x11;
- Blackdragoncoin (BDC): PoW – scrypt-j;
- BlackfridayCoin (BFC): PoS – scrypt;
- BlackMarket (BLM): PoS – x15;
- BlackTokencoin (BLKT): PoS – x13;
- Bladecoin (BLA): PoS – scrypt;
- BlakeBitCoin (BBTC): PoW – BLAKE;
- BlakeCoin (BLC): PoW – BLAKE;
- BlazeCoin (BLZ): PoW – scrypt;
- Blend (XBLD): PoS – SHA2-256;
- Blesscoin (BLS): PoW – scrypt;
- BlitzCoin (BLTZ): PoW – scrypt;
- Blockcredits (BKC): PoS – SHA2-256;
- Blocknet (BLOCK): PoS – x15;
- Blockshares (BKS): PoS – SHA2-256;
- Bloodcoin (BOD): PoW – quark;
- Blucoin (BLU): PoW – scrypt;
- Bluechip (BCH): PoS – x13;
- BlueCoin (BLU): PoS – scrypt;
- Blueplanetcoin (BLP): PoW – scrypt;
- BlueSteelCoin (BLUS): PoS – x11;
- Bluntcoin (BLUNT): PoW – x13;
- BMWcoin (BMC): PoW – quark;
- BnrtxCoin (BNX): PoS – x11;
- Boardcoin (BOARD): PoS – x11;
- BoatsnBitches (BNB): PoS – x11;
- Bolivarcoin (BOL): PoW – scrypt;
- Bollywoodcoin (BDC): PoW – x11;
- BomChickaWahWah (BCW): PoS – x11;
- Bones (BONES): PoW – scrypt;
- Bongger (BGR): PoW – scrypt;
- BonusCoin (BNS): PoW – SHA2-256;
- Boodle (BOOD): PoS – scrypt;
- Boolberry (BBR): PoW – SHA3-256;
- Boomcoin (BMC): PoW – scrypt;
- BoomCoin (BOOM): PoS – x13;
- Boost (BOST): PoS – x13;
- BootstrapCoin (BSP): PoS – x11;
- Borgcoin (BRG): PoW – scrypt;
- Boringcoin (ZZZ): PoW – SHA2-256;
- BoschiCoin (BCC): PoW – scrypt;
- Bosscoin (BSS): PoW – scrypt;
- Bosscoin (BOS): PoW – scrypt;
- Botcoin (BOT): PoS – scrypt;
- Bottlecaps (CAP): PoS – scrypt;
- Bountycoin (BOUN): PoS – x13;
- BountyCoin (BOC): PoS – SHA2-256;
- Bowcoin (BSC): PoW – x11;
- Boxcoin (BOX): PoS – scrypt;
- BoyCoin (BOY): PoW – scrypt;

- BRCoin (BRC): PoW – scrypt;
- Breakcoin (BRE): PoS – x11;
- Breakoutcoin (BRO): pow-pos – cryptonight;
- Brigadecoin (BRIG): PoS – x11;
- Brightcoin (BRI): PoW – scrypt;
- BrightCoin (BRC): PoW – scrypt;
- Britcoin (BRIT): PoS – x13;
- BroCoin (BRO): PoW – scrypt;
- BrotherCoin (BRC): PoW – x11;
- BTCtalkcoin (TALK): PoS – scrypt;
- BTIcoin (BTI): PoS – SHA2-256;
- Bubble (BUB): PoW – scrypt;
- BubbleTeaCoin (BUBL): PoS – x11;
- Buddhacoin (BDC): PoW – cryptonight;
- Buffalocoin (BFL): PoW – scrypt;
- BulbaCoin (BULBA): PoW – x11;
- Bulbcoin (BULB): PoW – x15;
- Bull City coin (BULB): PoW – SHA2-256;
- Bullcoin (TBC): PoW – quark;
- Bumbacoin (CLOT): PoW – scrypt;
- BunnyCoin (BUN): PoW – scrypt;
- Burbucoin (BUR): PoW – scrypt;
- Burnercoin (BURN): PoS – x13;
- Burnercoin2 (BURN): PoS – x13;
- Burstcoin (BURST): PoS – nxt;
- Businesscoin (BIZ): PoW – scrypt;
- Butterflycoin (BFC): PoS – scrypt;
- Butterflycoin (BFC): PoS – SHA2-256;
- Buycoin (BUY): PoW – scrypt;
- BuyLatercoin (BLTR): PoS – x13;
- BuyNowcoin (BNC): PoS – x13;
- BUZZ (BUZZ): PoW – scrypt;
- Buzzcoin (BUZZ): PoS – SHA2-256;
- Buzzcoin (BUZ): PoW – SHA2-256;
- Bwincoin (BWC): PoS – scrypt;
- Bytecent (BYC): PoW – prime6;
- Bytecoin (BTE): PoW – SHA2-256;
- Bytecoin (BCN): PoW – cryptonight;
- C0fferCoin (C0C0): PoS – scrypt;
- Cable Coin (CAB): PoW – scrypt;
- CACHEcoin (CACH): PoS – scrypt-j;
- Cagecoin (CAGE): PoW – scrypt;
- CaiShen Coin (CAI): PoW – scrypt-n;
- CAIx (CAIX): PoS – scrypt;
- Cake coin (CAKE): PoW – scrypt;
- CaliforniaCoin (CAC): PoW – scrypt;
- Californium (CF): PoW – SHA2-256;
- Camcoin (CAM): PoS – x11;
- CamorraCoin (CAM): PoS – scrypt;
- Canadacoin (CDA): PoS – scrypt;

- CanadaEcoin (CDN): PoW – scrypt;
- Cancercoin (CCC): PoW – scrypt;
- Candlecoin (CD): PoW – SHA2-256;
- Candycoin (YUM): PoW – scrypt;
- CannabisCoin (CANN): PoW – x11;
- CannabisDarkcoin (CND): PoS – x11;
- Cannacoin (CCN): PoW – scrypt;
- Cantorcoin (EIC): PoW – SHA2-256;
- CapitalCoin (CPTL): PoS – scrypt;
- Capitalistcoin (CPL): PoS – x11;
- Caponecoin (CPNC): PoS – x11;
- Caponecoin (CPN): PoS – x11;
- Capricoin (CPC): PoS – x11;
- CAPTcoin (CAPT): PoS – captcha;
- Carboncoin (CARB): PoW – scrypt;
- CarbonCredit (UNIT): PoS – scrypt;
- CarbonEmissionTradecoin (CT): PoW – scrypt-n;
- Carpediemcoin (DIEM): PoW – SHA2-256;
- ÇarsiCoin (CARSI): PoW – scrypt;
- Cash coin (CASH): PoS – scrypt;
- CashMe (CME): PoS – x13;
- CashTakers (CTK): PoS – SHA2-256;
- CasinoCoin (CSC): PoW – scrypt;
- Cassubian Detk (CDT): PoW – qubit;
- Cataloniacoin (CATC): PoW – scrypt-n;
- CatCoin (CAT): PoW – scrypt;
- CateDoge (CTD): PoW – SHA3-256;
- CATicoin (CATI): PoW – x11;
- C-bit (XCT): PoW – SHA2-256;
- CCoin (CC): PoW – scrypt;
- C-Coin (CCN): PoW – scrypt;
- CDNcoin (CDN): PoW – primechain;
- Centrifugal (XCF): PoW – x13;
- Cerium (XCE): PoS – SHA2-256;
- Cetuscoin (CETI): PoS – scrypt;
- Chaincoin (CHC): PoW – c11;
- ChainCoin (CHAIN): PoS – x11;
- Chakracoin (CKC): PoS – scrypt;
- Championcoin (CHAM): PoW – scrypt;
- Chancecoin (CHA): pob – SHA2-256;
- CharityCoin (CHA): PoW – scrypt;
- CHARONscoin (CHCO): PoW – myriad;
- Chatcoin (CHAT): PoW – nist5;
- Chavezcoin (CHVZ): PoS – x11;
- CHCcoin (CHCC): PoW – scrypt-j;
- Checkcoin (CKC): PoW – x11;
- Checkoutcoin (CXC): PoS – x13;
- Cheetahcoin (FAST): PoW – scrypt;
- Cherrycoin (CHE): PoW – scrypt-n;
- CherryNote (CRR): PoW – cryptonight;

- ChiChi Coin (UUC): PoW – scrypt;
- Chicoin (CHI): PoW – scrypt;
- Chikun (KUN): PoW – SHA2-256;
- Chilcoin (CLC): PoW – scrypt;
- Chingeling (CHL): PoS – x13;
- Chipcoin (CHIP): PoW – x11;
- CHNcoin (CNC): PoW – scrypt;
- Choclatecoin (CHOC): PoW – scrypt;
- Chococoin (CCC): PoW – SHA2-256;
- ChronoSphere (SPHR): PoW – scrypt;
- CineCoin (CINE): PoW – scrypt;
- CinemaCoin (CIC): PoW – scrypt;
- Cinnamoncoin (CIN): PoS – scrypt;
- Cinnicoin (CINNI): PoS – scrypt;
- Cionz (CIONZ): PoS – SHA2-256;
- Citicoin (CITI): PoW – scrypt;
- Citizen coin (CTZ): PoS – x11;
- Citycoin (CITY): PoS – x15;
- Civilisationcoin (CIV): PoS – scrypt;
- Clamcoin (CLAM): PoS – scrypt;
- CLAMScoin (GCS): PoS – x11;
- Cleancoin (CLN): PoS – x15;
- Clean Water Coin (WATER): PoS – scrypt;
- ClearingHouse (XCH): PoS – SHA2-256;
- Cleverbot (CLT): PoS – SHA2-256;
- Clevercoin (CLV): PoS – x11;
- CleverHash (CHASH): PoS – x13;
- Clickcoin (CLICK): PoS – x11;
- Cloak (CLOAK): PoS – x13;
- Clockcoin (CKC): PoW – scrypt;
- Cloudcoin (CDC): PoS – scrypt;
- Cloudtokens (CLOUD): PoS – x11;
- Clovercoin (CLC): PoS – scrypt;
- ClubCoin (CLUB): PoS – scrypt;
- Clustercoin (CLSTR): PoW – SHA2-256;
- C-Note (CNOTE): PoW – quark;
- Coca-ColaCoin (ICOKE): PoS – SHA2-256;
- CocaineCoin (COC): PoW – scrypt;
- CoCoCoin (COCO): PoW – x13;
- CoCoCurrency (COCO): PoS – x13;
- Coexistcoin (COEXST): PoW – x11;
- Coffeecoin (COF): PoS – x15;
- Coffeecoin (CFC): PoS – scrypt;
- CoffeeCoin (CFC2): PoS – scrypt;
- CoiledCoin (CLC): PoW – SHA2-256;
- Coin (COIN): PoW – scrypt;
- Coin2 (C2): PoW – scrypt;
- Coinaaa Coin (AAA): PoW – SHA2-256;
- Coinaid (CAID): PoS – x13;
- Coinapilla (CPL): PoW – x11;

- CoinAwesome (AWE): PoS – scrypt;
- Coinbuilder (BUILD): PoS – scrypt;
- Coincoin (COI): PoW – scrypt;
- Coinlabcoin (LAB): PoW – quark;
- Coinmarketscoin (JBS): PoS – scrypt;
- Co-innovationCoin (CIC): PoS – x13;
- Coino (COINO): PoS – scrypt;
- Coinomat (CNMT): PoS – nxt;
- CoinoUSD (XUSD): PoS – nxt;
- Coinsy (CSY): PoS – scrypt;
- Coin Wayne (CWY): PoW – scrypt;
- CoinyeCoin (KOI): PoW – scrypt;
- ColaCoin (COLA): PoW – scrypt;
- Colbertcoin (CC): PoW – SHA2-256;
- Coldcoin (COLD): PoS – scrypt;
- Coloradocoin (COLC): PoW – scrypt;
- Colorcoin (CC): PoS – x11;
- Colossuscoin (COL): PoS – scrypt;
- Colossuscoin2 (CV2): PoS – x13;
- ComCoin (CC): PoS – SHA2-256;
- ComedyGold (LEL): PoW – scrypt;
- Communitycoin (CTC): PoW – scrypt;
- Community coin (COMM): PoS – scrypt;
- Compasscoin (CPC): PoW – SHA2-256;
- CompuCoin (CPN): PoW – scrypt;
- Computercoin (CMPT): PoW – x13;
- Comrade (COM): PoW – scrypt;
- Concealcoin (CNL): PoS – x11;
- Confessioncoin (CFN): PoW – scrypt;
- Conspiracycoin (CYC): PoW – x11;
- Containercoin (TEU): PoW – scrypt;
- Continentcoin (CONT): PoW – scrypt;
- Continuumcoin (CTM): PoW – SHA2-256;
- Cookies (CKE): PoW – SHA2-256;
- Coolcoin (COOL): PoS – scrypt;
- Coolingcoin (CLC): PoS – nist5;
- CooperationAndSolidarityCoin (CAS): PoW – x13;
- Cooperationcoin (COOP): PoW – scrypt;
- CopperBars (CPR): PoS – scrypt-j;
- CopperCoin (CU): PoW – scrypt;
- Copperlark (CLR): PoW – SHA3-256;
- Corecoin (CORE): PoS – x15;
- Corecoin (COR): PoW – scrypt;
- Corgicoin (CORG): PoS – scrypt;
- CorgiCoin (CORG): PoW – scrypt;
- CorgiCoin (CORGI): PoW – scrypt;
- CornerstoneCoin (CCX): pow-pos – scrypt;
- Cosmoscoin (CMC): PoS – scrypt;
- Counterparty (XCP): PoW – SHA2-256;
- Counterscoin (CSC): PoW – scrypt;

- Coven (COV): PoS – SHA2-256;
- CowCoin (COW): PoW – scrypt;
- CPU2Coin (CP2): PoW – quark;
- Cpucoin (CPC): PoW – Whirlpool;
- Crackcoin (CRK): PoS – x11;
- CraftCoin (CRC): PoW – scrypt;
- Craigscoin (CRAIG): PoS – x11;
- Crankcoin (CRNK): PoS – x11;
- Crapcoin (CRAP): PoW – scrypt;
- Crave (CRAVE): PoW – scrypt;
- Crazycoin (CYC): PoW – scrypt;
- Createcoin (CREAT): PoS – x13;
- CreativeFund (BCF): PoS – SHA2-256;
- Credit (CRDE): PoW – scrypt;
- Creditbit (CREDIT): PoW – x11;
- Creditcoin (CRDC): PoW – SHA2-256;
- CreditCoin (CTC): PoS – *unknown* (desconhecido);
- Credits (CRD): PoW – scrypt;
- Credits (CR): PoW – scrypt;
- CREDS (XXC): PoW – SHA2-256;
- CrevaCoin (CREVA): PoW – scrypt;
- Criccoin (CRIC): PoS – x11;
- CrimeaCoin (CMA): PoW – scrypt;
- CrimeCoin (CRIME): PoW – scrypt;
- Crowncoin (CC): PoW – Fugue;
- Crowncoin (CROWN): PoW – scrypt;
- CrownCoin (CRW): PoW – SHA2-256;
- CRYcoin (CRY): PoS – scrypt;
- Cryptbit (CBIT): PoW – scrypt;
- CryptCash (CYPT): PoW – quark;
- Cryptcoin (CRYPT): PoW – x11;
- CryptekSilvercoin (CTS): PoW – desconhecido;
- Cryptex (CYX): PoS – x11;
- Crypti (XCR): PoS – ellipticcurve;
- Crypto (CTO): PoW – lyra2re;
- Cryptoapples (CRA): PoW – scrypt;
- CryptoBancor (CBR): PoW – x11;
- Cryptobits (CYB): PoW – scrypt;
- Cryptobuck (BUK): PoS – scrypt;
- CryptoBullion (CBX): PoS – scrypt;
- Cryptobyte (CB): PoS – x11;
- CryptoCircuits (CIRC): PoS – x11;
- CryptoClub (CCB): PoS – x11;
- Cryptocoin (CTC): PoW – scrypt;
- Cryptocoin Inc Shares (CCI): PoS – scrypt;
- Cryptodollar (CD): PoW – scrypt;
- Cryptoeagle (CREA): PoW – SHA2-256;
- CryptoEscudo (CESC): PoW – scrypt;
- CryptoFocus (FCN): PoS – x11;
- Cryptogenic Bullion (CGB): PoS – scrypt;

- Cryptographic Anomaly (CGA): PoW – scrypt;
- CryptographicCoin (CRT): PoW – scrypt;
- Cryptographic eCash (XCTE): PoS – MD5;
- Cryptographic Triangles (TRI): PoS – x13;
- Cryptoken (CRYP): PoW – scrypt;
- Cryptoken (CYT): PoS – scrypt;
- CryptoLOOT (LOOT): PoW – SHA2-256;
- CryptoMETH (METH): PoW – SHA3-256;
- Cryptonite (XCN): PoW – m7;
- Cryptonium coin (CRN): PoW – scrypt;
- CryptoNotecoin (CNN): PoW – cryptonight;
- CryptoNoteCoin (CNC): PoW – cryptonight;
- CryptoPennies (CP): PoS – x11;
- CryptoPowers (CPS): PoW – x11;
- CryptoShekel (SHKL): PoW – scrypt;
- CryptoSpots (CS): PoS – x11;
- Cryptostuds (CSD): PoW – scrypt;
- Cryptotarget (CRT): PoW – SHA2-256;
- CryptoWon (CWON): PoS – x13;
- CryptoXTC (XTC): PoW – x11;
- CrystalCoin (CRYSTAL): PoS – x15;
- CScoin (CSO): PoS – x11;
- Cthulhu (OFF): PoW – scrypt;
- Cubit (QBT): PoW – SHA2-256;
- Cummingtonite (CUM): PoS – scrypt;
- Curecoin (CURE): PoW – scrypt;
- CurrencyLinkedCurrency (CUC): PoS – SHA2-256;
- CurrencyofLight (CURA): PoW – SHA2-256;
- Curvatures (CURVES): PoS – x11;
- Cybercoin (CYC): PoW – scrypt;
- CyberCoin (CC): PoS – scrypt;
- Cyclecoin (CCC): PoS – scrypt;
- Cyclingcoin (CYC): PoS – x11;
- Cygnus (CYG): PoS – x11;
- Cypher (CYP): PoS – qubit;
- Cypherfunks (FUNK): PoW – scrypt;
- Czarcoin (CZR): PoS – scrypt;
- Czechcoin (CZC): PoW – myriad;
- CzechCrownCoin (CZC): PoW – scrypt-n;
- Czecoin (CZECO): PoS – x13;
- Dadcoin (DAD): PoW – SHA3-256;
- DaffyBucks (DFY): pow-pos – scrypt;
- DafuqCoin (DFQ): PoW – scrypt;
- DaggaCoin (DAG): PoS – x13;
- DaMaCoin (DMC): PoW – scrypt;
- DarkBit (DB): PoS – scrypt;
- Darkblock (DBLO): PoS – x11;
- Darkcash (DRKC): PoS – x11;
- DarkCash (DSK): PoS – stackhash;
- Darkchaincoin (DC): PoW – x11;

- Darkcoin (DARK): PoS – SHA2-256;
- Darkcoin (DRK): PoW – x11;
- DarkCorgi (DCORG): PoW – scrypt;
- DarkCrave (DCC): PoS – SHA2-256;
- DarkCredit (DKC): PoS – x13;
- DarkCypher (DCYP): PoS – x11;
- Darkether (DETH): PoS – x11;
- DarkEyeCoin (XE): PoW – scrypt;
- DarkFoxcoin (DRX): PoS – SHA2-256;
- DarkGold (DGD): PoS – x13;
- DarkKush (DANK): PoS – x13;
- Dark Moon (MOOND): PoS – scrypt;
- Darknet (DNET): PoS – quark;
- DarkNetCoin (DNC): PoW – SHA3-512;
- Darknetmarketcoin (DNM): PoS – x13;
- Darkpay (DRKPY): PoS – SHA2-256;
- DarkPeer (DPC): PoS – scrypt;
- DarkScrypt (DASC): PoW – scrypt;
- DarkShibe (DSB): PoS – scrypt;
- DarkSig (DSIG): PoS – SHA2-256;
- Darkswift (DS): PoW – x13;
- DarkToken (DT): PoW – nist5;
- Darktron (DRKT): PoS – SHA2-256;
- Dash (DASH): PoW – x11;
- Dashcoin (DSH): PoW – cryptonight;
- DashLite (DASHL): PoW – SHA2-256;
- Datacoin (DTC): PoW – primechain;
- DaVinciCoin (DAV): PoS – scrypt;
- Daycoin (DAC): PoW – scrypt;
- DayTraderCoin (DTC): PoS – x13;
- DeafDollars (DEAF): PoW – scrypt;
- DeathisNear (DIN): PoS – x11;
- Debtcoin (DBT): PoW – x11;
- Decennary (ARY): PoW – SHA2-256;
- Deciphercoin (DEC): PoW – scrypt;
- DecryptRcoin (DECR): PoW – SHA2-256;
- Deepcoin (DCN): PoW – trisha;
- Defusedcoin (DEC): PoW – scrypt;
- DeleteCoin (DEL): PoW – scrypt;
- Deltacoin (DELTA): PoW – scrypt;
- DeltaCredits (DCR): PoS – x11;
- DeluxCoin (DLUX): PoS – scrypt;
- DemonCoin (DC): PoW – scrypt;
- Demonic (DMON): PoS – quark;
- Denarius (DRS): PoW – scrypt;
- DeOxyRiboseCoin (DNA): PoS – x11;
- DeOxyRiboseCoin (XNA): PoS – thiamine;
- DEPO-* (DEPO): PoS – x11;
- Desicoin (DESI): PoW – scrypt;
- Destiny (D): PoW – scrypt;

- Destinycoin (DTC): PoW – scrypt-j;
- Deucecoin (DEUCE): PoW – scrypt;
- Deutsche eMark (DEM): PoS – SHA2-256;
- Devascoin (DEC): PoS – x13;
- Devcoin (DVC): PoW – SHA2-256;
- Diamond (DMD): PoS – scrypt;
- DiamondBack (DBK): PoW – cryptonight;
- DianKacoin (YXC): PoW – scrypt;
- Dibbits (DIBS): PoS – scrypt;
- Dicecoin (DC): PoS – x13;
- Dickcoin (SMD): PoW – scrypt;
- Dieselcoin (DZL): PoW – scrypt;
- Diffcoin (DIFF): PoW – scrypt;
- Diggits (DGT): PoS – scrypt;
- DIGI (DIGI): PoW – scrypt;
- DigiByte (DGB): PoS – scrypt;
- Digicube (CUBE): PoS – SHA2-256;
- DigiEuro2 (DEUR2): PoW – SHA2-256;
- DigiEuro SCRYPT (DEUR): PoW – scrypt;
- DigiEuroSHA256 (DEUR): PoW – SHA2-256;
- Digigems (DGMS): PoW – scrypt;
- Digit (DIG): PoS – scrypt;
- Digitalblock (DBLK): PoW – scrypt;
- Digitalcoin (DGC): PoW – scrypt;
- DigitalCommercecoin (DCM): PoS – scrypt;
- DigitalCredits (DGCS): PoW – SHA2-256;
- DigitalPrice (DP): PoW – x11;
- DigitalTaler (DTR): PoS – x13;
- Dijkstracoin (DKC): PoS – scrypt;
- Dilmacoin (DILMA): PoW – x11;
- Dimecoin (DIME): PoW – quark;
- Dimecoindirty (DIRT): PoW – SHA2-256;
- Dinarcoin (IQD): PoW – SHA2-256;
- Dinosaurcoin (DINO): PoS – x15;
- Diocoin (DIO): PoW – scrypt;
- Diode (DIO): PoS – x13;
- Diraccoin (XDQ): PoW – BLAKE;
- Dirkcoin (DKC): PoW – scrypt;
- DirtyCoin (DIT): PoW – x11;
- Discountcoin (DCT): PoS – SHA2-256;
- DisneyCoin (IDISNEY): PoS – SHA2-256;
- Distroblitz (DB): PoS – scrypt;
- Distrocoin (DISTRO): PoW – scrypt;
- Dizhucoin (DIZ): PoS – x13;
- DNAcoin (XNA): PoW – cryptonight;
- DNotes (NOTE): PoW – scrypt;
- Dobbscoin (BOB): PoW – scrypt;
- DoctorByte (DB): PoS – cryptonight;
- DogeBlackCoin (DOGEBC): PoW – SHA2-256;
- Dogecoin (DOGE): PoW – scrypt;

- DogecoinCash (DOGEC): PoW – scrypt;
- DogecoinDark (DD): PoS – x13;
- DogeCoinDark (DOGED): PoS – scrypt;
- DogeGorecoin (DGORE): PoW – x11;
- Dogeparty (XDP): PoS – SHA2-256;
- Dojecoin (DOJE): PoS – scrypt;
- Dokdocoin (DDC): PoW – scrypt;
- DollarPound (DPZ): PoW – scrypt;
- DolphinCoin (DOLP): PoS – scrypt;
- Domecoin (DOME): PoW – scrypt;
- Donatecoin (DON): PoW – scrypt;
- Donationcoin (DON): PoW – scrypt;
- Doomcoin (DOOM): PoW – Luffa;
- DopeCoin (DOPE): PoW – scrypt;
- Doscoin (DOS): PoS – x13;
- DoshKapitalcoin (DOSH): PoW – cryptonight;
- Dotacoin (DOC): PoW – SHA2-256;
- Dotcoin (DOT): PoW – scrypt;
- Doublecoin (XDBL): desconhecido – novel;
- DoubleEaglecoin (XDE): PoS – x15;
- Doubloon (DBL): PoW – scrypt;
- Dougcoin (DOUG): PoW – quark;
- Down coin (DOWN): PoW – scrypt-n;
- Doxcoin (DOX): PoS – scrypt;
- DRACHMacoin (DRAC): PoW – myriad;
- Draco (DRACO): PoS – SHA2-256;
- DraculaCoin (DRA): PoS – scrypt;
- Draftcoin (DFT): PoS – scrypt;
- DragonCoin (DNC): PoW – scrypt;
- Dragonsphere (XDB): PoS – x11;
- Drcoin (ISK): PoW – scrypt;
- Dreamcoin (DRM): PoW – x11;
- DrizzyCoin (DRKE): PoW – scrypt;
- Droidz (DRZ): PoS – qubit;
- Dropcoin (DROP): PoW – droplp;
- DSValue (DSV): PoW – x11;
- Dubaicoin (DBIC): PoW – SHA2-256;
- Dubcoin (DUB): PoS – x15;
- Dubeucoin (DBU): PoW – scrypt;
- Dubstep (DUB): PoS – qubit;
- Dubstepcoin (WUBS): PoW – scrypt;
- Ducats (DUC): PoW – quark;
- DuckDuckCoin (DUCK): PoW – scrypt;
- duckNote (XDN): PoW – cryptonight;
- Dulorcoin (DUL): PoS – x13;
- DumDumGumGum (DUMDUM): PoW – x11;
- Duoduocoin2 (DDC2): PoS – SHA2-256;
- Dustcoin (DUST): PoS – x11;
- Dvorakoin (DVK): PoW – myriad;
- Dynamiccoin (DC): PoW – scrypt;

- Dynasty (DYN): PoS – scrypt;
- Eagle (EA): PoW – SHA2-256;
- Eaglecoin (EAGLE): PoW – scrypt;
- EagleCoin (EGC): PoW – scrypt;
- EAGScurrency (EAGS): PoS – SHA2-256;
- EarthCoin (EAC): PoW – scrypt;
- EarthDollar (ED): PoS – x11;
- EasterCoin (ETR): PoW – quark;
- Ebolacoin (EBOLI): PoS – scrypt;
- EbolaShares (EBOLA): PoS – x11;
- ECash (CASH): PoW – x11;
- ECCoin (ECC): PoS – scrypt;
- eCent (ECNT): PoW – scrypt;
- EchoCoin (ECHO): PoW – scrypt;
- Eclipse (EC): PoS – SHA2-256;
- Eclipse (ECP): PoS – quark;
- eClipse-coin (ECLI): PoW – scrypt;
- Ecocoin (ECO): PoW – scrypt;
- eCoin (ECN): PoW – SHA3-256;
- ECurrency (ISO): PoW – SHA2-256;
- Edge (EDGE): PoS – SHA2-256;
- Edgecoin (EDC): PoS – x15;
- EdisonX3 (EDISON): PoW – scrypt;
- eDollar (EDC): PoW – scrypt;
- EduCoin (EDU): PoW – scrypt;
- EdwardSnowdenCoin (ESC): PoW – SHA2-256;
- Eggcoin (EGG): PoS – scrypt;
- EiniaOraCoin (EOC): PoS – scrypt;
- Einsteinium (EMC2): PoW – scrypt;
- Eirecoin (EIR): PoW – scrypt;
- Ekitacoin (EKITA): PoS – x11;
- Ekrona (KRN): PoW – scrypt;
- Elacoin (ELC): PoW – scrypt;
- Electric (ELE): PoW – scrypt;
- ElectricCoin (VOLT): PoS – scrypt;
- Electroncoin (ELT): PoW – BLAKE;
- ElectronicBenefitTransfer (EBT): PoS – scrypt;
- ElectronicGeoCacheCoin (EC): PoW – scrypt;
- Electronic Gulden (EFL): PoW – scrypt;
- Electronic Lira (LIRE): PoW – x11;
- ElectronicYen (EYEN): PoW – x11;
- Elektron (EKN): PoS – x13;
- Element (ELM): PoS – SHA2-256;
- ElephantCoin (ELP): PoW – scrypt;
- Elira (ELIRA): PoW – x11;
- Elitecoin (ELITE): PoS – x11;
- EmbargoCoin (EBG): PoW – SHA2-256;
- Emerald (EMD): PoW – scrypt;
- Emercoin (EMC): PoS – SHA2-256;
- EmiratesCoin (UAE): PoS – x11;

- EMoney (ECASH): PoS – SHA2-256;
- Emoticoin (EMO): PoW – scrypt;
- Emperor coin (EPC): PoW – scrypt;
- EmpoCredits (XEMP): PoS – x11;
- Emptycoin (EMP): PoS – scrypt;
- Empyrean (EPY): PoW – scrypt;
- Emucoin (EMU): PoW – scrypt-n;
- Endthebloodshed (BLOOD): PoS – qubit;
- Enecoin (ENE): PoW – x13;
- Energycoin (ENRG): PoS – scrypt;
- Enigmacoin (XEN): PoS – x11;
- EnigmaCoin (ENC): PoS – x13;
- Entertaincoin (ETC): PoW – scrypt;
- Entropybit (EBT): PoS – scrypt;
- EntropyCoin (ENC): PoW – scrypt;
- Entrustcoin (ETRUST): PoS – scrypt;
- EnvyCoin (ENVY): PoW – x11;
- EonCoin (EON): PoS – scrypt;
- ePayerCoin (PAYER): PoW – SHA2-256;
- Equalicoin (EQC): PoW – scrypt;
- EquestrianBit (EQB): PoW – scrypt;
- Equilibria (EQI): PoW – SHA3-256;
- EquilibriumCoin (EQM): PoS – SHA2-256;
- EquinoxManagement (EQX): PoS – x11;
- Ermahgerd (EMG): PoW – scrypt;
- Ermiscoin (ERM): PoS – SHA2-256;
- Error502Coin (502): PoW – scrypt;
- ErrorCoin (ERR): PoW – scrypt;
- EscudoPt (ESC): PoW – scrypt;
- ESportsCoin (ESC): PoW – x11;
- eSportsMoney (ESM): PoW – scrypt;
- eTaler (TALER): PoW – SHA2-512;
- Eternalcoin (ETC): PoW – scrypt;
- EternalCoin (ETC): PoW – scrypt;
- Eternitycoin (ETC): PoS – scrypt;
- Ethancoin (ETHAN): PoS – nist5;
- Ethanolium (C2H5OH): PoW – cryptonight;
- Ethercoin (ETC): PoS – scrypt;
- EtherDoge (DOGETH): PoS – x11;
- Ethereum (ETH): PoW – Dagger;
- EthereumDark (ETD): PoS – x11;
- Eticoin (ETC): PoW – scrypt;
- eToken (ETOK): PoS – scrypt;
- eUK (EUK): PoW – scrypt;
- Euphoriacoin (EUP): PoW – scrypt-n;
- Euphoriacoin (EUPH): PoS – x13;
- Eurasiancoin (EAC): PoW – scrypt;
- Eurobit (EBI): PoW – scrypt;
- Eurocoin (EUC): PoW – SHA2-256;
- Eurocoin (EURC): PoS – scrypt;

- EuroCoin (EUK): PoW – scrypt;
- Europacoin (EUROPA): PoW – scrypt;
- Europecoin (ERC): PoS – x11;
- eUtopiumCoin (UPM): PoS – nist5;
- EventToken (EVENT): PoS – scrypt;
- Evergreencoin (EGC): PoS – x15;
- Evilcoin (EVIL): PoS – x11;
- Evolvecoin (EVC): PoW – scrypt;
- Evopoints (XEV): PoS – scrypt;
- Evotion (EVO): PoS – SHA2-256;
- ExaByte (EXB): PoW – myriad;
- Exchangecoin (EXC): PoW – myriad;
- ExclusiveCoin (EXCL): pow-pos – x11;
- Execoin (EXE): PoW – scrypt-n;
- Exilecoin (EXN): PoS – scrypt;
- Exocoin (EXO): PoW – desconhecido;
- Expanse (EXP): PoW – Dagger;
- Experiencecoin (EPC): PoW – scrypt;
- Extractcoin (XTR): PoW – scrypt;
- ExtremeCoin (EXC): PoS – scrypt;
- EZCoin (EZC): PoW – scrypt;
- FacebookCoin (FBC): PoS – scrypt;
- Factoid (FCT): PoW – SHA2-256;
- Fade (FADE): PoS – x11;
- FailCoin (FAIL): PoW – scrypt;
- Fairbrix (FBX): PoW – scrypt;
- Fairbytecoin (FBT): PoW – x13;
- FairCoin (FAIR): PoS – scrypt;
- Fairquark (FRQ): PoW – quark;
- FakeCoin (FKC): PoW – scrypt;
- Falcoin (FALC): PoW – nist5;
- FaldoranScrypt (FSC): PoW – scrypt;
- Fantom (FNX): PoS – velvet;
- Fantomcoin (FCN): PoW – cryptonight;
- Fastcoin (FST): PoW – scrypt;
- Fastcoin2 (FSC2): PoW – scrypt;
- FastcoinSHA (FSS): PoW – SHA2-256;
- Fatecoin (FATE): PoW – scrypt-j;
- FateofWhale (WHL): PoW – scrypt;
- Faucetcoin (FEC): PoW – scrypt;
- Faucetcoin (DROP): PoS – x13;
- FBcoin (XFB): PoS – scrypt;
- Fckbankscoin (FCK): PoW – scrypt;
- Feathercoin (FTC): PoW – scrypt;
- FeatherCoinClassic (FTCC): PoW – scrypt;
- FederalReserveCoin (FRSC): PoW – scrypt;
- FedoraCoin (TIPS): PoW – scrypt;
- Feecoin (FEE): PoW – pluck-128;
- Feelscoin (FEEL): PoS – scrypt;
- FellatioCoin (BLO): PoW – scrypt;

- Ferengicoin (FER): PoW – SHA2-256;
- Ferretcoin (FEC): PoS – scrypt-j;
- Fetishcoin (FETISH): PoW – SHA2-256;
- FFFCoin (FFF): PoW – SHA2-256;
- FHRITPcoin (FRED): PoW – x15;
- Fiatcoin (FIAT): PoS – *unknown* (desconhecido);
- Fibrecoin (FIBRE): PoS – nist5;
- FIFAWCcoin (FWCC): PoS – x13;
- FiftyShadesofCoin (FIFTY): PoW – SHA2-256;
- FileBitcoin (FBIT): PoS – x15;
- Filecoin (FC): PoW – novel;
- FilmCoin (FILM): PoS – x13;
- FimKcoin (FIMK): PoS – nxt;
- Findcoin (FIND): PoS – x13;
- Finercoin (XFC): PoS – x11;
- Firecoin (FEC): PoS – scrypt-j;
- Firecoin (FIRE): PoS – x15;
- Firecoin2 (FC2): PoW – scrypt;
- FireflyCoin (FFC): PoW – SHA2-256;
- FireGeek (GEEK): PoW – x11;
- Fire-ice (FICE): PoS – x11;
- FirstAfricanCoin (FACC): PoS – x11;
- Fishcoin (FISH): PoW – scrypt;
- FistBumpcoin (FIST): PoS – x13;
- Fitcoin (FIT): PoW – x11;
- FiveHundredCoins (FHC): PoW – SHA2-256;
- Fixcoin (FIX): PoW – scrypt;
- FlappyCoin (FLAP): PoW – scrypt;
- Flashcoin (FLC): PoW – scrypt;
- FlashCoin (FLASH): PoS – x13;
- FlavorCoin (FLAV): PoW – x13;
- Flaxcoin (FLAX): PoW – c11;
- FlexCoin (FCX): PoW – SHA2-256;
- Flexiblecoin (FLEX): PoS – x15;
- Flirtcoin (FLIRT): PoW – SHA2-256;
- Floridacoin (FLC): PoW – scrypt;
- FlorinCoin (FLO): PoW – scrypt;
- Floripacoin (FLN): PoW – scrypt;
- FlowerCoin (FLOW): PoS – x11;
- Floz (FLOZ): PoS – SHA2-256;
- Fluttercoin (FLT): PoW – scrypt;
- Flux (FLX): PoW – SHA3-256;
- Flycoin (FLY): PoS – x13;
- Foldingcoin (FLDC): PoS – folding;
- Folkart (FOLK): PoW – scrypt;
- FonzieCoin (XFC): PoS – SHA2-256;
- Football2014coin (FBC): PoS – scrypt;
- Footballcoin (FBC): PoW – scrypt;
- Footy Cash (FOOT): PoS – scrypt;
- ForeverCoin (XFC): PoS – SHA2-256;

- Forexcoin (FRX): PoW – scrypt;
- Forumcoin (FRM): PoW – x13;
- Forvikcoin (FKG): PoW – SHA2-256;
- FourOhFourCoin (FOF): PoW – scrypt;
- FoxCoin (FOX): PoW – scrypt;
- Fractalcoin (FRAC): PoW – x11;
- Franc Noir (FRN): PoW – scrypt;
- Franko (FRK): PoW – scrypt;
- FreeAnonymousInternet (FAI): PoW – mhash;
- FreebiesCoin (FREEB): PoW – scrypt;
- Freecoin (FRE): PoW – scrypt-j;
- Freedom (FRDC): PoS – x11;
- Freedomcoin (FDC): PoW – scrypt;
- Freemasoncoin (FMC): PoW – SHA2-256;
- Freicoin (FRC): PoS – SHA2-256;
- FrenchGenius (GENIUS): PoS – scrypt;
- Frequency (FREQ): PoS – SHA2-256;
- Freshcoin (FRSH): PoW – fresh;
- Frictionlesscoin (FLC): PoW – friction;
- Friendshipcoin (FSC): PoW – scrypt;
- FriendshipCoin2 (FSC2): PoS – scrypt;
- Frogcoin (FGC): PoW – scrypt;
- FrozenCoin (FZ): PoW – quark;
- Fruitcoin (FRUIT): PoS – x11;
- Fruppocoin (FRP): PoW – SHA2-256;
- Frycoin (FRY): PoW – scrypt;
- Fuckcoin (FUCK): PoW – scrypt;
- Fucoin (FU): PoW – SHA2-256;
- FuCoin (FUC): PoS – scrypt;
- FUDcoin (FUD): PoW – SHA2-256;
- FuelCoin (FUEL): PoW – SHA2-256;
- FuelCoin (FC2): PoS – x11;
- Fuguecoin (FC): PoW – Fugue;
- Fujicoin (FJC): PoW – scrypt-n-f;
- FullIntegritycoin (FIC): PoW – scrypt;
- Funcoin (FUN): PoW – scrypt;
- FunCoin (FNC): PoS – x11;
- Functioncoin (FCC): PoW – hefty1;
- FundCoin (FUND): PoS – x13;
- FunUnderCoinKing (FUCK): PoW – SHA2-256;
- FuriousandFast (FAF): PoS – x13;
- FurryCoin (FUR): PoW – scrypt;
- Fusecoin (FUSE): PoS – x11;
- Fusion (FSN): PoS – SHA2-256;
- Fusioncoin (FSC): PoW – scrypt;
- Futcoin (FUT): PoS – x13;
- Futurecash (FRC): PoS – scrypt;
- Futurecoin (FTR): PoS – nxt;
- Futurecoin (KFC): PoW – trisha;
- Fuzonc (FZN): PoS – nxt;

- Fuzzballs (FUZZ): PoW – scrypt;
- FVZcoincoin (FVZ): PoW – x11;
- G8coin (G8): PoW – scrypt;
- GabeCoin (GAC): PoW – scrypt;
- Gabencoin (GBN): PoW – scrypt;
- GadgetCoin (GDC): poc – unknown;
- Gadsdencoin (GAD): PoW – SHA2-256;
- Gaelcoin (GAC): PoW – scrypt;
- GAIAcoin (GAIA): PoS – scrypt;
- GalacticCreditStandard (GCR): PoW – x11;
- Galaxycoin (GLX): PoS – scrypt;
- Galleon (GLN): PoW – SHA3-256;
- Galtcoin (GLT): PoW – scrypt;
- Gambit (GAM): PoS – scrypt;
- GameCoin (GME): PoW – scrypt;
- GameCredits (GMC): PoW – scrypt;
- GameCryptocoin (GEC): PoS – x11;
- Gameleaguecoin (GML): PoS – scrypt;
- GamerHolicCoin (GHC): pow-pos – SHA2-256;
- GamersCoin (GMC): PoW – scrypt;
- GammaCoin (GMC): PoW – scrypt;
- Gangnamstylecoin (GSC): PoW – scrypt;
- Ganjacoin (GANJA): PoS – x14;
- Gapcoin (GAP): PoW – primegap;
- Gascoin (GAS): PoW – scrypt;
- Gascoin (GAS): PoS – x11;
- GascoinExtreme (GSX): PoW – SHA2-256;
- Gatescoin (GTC): PoW – scrypt;
- Gatlingcoin (GC): PoS – scrypt;
- Gaycoin (GAY): PoW – SHA2-256;
- GBCGoldCoin (GBC): PoS – scrypt;
- GB Coin (GBC): PoW – scrypt-n;
- GCoin (GCN): PoW – scrypt;
- Geekkoscoin (GEEK): PoS – scrypt;
- GeistGeld (GG): PoW – SHA2-256;
- Genercoin (GEN): PoS – SHA2-256;
- Genesiscoin (GENE): PoW – scrypt;
- GenesisCoin (GNS): PoW – scrypt-n;
- GenesysCoin (GSY): PoS – SHA2-256;
- Genius (GNS): PoW – scrypt;
- Genstake (GEN): PoS – scrypt;
- GeoCoin (GEO): PoS – qubit;
- GeoCoin (GEO): PoS – x11;
- GeoCoin (GEO): PoW – scrypt;
- Germanycoin (GER): PoW – scrypt;
- Ghostcoin (GHC): PoS – scrypt;
- GhostCoin (GHOST): PoS – x11;
- Ghoul (GHOUL): PoW – scrypt;
- Giarcoin (GIARCOC): PoW – scrypt-n;
- GiftCardCoin (GIFT): PoS – x13;

- Giftcoin (GFT): PoW – scrypt;
- GigaCoin (GIG): PoS – fresh;
- GilCoin (GIL): PoW – scrypt;
- Gimpcoin (GMP): PoS – x13;
- GirlCoin (GIRL): PoW – scrypt;
- Giveawaycoin (GC): PoS – scrypt;
- Givebackcoin (GIV): PoW – myriad;
- Give Coin (GIVE): PoW – x11;
- Gizmocoin (GIZ): PoS – x11;
- Glaricoin (GLC): PoW – SHA2-256;
- Glidecoin (GLIDE): por – scrypt;
- GlobalBoost (BST): PoW – scrypt;
- GlobalBoost-Y (BSTY): PoW – scrypt;
- GlobalCoin (GLC): PoW – scrypt;
- Globalcurrency (GLOBE): PoS – SHA2-256;
- GlobalCurrencyReserve (GCR): PoS – scrypt;
- Global Denomination (GDN): PoW – x11;
- GlobalInternetcoin (GIC): PoS – x13;
- Globe (GLB): PoW – SHA2-256;
- GlowCoin (GLOW): PoS – x13;
- Glowshares (GSX): PoS – scrypt;
- Glyphcoin (GLYPH): PoS – x11;
- Gnosiscoin (GNS): PoS – scrypt;
- Goalcoin (GOAL): PoW – scrypt;
- Goat (GOAT): PoS – scrypt;
- Gobangcoin (GBC): PoS – x11;
- Godcoin (GDC): PoW – x11;
- Goddesscoin (GODD): PoS – x13;
- Godzillacoin (ZILLA): PoS – Grøstl;
- Gold Backed Coin (GBC): PoW – ripple;
- GoldBars (GDB): PoW – scrypt;
- GoldCoin (GLD): PoW – scrypt;
- GoldenLoafcoin (GLY): PoW – x11;
- Gold Flexibly (JRY): PoW – scrypt;
- Goldmaxcoin (GMX): PoW – SHA2-256;
- Goldpieces (GP): PoS – x11;
- GoldPressedLatinum (GPL): PoW – scrypt;
- Gold Pressed Latinum (GPL): PoS – scrypt-j;
- GoldReserve (XGR): PoS – x11;
- GoldRushcoin (GRC): pow-pos – scrypt;
- GoldRushcoin (GOLDR): PoW – scrypt;
- Goldstake (GDST): PoS – x13;
- Golfcoin (GOLF): PoW – scrypt;
- Gollumcoin (GLM): PoW – scrypt;
- Gongyicoin (GYC): PoW – x13;
- Goodbye coin (BYE): PoW – scrypt;
- GoodCoin (GOOD): pow-pos – scrypt;
- GoodLuck (GLUCK): PoS – SHA2-256;
- GorillaBalloons (GBLS): PoW – scrypt;
- GorillaBucks (BUCKS): PoS – SHA2-256;

- Gorillateeth (TEETH): PoS – scrypt;
- Gotfomo (GTFO): PoS – SHA2-256;
- Goxcoin (GOX): PoS – scrypt;
- GPU Coin (GPUC): PoW – scrypt-n;
- Graffiti (GRF): PoS – scrypt;
- Grain (GRA): PoS – scrypt;
- Gramcoin (GRAM): PoW – SHA2-256;
- GrandCoin (GDC): PoW – scrypt;
- Granite (GRN): PoS – x11;
- Grantcoin (GRT): PoS – SHA2-256;
- Graph (GRAPH): PoS – scrypt;
- Graphene (GRP): PoW – scrypt-j;
- Graviton (GRAV): PoS – SHA2-256;
- GravityBits (GBIT): PoS – SHA2-256;
- Grdtcoin (GRDT): PoW – scrypt;
- Greececoin (GRCE): PoW – scrypt;
- Greed (GREED): PoS – SHA2-256;
- Greedcoin (GDC): PoW – x11;
- GreedEvolved (GE): PoW – scrypt;
- Greekcoin (GRK): PoS – x11;
- GreenBacks (GB): PoS – nist5;
- Greencoin (GRE): PoW – scrypt;
- GreenCoinX (GREX): PoW – x11;
- Greenshilling (GRS): PoW – x11;
- Grexitcoin (GREXIT): PoS – x11;
- GreyCoin (GREY): PoW – c29;
- GridBit (GRID): PoS – x13;
- Gridcoin Classic (GRCX): PoW – scrypt;
- Gridcoin Research (GRC): por – boinc;
- Gridmaster (GMC): PoS – SHA2-256;
- Grifcoin (GFC): PoW – scrypt;
- Griftcoin (GRIFT): PoS – x17;
- GroestlCoin (GRS): PoW – Grøstl;
- Groincoin (GXG): PoW – x11;
- Groupcoin (GPC): PoS – x13;
- GroupCoin (GRP): PoW – SHA2-256;
- Growcoin (GROW): PoS – scrypt;
- GrowthCoin (GRW): PoS – scrypt;
- Grumpycoin (GRUMP): PoW – scrypt;
- Gryfencoin (GRYF): PoW – x15;
- GSCcoin (GSC): PoW – scrypt;
- GSMcoin (GSM): PoS – x11;
- GuarantCoin (GTC): PoW – scrypt-n;
- Guarany (GUA): PoW – scrypt;
- Guccionecoin (GCC): PoS – scrypt;
- Guccione Crypto Moneta (GCMA): PoS – scrypt;
- Guerillacoin (GUE): PoS – x11;
- Guineacoin (GUINEA): PoW – SHA2-256;
- Guldencoin (NLG): PoW – scrypt;
- Guncoin (GUN): PoW – scrypt;

- Guzhicoin (XPC): PoS – x11;
- Gytecoin (GEC): PoW – scrypt;
- H2Ocoin (H2O): PoW – scrypt-n;
- h4xx0rcoin (H4X): PoS – scrypt;
- HackCoin (HACK): PoW – x11;
- Hadokencoin (HDK): PoS – scrypt;
- Halcyoncoin (HAL): PoS – x15;
- Halfcoin (HLFC): PoW – SHA2-256;
- Hamburgercoin (HAC): PoW – scrypt;
- Hamradiocoin (HAM): PoW – SHA2-256;
- Hamstercoin (HAM): PoW – scrypt;
- HansaCoin (HANSA): PoS – scrypt;
- HappyCoin (HPY): PoS – x11;
- Harcoin (HAR): PoW – myriad;
- HardCidercoin (WHC): PoS – x13;
- Hardforkcoin (HFC): PoW – BLAKE;
- Harmonycoin (HMY): PoS – x13;
- HashBars (HSB): PoW – SHA2-256;
- Hashcoin (HASH): PoW – x11;
- HashPay (HAP): PoS – scrypt;
- Hawaiicoin (HIC): PoW – scrypt;
- Hawk (HAWK): PoS – SHA2-256;
- Hayekcoin (HKC): PoW – scrypt;
- Hayekcoin (HAYEK): PoS – scrypt;
- Hazecoin (HAZE): PoW – scrypt;
- HazMatCoin (HZT): PoS – scrypt;
- Heavycoin (HVC): PoW – hefty1;
- Hedge (HEDG): PoW – x13;
- Heelcoin (HEEL): PoS – scrypt;
- Heisenberg (HEX): PoW – scrypt;
- Helixcoin (HXC): PoW – SHA3-256;
- Hellascoin (HLC): PoW – scrypt;
- Helleniccoin (HNC): PoW – scrypt;
- Helveticacoin (CHC): PoW – scrypt;
- Hempcoin (THC): PoS – scrypt;
- HempFarmcoin (THC): pow-pos – scrypt;
- Heracoin (HRC): PoW – scrypt-j;
- Herocoin (HRO): PoW – scrypt-j;
- Hertzcoin (HZ): pow-pos – x13;
- Hexacoin (HEX): PoW – scrypt;
- Hexion (HXC): PoS – SHA2-256;
- Hexx (HXX): PoS – scrypt;
- HighFiveCoin (H5C): PoW – x11;
- Hirocoin (HIRO): PoW – x11;
- Hispacoin (HPC): PoW – SHA2-256;
- Hispacoin2 (HPC): PoW – scrypt;
- Hive (HIVE): PoS – hive;
- Hmoobcoin (HMO): PoW – scrypt;
- Hobbitcoin (HBC): PoW – scrypt;
- HoboNickels (HBN): PoS – scrypt;

- HODLCoin (HODL): PoW – x11;
- Hodorcoin (HODOR): PoS – x11;
- Homocoin (GAY): PoW – scrypt;
- Hongketocoin (HKC): PoW – SHA2-256;
- Hongkongcoin (HKC): PoW – SHA2-256;
- HongxingCredits (HXC): PoW – SHA2-256;
- Honorcoin (XHC): PoS – x11;
- HonorCoin (HC): PoS – scrypt;
- Honorcoin2 (XHC): PoS – x13;
- HooliganPound (HOP): PoW – scrypt;
- Horsecoin (HORS): PoW – scrypt;
- HorsePowerCoin (HSP): PoW – scrypt;
- Horuscoin (RX): PoW – scrypt-n-r;
- Hotcoin (HOT): PoW – scrypt;
- Hotdogcoin (HDC): PoW – scrypt;
- Hotelcoin (HOTEL): PoW – scrypt;
- HouseMonkeycoin (HMC): PoW – fresh;
- Houseofcoins (HOC): PoW – scrypt;
- Htmlcoin (HTML): PoW – scrypt;
- HTMLCoin (HTML5): PoS – x15;
- HuaShengCoin (HSC): PoS – SHA2-256;
- Huaxiabicoin (HXC): PoW – scrypt;
- Huitong (HC): PoW – scrypt;
- HumanCoin (HMC): PoS – x11;
- Hundredcoin (HUN): PoW – scrypt;
- HunterCoin (HUC): PoS – scrypt;
- Huskycoin (HC): PoS – x11;
- Hydrogencoin (H2): PoS – scrypt;
- Hyper (HYPER): PoS – scrypt;
- Hypercoin (HYC): PoW – scrypt;
- Hyperstakecoin (HYP): PoS – x11;
- I0Coin (I0C): PoS – SHA2-256;
- Iamcoin (IAM): PoW – x11;
- IaurabCoin (IAURAB): PoS – x11;
- iBits (IBIT): PoS – scrypt;
- ICash (ICASH): PoW – x11;
- Iceberg (ICB): PoS – nist5;
- IceCoin (ICE): PoW – scrypt;
- Icecube45 coin (ICE): PoW – scrypt;
- ICOCoin (ICO): PoS – scrypt;
- iCoin (ICN): PoW – scrypt;
- IconicExpertCoin (IEC): PoS – x11;
- IconicXcoin (ICNX): PoS – x11;
- IdeaCoin (IDC): PoW – nist5;
- Illuminati (ILM): PoS – x11;
- ILoveYoucoin (ILY): pow-pos – scrypt;
- IMAcreditcoin (IMAC): PoW – scrypt-n;
- ImperialCoin (IMP): PoW – SHA2-256;
- ImperialCoin (IPC): PoW – scrypt;
- ImperiumCoin (IMPC): PoW – scrypt;

- IMPSasset (IMPS): PoS – nxt;
- IMScoin (IMS): PoS – scrypt;
- Imymoney (IMM): PoS – scrypt;
- Incakoin (NKA): PoS – SHA2-256;
- Incogcoin (ICG): PoS – x11;
- Incrementum (INC): PoS – x11;
- Index (IDX): PoW – x11;
- Indexcoin (IDC): PoW – scrypt;
- IndoCoin (IDC): PoW – scrypt;
- Industrycoin (IND): PoW – scrypt;
- Infinitecoin (IFC): PoW – scrypt;
- Infinium-8coin (INF8): PoW – cryptonight;
- Influxcoin (INFX): PoS – x11;
- Informationcoin (ITC): PoS – scrypt;
- INKcoin (INK): PoW – SHA3-256;
- InkWayCoin (LKNX): PoS – x11;
- Insanitycoin (INS): PoW – scrypt;
- Insanitycoin (WOLF): PoW – scrypt;
- Insertcoin (ISC): PoW – scrypt-j;
- Instacoin (INS): PoS – scrypt;
- InstaMineNuggets (MINE): PoW – scrypt;
- InstaMineNuggetsA (MINEW): PoW – scrypt;
- InstaMineNuggetsB (MINEZ): PoW – scrypt;
- Instantcoin (BTI): PoW – SHA2-256;
- InstantDEX (DEX): PoS – nxt;
- Instapay (IPC): PoW – scrypt-j;
- Intellect (ITL): PoS – x11;
- Intellicoin (INT): PoS – x13;
- Intercoin (INC): PoW – intercoin;
- Intercoin (ITC): PoW – scrypt;
- Internationalcoin (INC): PoW – quark;
- InternationalEurocoin (IEURO): PoW – lyra2re;
- Internetcoin (WWW): PoW – scrypt;
- InternetMarketingCoin (IMC): PoS – fresh;
- Investcoin (IC): PoS – x13;
- Investmentcoin (INC): PoW – SHA2-256;
- InvisibleCoin (IVZ): PoS – scrypt;
- I/Ocoin (IO): PoS – x11;
- Irccoin (IRC): PoW – scrypt;
- IRCoin (IRC): PoW – scrypt;
- IridiumCoin (IRI): PoW – scrypt;
- Irishcoin (IRL): PoW – scrypt;
- Ironbankcoin (IBC): PoS – scrypt;
- Isiscoin (ISIS): pow-pos – x15;
- IslaCoin (ISL): PoW – x11;
- Isotope (XTP): PoS – SHA2-256;
- Isracoin (ISR): PoW – scrypt;
- ItalyCoin (ITC): PoW – scrypt;
- iTcoin (ITC): PoW – SHA2-256;
- ITcoin (XIT): PoS – x11;

- Ivorycoin (IVC): PoS – x11;
- IvugeoEvolutionCoin (IEC): PoW – scrypt;
- Ivycoin (IVY): PoW – scrypt;
- Ivyleaguecoin (IVY): PoS – x11;
- iXcoin (IXC): PoW – SHA2-256;
- JackpotCoin (JACKPOT): PoW – jackpot;
- Jadecoin (JADE): PoW – x11;
- Jaguarcoin (JGR): PoS – x11;
- J-Coin (JPU): PoS – scrypt;
- JebigaCoin (JBG): PoW – scrypt;
- JennyCoin (JNY): PoW – scrypt;
- Jerkycoin (JKY): PoW – SHA2-256;
- Jesuscoin (GOD): PoW – scrypt;
- Jet (JET): PoW – SHA2-256;
- Jetcoin (JTC): PoS – nxt;
- JewelCoin (JEWEL): PoS – x13;
- JFKcoin (JFK): PoS – scrypt;
- JiffyCoin (JIF): PoW – SHA2-256;
- Jixiangcoin (JXC): PoW – scrypt;
- JJCoin (JJC): PoS – x13;
- jl777hodl (JLH): PoW – SHA2-256;
- JohnKeyoin (KEY): PoS – scrypt;
- Joincoin (J): PoW – myriad;
- JokeCoin (JOK): PoW – SHA2-256;
- Joulecoin (XJO): PoW – SHA2-256;
- Jubaocoin (JBC): PoW – scrypt-j;
- Judgecoin (JUDGE): PoS – x13;
- Juggalocoin (JUG): PoW – x11;
- JunkCoin (JKC): PoW – scrypt;
- JunnonCoin (JNC): PoW – scrypt;
- JupiterCoin (JPC): PoW – scrypt;
- Kachingcoin (KAC): PoW – scrypt;
- KaKacoin (KKC): PoW – scrypt;
- Karmacoin (KARM): PoS – scrypt;

- KarpelesCoin (KAR): PoW – scrypt;
- KashmirCoin (KSC): PoW – scrypt;
- KateCoin (KTC): PoW – SHA2-256;
- Katz (KAT): PoS – SHA2-256;
- Keplercoin (KPL): pow-pos – myriad;
- Kernalcoin (KC): PoS – SHA2-256;
- Keycoin (KEY): PoS – x13;
- KFcoin (KFC): PoW – quark;
- Khancoin (KNC): PoS – SHA2-256;
- Kibweecoin (KIB): desconhecido – x11;
- KillerCoin (KILR): PoW – scrypt;
- Kilocoin (KILO): PoW – scrypt;
- Kimcoin (KMC): PoW – quark;
- Kimcoin (KMC): PoW – nist6;
- Kimdotcoin (DOT): PoW – scrypt;
- KimJonguncoin (KJC): PoS – x13;
- Kimocoin (KIMO): PoW – scrypt-n;
- Kimotocoin (KMC): PoW – scrypt-n;
- KingCoin (KING): PoS – scrypt;
- Kingdomcoin (KING): PoS – x13;
- Kingkongcoin (K2C): PoW – scrypt;
- Kittehcoin (MEOW): PoW – scrypt;
- Kiwicoin (KIWI): PoW – x11;
- Klingon Empire Darsek (KED): PoS – scrypt;
- Klondikecoin (KDC): PoS – scrypt;
- Knavecoin (KNC): PoW – scrypt;
- Knifemoney (KM): PoW – scrypt;
- Knightcoin (KGC): PoW – x11;
- Koalacoin (KOALA): PoS – scrypt;
- Kobocoin (KOBO): PoS – x15;
- KOKain COIN (COC): PoW – scrypt;
- Kölschcoin (CGN): PoS – x11;
- Kooliocoin (KOOL): PoW – scrypt;
- KoreCoin (KORE): PoS – x13;
- Korunacoin (KORUNA): PoW – scrypt;
- Kozakcoin (KOZ): PoS – x11;
- Kraken (KRAK): PoS – SHA2-256;
- Krugercoin (KGC): PoW – scrypt;
- Krypt koin (KTK): PoS – scrypt;
- Kryptohash (KHC): PoW – kshake320;
- Krypton (KR): PoW – Dagger;
- Kryptonite (KRYP): PoW – x11;
- Kudos (KDS): PoW – scrypt;
- Kumacoin (KUMA): PoS – quark;
- KushCoin (KHC): PoW – scrypt;
- Labocoin (LBC): PoW – scrypt;
- LadyCoin (LADY): PoW – scrypt;
- Landcoin (LND): PoW – BLAKE;
- Latinocoin (LAT): PoW – scrypt;
- Latinumcoin (LTM): PoW – SHA2-256;

- Latium (LAT): PoS – scrypt;
- LeaCoin (LEA): PoW – SHA2-256;
- Leadcoin (LDC): PoW – scrypt;
- LeafCoin (LEAF): PoW – scrypt;
- LeagueCoin (LOL): PoS – x11;
- Learncoin (LERN): PoW – scrypt;
- Lebowskis (LBW): PoS – scrypt;
- LeCoin (LEC): PoS – scrypt;
- Ledgercoin (LDR): PoS – SHA2-256;
- Leetcoin (LEET): PoS – scrypt;
- Legendary Coin (LGD): PoS – scrypt;
- Legitcoin (XGT): PoS – x13;
- Lemonadecoin (LEO): PoW – SHA2-256;
- Lemoncoin (LMC): PoW – scrypt;
- LemonCoin (LEMON): PoW – argon2;
- Lemurcoin (LMR): PoW – x11;
- Lendcoin (LNC): PoS – scrypt;
- Lennycoin (LENNY): PoW – scrypt;
- LEOcoin (LEO): PoS – scrypt-j-n;
- Leprocoin (LPC): PoW – scrypt;
- Leverage (LVG): PoS – scrypt;
- LFTCCoin (LFTC): PoS – x11;
- LGBTQoin (LGBTQ): PoW – x11;
- Liberty coin (XLB): PoS – x11;
- LibertyReserve (LR): PoS – x11;
- Libertyreserved (LRD): PoS – nxt;
- Librarycoin (LIB): pow-pos – scrypt;
- Libremoney (LM): PoS – nxt;
- Librexcoin (LXC): PoS – x11;
- LickyBallyCoin (LBC): PoS – x11;
- Lifecoin (LIFE): PoW – scrypt;
- Life Extension (EXT): PoS – qubit;
- Lightcoin (LIT): PoS – x11;
- Lightspeedcoin (LSD): PoS – nist5;
- Likecoin (LIKE): PoW – scrypt;
- Limecoin (LC): PoW – scrypt;
- Limecoin (LMC): PoS – x11;
- Limecoin lite (LCL): PoW – SHA2-256;
- LimecoinX (LIMX): PoW – x11;
- Limicoin (LIMI): PoS – x15;
- Limitedcoin (LTD): PoS – x11;
- Linearcoin (LNC): PoW – x11;
- Linkcoin (LNC): PoW – scrypt;
- Lioncoin (LIC): PoW – SHA2-256;
- Lioncoin (LION2): PoS – x15;
- LionCoin (LION): PoW – x11;
- LiquidCoin (LQC): PoW – scrypt;
- Lisk (LISK): PoW – 3s;
- LiteBar (LTB): PoW – scrypt;
- Litecoin (LTC): PoW – scrypt;

- LitecoinDark (LTCD): PoW – scrypt;
- LitecoinNEW (LTN): PoW – scrypt;
- Litecoinplus (XLC): PoS – scrypt;
- Litecoinscrypt (LTCS): PoW – scrypt;
- LiteCoinX (LTCX): PoS – x11;
- LitecoinXT (LXT): PoW – scrypt;
- Litecred (LTCR): PoS – qubit;
- LiteDoge (LDOGE): PoS – scrypt;
- Litefeathercoin (LTFC): PoS – x11;
- Litercoin (LTR): PoW – x13;
- Liteshares (LTS): PoW – scrypt;
- Litestarcoin (LTS): PoS – x11;
- Lithiumcoin (LIT): PoW – BLAKE;
- LittleDarkcoin (LTD): PoW – x11;
- Livecoin (LVC): PoW – scrypt;
- LiveCoin (LC): PoW – x11;
- Lizardecoin (LIZE): PoS – x15;
- LoanCoin (LOANCO): PoS – x13;
- LocalFamilyOwned (LFO): PoS – scrypt;
- Lockcoin (LOCK): PoS – x11;
- Logicoin (LGC): PoW – x11;
- Logos (LGS): PoW – scrypt-n;
- Logoscoin (LOGOS): PoW – SHA2-256;
- LondonGoldCoin (LGC): PoW – SHA2-256;
- LongCoin (LNG): PoW – x11;
- Loot (LOOT): PoW – scrypt;
- LootCoin (LT): PoW – scrypt;
- LotteryShare (HAYEK): PoS – scrypt;
- Lotterytickets (TIX): PoW – scrypt-j;
- LottoCoin (LOT): PoW – scrypt;
- LottoShares (LTS): PoS – scrypt;
- Lotuscoin (LTS): PoS – x13;
- Lovecoin (LOVE): PoW – scrypt;
- LOVEcoin (LOVE): PoS – scrypt;
- Lovercoin (LVC): PoW – scrypt;
- LTBcoin (LTBC): PoS – SHA2-256;
- LTCGearCoin (XLTCG): PoW – x13;
- Lucky7Coin (LK7): PoS – scrypt;
- LuckyBlocks (BONUS): PoW – x11;
- Luckycoin (LKY): PoW – scrypt;
- LuckySevens (L7S): PoW – scrypt;
- Lunarcoin (LUN): PoS – x11;
- Lunarcoin (LNR): PoS – x13;
- Lure (LURE): PoS – SHA2-256;
- Lusocoin (LUC): PoW – SHA2-256;
- Luxurycoin (LXY): PoW – SHA2-256;
- LxcCoin (XWBC): PoS – scrypt;
- Lycancoin (LYC): PoW – scrypt;
- Lyrabar (LYB): PoS – lyra2re;
- Maccoin (MAC): PoW – SHA2-256;

- MACDcoin (MACD): PoS – x13;
- MacheteCoin (MCT): PoW – scrypt;
- Machinecoin (MAC): PoW – SHA2-256;
- MachineryCoin (MHYC): PoS – x11;
- Macoin (RM): PoW – scrypt;
- Macro (MACRO): PoW – x11;
- Macrocoin (MCR): PoW – scrypt;
- MadCowCoin (MCC): PoW – scrypt;
- Magcoin (MAG): PoW – x11;
- Magic Internet Money (MIM): PoW – scrypt;
- Magicoin (XMG): PoS – m7;
- Magicoin (MAGIC): PoW – scrypt;
- Magnatoj (XMN): PoW – cryptonight;
- Magneticoin (MGC): PoW – SHA2-256;
- Magnetz (MGT): PoW – x13;
- MaiaCoin (MAIA): pow-pos – x15;
- Maidsafecoin (MAID): PoS – SHA2-256;
- MajorCoin (MAJ): PoW – scrypt;
- Maki (MAKI): PoW – scrypt;
- Malecoin (MLC): PoW – scrypt;
- Malegebe (MLGB): PoS – x11;
- MalibuCoin (MAL): PoS – x11;
- Mammothcoin (MAMM): PoS – x13;
- Manacoin (MANA): PoW – scrypt;
- Mandarincoin (MAC): PoW – scrypt;
- Mangocoinz (MCZ): PoS – desconhecido;
- Mantiscoin (MNS): PoS – x11;
- ManulCoin (MANUL): PoW – scrypt;
- Mapcoin (MAPC): PoS – x11;
- Maplecoin (MPL): PoW – scrypt;
- Maples (MAP): PoW – scrypt;
- Marbles (MRB): PoS – SHA2-256;
- Marinecoin (MTC): PoW – scrypt;
- Marketchangecoin (CHG): PoW – scrypt;
- Marscoin (MRS): PoW – scrypt;
- MarteXcoin (MXT): PoW – scrypt;
- Marucoin (MARU): PoW – x13;
- Marxcoin (TYC): PoW – scrypt;
- MaryJanecoin (MARYJ): PoS – x15;
- Masoncoin (BROS): PoW – x11;
- Masoncoin (MAC): PoW – scrypt;
- Mastercoin (MSC): PoW – SHA2-256;
- MasterCoin (MST): PoW – scrypt;
- Masterdoge (MDOGE): PoS – scrypt;
- MasterMint (MM): PoW – x11;
- MasterMold (MOLD): PoS – scrypt;
- MasterTradercoin (MTR): PoS – x11;
- MastiffCoin (MAST): PoS – x11;
- MatrixCoin (MTX): PoW – SHA2-256;
- Mavro (MMM): PoW – SHA2-256;

- Maxcoin (MAX): PoS – SHA3-256;
- Mayancoin (MYNC): PoS – scrypt;
- Mazacoin (MZC): PoW – SHA2-256;
- Mazecoin (MAZE): PoW – x11;
- Mcoin (M): PoS – x15;
- MeatBallCoin (MBC): PoW – x11;
- Mediacoin (MDC): PoW – scrypt;
- Mediccoin (MDC): PoS – scrypt;
- Medicoin (MDC): pow-pos – scrypt;
- Mediterraneancoin (MED): PoW – scrypt;
- Megacoin (MEC): PoW – scrypt;
- Megastake (XMS): PoS – x11;
- Megcoin (MEG): PoW – scrypt-n-r;
- Melange (SPICE): PoW – Skein;
- Memecoin (MEM): PoW – scrypt;
- MemoryCoin (MMC): PoW – scrypt-n;
- Mental Health Awareness Coin (MHA): PoW – x11;
- Merelcoin (MEREL): PoW – scrypt;
- Metacoin (MET): PoW – quark;
- Metalcoin (MTT): PoW – x11;
- Metalcoin (METAL): PoS – x11;
- Metalcoin (MTC): PoW – scrypt;
- MetalMusiccoin (MMC): pow-pos – scrypt;
- Metiscoin (MTS): PoW – trisha;
- Metrocoin (MET): PoW – SHA2-256;
- MewnCoin (MEWN): PoS – x13;
- MgwBTC (MGWBTC): PoS – desconhecido;
- Microcash (MCR): PoW – scrypt;
- MicroCoin (MRC): PoS – scrypt-j;
- Microcoinarduino (GEO): PoW – SHA2-256;
- MidasCoin (MID): PoW – scrypt;
- Middle Earth Coin (MEA): PoW – SHA2-256;
- MiddleFingercoin (MDF): PoW – x11;
- Midnight (MDT): PoS – BMW;
- Milancoin (MLC): PoW – scrypt-j;
- MileyCyruscoin (MCC): PoW – scrypt;
- Millenniumcoin (MIL): PoS – x11;
- MillenniumCoin (MIL): PoS – x11;
- MillionaireCoin (MIL): PoS – x11;
- Mimiccoin (MMC): PoW – quark;
- Mincoin (MNC): PoW – scrypt;
- Mindcoin (MIND): PoW – x11;
- Minecoin (XMINE): PoW – scrypt;
- Minerals (MIN): PoS – x11;
- Minerscoin (MIC): PoW – x15;
- MinerTokens (MTK): PoW – scrypt-n;
- Mine-Treasure (MTG): PoS – myriad;
- Minicoin (MINI): PoW – quark;
- Mintcoin (MINT): PoS – scrypt;
- MiracleCoin (MCL): PoS – x13;

- Miscoin (MIS): PoW – x11;
- Mistcoin (MIC): PoS – nist5;
- M.Jcoin (MJ): PoS – scrypt;
- Mjollnircoin (MNR): PoW – hefty1;
- MLKCoin (MLK): PoW – scrypt;
- MMXIVcoin (MMXIV): PoW – SHA2-256;
- MMXVIcoin (MMXVI): PoW – salsarg;
- Mobcoin (MOB): PoS – x11;
- MobileCash (MBL): PoW – lyra2re;
- MöbiusCoin (MOBI): PoW – SHA2-256;
- MogliCoin (MOG): PoW – x11;
- MoinCoin (MOIN): PoS – SHA2-256;
- Molecule (MOL): PoW – quark;
- Mollycoin (TAB): PoS – scrypt;
- Monacoin (MONA): PoW – scrypt;
- Monero (XMR): PoW – cryptonight;
- Moneta (XMN): PoW – SHA2-256;
- Moneta (MONET): PoW – scrypt;
- Monetacoin (MNTA): PoS – SHA2-256;
- MonetaryUnitcoin (MUE): PoW – quark;
- MonetaVerde (MCN): PoW – cryptonight;
- Money ($$$): PoW – scrypt;
- Moneyenom (MYM): PoW – scrypt;
- Monkeycoin (MKY): PoW – quark;
- Monocle (MON): PoW – scrypt;
- MoonCoin (MOON): PoW – scrypt;
- Morpheus (MRP): PoW – x11;
- Mortgagecoin (MTG): PoW – scrypt;
- MotaCoin (MOTA): PoS – x13;
- MothManCoin (MOM): PoS – x15;
- MotoCoin (MOTO): PoW – novel;
- MountCoin (MNT): PoW – cryptonight;
- Mouse (MOC): PoS – x11;
- Mousecoin (MOSC): PoW – scrypt;
- Moviecoin (MVC): PoW – scrypt;
- Moxencoin (MOXN): PoW – SHA2-256;
- Mozzshare (MLS): PoW – hefty1;
- MtGoxCoin (GOX): PoW – scrypt;
- Mugatucoin (MUGA): PoS – x11;
- MultiCoin (MC): PoS – x11;
- MultiCoin (MUL): PoW – scrypt;
- MultiWalletCoin (MWC): PoS – x11;
- Muniti (MUN): PoW – x11;
- Munne (MNE): PoS – x13;
- Murica Coin (FREE): PoW – scrypt;
- Murraycoin (MRY): PoW – scrypt;
- Mushroomcoin (XMS): PoS – x14;
- MusicCoin (MIC): PoW – scrypt;
- Mustachecoin (MUST): PoW – scrypt;
- Mybrocoin (MBC): PoW – scrypt;

- Mycoin (MYC): PoW – scrypt;
- MyriadCoin (MYR): PoW – myriad;
- Mysterycoin (MYST): PoS – x11;
- Mysterycoin (MYST): PoW – SHA2-256;
- MysticCoin (MYSTIC): PoS – x11;
- N2coin (N2): PoS – nxt;
- N5coin (N5X): PoS – nist5;
- NaanaYaM (NYM): PoS – SHA2-256;
- NakamotoDark (NKT): PoS – x11;
- Namecoin (NMC): PoW – SHA2-256;
- Nanite (XNAN): PoS – x11;
- NANOcore (XNN): PoS – SHA2-256;
- Nanolite (NL): PoW – x11;
- Nanotoken (NAN): PoW – scrypt;
- NanyangTUcoin (NTU): PoS – x13;
- Napalcoin (NAC): PoW – x11;
- NasCoin (NAS): PoS – nxt;
- Naturecoin (NAT): PoW – x11;
- Nautiluscoin (NAUT): PoW – scrypt;
- Navajocoin (NAV): PoS – x13;
- NBCoin (NBC): PoS – SHA2-256;
- Nebuchadnezzar (NEBU): PoS – qubit;
- Nebulacoin (NEB): PoS – x11;
- Nectarcoin (SWEET): PoS – desconhecido;
- Negotium (NTM): PoW – scrypt;
- NEM (NEM): PoW – ellipticcurve;
- Neocoin (NEC): PoS – scrypt;
- NeoCortexCcoin (NEOC): PoW – NeoScrypt;
- Neoscoin (NEOS): PoW – myriad;
- Neptune (NEP): PoS – x11;
- Neptunium (NPT): PoW – cryptonight;
- Nerdycoin (NERDC): PoW – x11;
- Nerocoin (NERO): PoS – scrypt;
- Nest (NST): PoS – scrypt;
- Netbits (NBS): PoW – SHA2-256;
- Netcoin (NTC): PoW – scrypt;
- NetCoin (NET): PoW – scrypt;
- Netcoin2 (NET2): PoW – quark;
- Networkcoin (NETC): PoS – x13;
- Networkcoin (NWC): PoW – scrypt;
- NetworkDrafts (EDS): PoS – SHA2-256;
- Neucoin (NEU): PoW – SHA2-256;
- NeuroCoin (NRC): PoW – scrypt;
- Neutralitycoin (NTC): PoW – scrypt;
- Neutrinocoin (NTR): PoW – scrypt;
- Neutron (NTRN): PoW – SHA2-256;
- Neva (NEVA): PoS – BLAKE2s;
- Neverhoodcoin (NHC): PoS – x15;
- Newbiecoin (NEWB): PoS – SHA2-256;
- Newcoin (NEWC): PoS – x13;

- NewoCoin (NEWO): PoW – myriad;
- NewPiggycoin (PIGGY): PoS – x11;
- NewSpringCoin (NSC): PoS – x11;
- NewUniversalDollar (NUD): PoW – bcrypt;
- NewUniversalEurocoin (NUE): PoW – scrypt;
- NewWorldOrdercoin (NWO): PoS – x13;
- NewYorkCoin (NYC): PoW – scrypt;
- NextCoin (NXT): PoW – nxt;
- NeXTHorizon (NHZ): PoS – nxt;
- NeXTWorldBullion (NWB): PoS – nxt;
- Nexus (NXS): PoS – nist5;
- Nexuscoin (NXC): PoW – scrypt;
- NFDcoin (NFD): PoS – nxt;
- NhzKARM (NHZK): PoS – nxt;
- Nibble (NBL): PoW – scrypt;
- Nicecoin (NIC): PoS – x11;
- NiceCoin (NICE): PoW – scrypt;
- Nigeria Coin (NGC): PoW – Skein;
- Nightlife (NLF): PoS – x11;
- Nightmarecoin (NM): PoS – fresh;
- Nimbuscoin (NMB): PoS – x15;
- NineElevenTruthCoin (NTC): pow-pos – scrypt;
- Ninjacoin (NJA): PoW – x11;
- Ninjacoin (NINJA): PoS – SHA2-256;
- Ninja Doge (NDOGE): PoW – x11;
- Nintencoin (NINTEN): PoW – scrypt;
- Nitcoin (NIT): PoW – scrypt-j;
- NOAHcoin (NOAH): PoS – x13;
- NobleCoin (NOBL): PoS – scrypt;
- Nocoin (NO): PoW – x11;
- Nocturna (NOC): PoS – scrypt;
- NodeCoin (NODE): PoS – ellipticcurve;
- NodesForAll (NODES): PoS – x11;
- Nodex (NODEX): PoS – SHA2-256;
- NoFiatcoin (XNF): PoW – ripple;
- Noirbits (NRB): PoW – scrypt;
- Noirshares (NRS): PoS – momentum;
- NoNameCoin (NONC): PoW – x13;
- nOObcoin (NOOB): PoW – scrypt-j;
- Noocoin (NOO): PoS – x13;
- NoodlyAppendage (NDL): PoW – scrypt;
- NopeCoin (NOPE): pow-pos – x11;
- Norrencoin (XNC): PoW – scrypt;
- Nosferatu (NOS): PoW – scrypt;
- Nostrum (NOS): PoS – scrypt;
- Novacoin (NVC): PoS – scrypt;
- NovaCoinDark (NVCD): PoW – myriad;
- Novuscoin (NOVUS): PoW – scrypt;
- NPCCoin (NPC): PoS – SHA2-256;
- NRJcoin (NRJ): PoW – scrypt;

- NTXcoin (NTX): PoS – nxt;
- Nubiscoin (NUBIS): PoW – SHA2-256;
- NuBits (NBT): PoS – SHA2-256;
- Nuclearcoin (NCC): PoS – x13;
- Nucoin (NUC): PoS – scrypt;
- Nuggetcoin (NGT): PoS – x11;
- Nuggets (NUG): PoW – scrypt;
- Nukecoin (NUKE): PoS – qubit;
- Nukecoinz (NUKE): PoS – SHA2-256;
- Nullcoin (NULL): PoS – fresh;
- Numbercoin (NUMC): PoS – scrypt;
- NuShares (NUSH): PoS – SHA2-256;
- Nutcoin (NUT): PoW – scrypt;
- NXE (NXE): PoS – fresh;
- NxtMultigateway (MGW): PoS – nxt;
- Nxttycoin (NXTTY): PoS – SHA2-256;
- NyanCoin (NYAN): PoS – scrypt;
- O2oCoin (O2O): PoW – quark;
- Obamacoin (OBC): PoW – SHA3-256;
- Obscurebay (OBS): PoS – x11;
- Octane (OCTN): PoS – BLAKE2b;
- OctoCoin (888): PoW – scrypt;
- Ocultcoin (OCC): PoS – x13;
- Ocupycoin (OCUPY): PoS – x13;
- OddCoin (ODC): PoW – x13;
- OHLC (OHLC): pow-pos – x13;
- OhMyGod (OMG): PoS – x11;
- Oilcoin (OIL): PoW – scrypt;
- OilGasCoin (OGC): PoW – scrypt;
- OKCash (OK): PoS – scrypt;
- OldDogsNewTricks (ODNT): PoS – SHA2-256;
- OlympicCoin (OLY): PoW – scrypt;
- Omega (OMA): PoS – x14;
- Omnicoin (XOM): PoW – shanghai;
- OmniCoin (OMC): PoW – scrypt;
- Omnicore (OMNI): PoW – SHA2-256;
- OneCoin (ONC): PoW – scrypt-j;
- OneEvilCoin (OEC): PoW – cryptonight;
- OnelastCoin (OLC): PoW – scrypt;
- Onioncoin (ONI): PoW – scrypt;
- Online (ONE): PoW – SHA2-256;
- Onlinegamingcoin (OGC): PoW – scrypt;
- OnyxCoin (ONYX): PoS – x13;
- OnyxcoinV2 (ONYX2): PoS – x13;
- O_Ocoin (OO): PoS – x11;
- Opalcoin (OPAL): PoS – x13;
- OPEC Coin (OPC): PoS – x13;
- OpenSourcecoin (OSC): PoS – SHA2-256;
- Opescoin (OPES): PoW – salsarg;
- OptimumCoin (OPTI): PoS – x11;

- Optioncoin (OPTION): PoS – x11;
- OrangeCoin (OC): PoW – scrypt;
- Orbitcoin (ORB): PoS – scrypt;
- Orcacoin (ORCA): PoW – scrypt;
- OreoCoin (OREO): PoW – scrypt;
- Orgcoin (ORG): PoW – scrypt;
- Orient (ORT): PoW – scrypt;
- Origincoin (OGC): PoW – scrypt;
- Orioncoin (ORION): PoW – scrypt;
- Orlycoin (ORLY): PoS – x15;
- Orobit (ORO): PoW – SHA2-256;
- OrthoCoin (ORTHO): PoS – x13;
- Oseturacoin (OSE): PoS – scrypt;
- OSIcoin (OSI): PoW – scrypt;
- Osmiumcoin (OS76): PoW – scrypt;
- Osmosis (OSMO): PoW – scrypt;
- Ottomancoin (OTC): PoS – x13;
- Ourcoin (ORC): PoW – x11;
- Overly Attached Coin (OAC): PoW – SHA3-256;
- Overseas Chinese coin (OCC): PoW – scrypt;
- OverTimecoin (OT): PoS – x15;
- OverUnitycoin (OVU): PoW – scrypt;
- Oxcoin (OXC): PoW – quark;
- Oxen (OXN): PoW – BLAKE2s;
- Ozcoin (OZC): PoW – x11;
- P7Coin (P7C): PoW – scrypt;
- Paccoin (PAC): PoS – SHA2-256;
- PaiMaiBi (PMB): pow-pos – scrypt;
- Pakcoin (PAK): PoS – scrypt;
- Paladincoin (PLD): PoW – cryptonight;
- PALCoin (PALC): PoW – SHA3-256;
- Palestinecoin (PAL): PoS – x11;
- Pandacoin (PAND): PoS – scrypt;
- Pandacoin (PND): PoW – scrypt;
- Pangu (PGC): PoW – scrypt;
- ParallaxCoin (PLX): PoW – scrypt-n;
- Parallelcoin (DUO): PoW – SHA2-256;
- Paranoiacoin (PAC): PoW – scrypt;
- ParkByte (PKB): PoS – SHA2-256;
- Parlings (PLG): PoW – SHA3-256;
- Particle (PRT): PoW – quark;
- Partycoin (PARTY): PoW – scrypt;
- Passioncoin (PON): PoW – x11;
- Pastacoin (PAS): PoW – scrypt;
- PathFinder (XPH): PoS – x11;
- PatriotCoin (USA): PoW – scrypt;
- Pawncoin (PAWN): PoW – scrypt;
- Paycoin (XPY): pow-pos – SHA2-256;
- Paycoin (PYC): PoW – scrypt;
- PayCon (CON): PoS – x13;

- Paypalcoin (PPC): PoW – scrypt;
- PayPeer (PAYP): PoW – x11;
- Payprocoin (PRO): PoW – SHA2-256;
- Payzorcoin (PZR): PoS – scrypt;
- PeaceCoin (PEC): PoW – scrypt;
- Pebblecoin (XPB): PoW – cryptonight;
- Peercoin (PPC): PoS – SHA2-256;
- PeercoinDark (PPCD): PoW – SHA2-256;
- Peerpay (PP): PoS – x11;
- Pegasuscoin (PEG): PoW – scrypt;
- Pelecoin (PELE): PoW – novel;
- Pencilcoin (PENCL): PoS – x13;
- PENCoin (PEN): PoS – scrypt;
- Penguincoin (PENG): PoW – scrypt;
- Pennies (CENT): PoS – scrypt-j;
- PennyPincher (XPP): PoS – scrypt;
- Pentacoin (PTA): PoS – SHA2-256;
- Pentaquark (LHC): PoW – SHA2-256;
- Peonycredit (PNC): PoW – myriad;
- Peoplecoin (PC): PoW – scrypt;
- PeopleCoin (PPL): PoW – scrypt;
- Peoplescurrency (PPL): PoW – x17;
- Pepecoin (PEP): PoW – scrypt;
- Pepecoin (PEPE): PoS – x11;
- Pepecoin (PEPE): PoS – x11;
- Peppsycoin (PSY): PoW – scrypt;
- Perfectcoin (PERFECT): PoW – x15;
- Perfectcoin (PERC): PoW – scrypt-n;
- Pesacoin (PES): PoS – x13;
- Pesetacoin (PTC): PoW – scrypt;
- PetroDollar (XPD): PoW – SHA2-256;
- Phalanx (PLX): PoW – SHA2-256;
- Pharma (XPH): PoS – x11;
- PHCoin (PHC): PoW – x11;
- Phenixcoin (PXC): PoW – scrypt;
- Phicoin (PHI): PoW – scrypt;
- PhilosopherStone (PHS): PoS – scrypt;
- Phoenixcoin (PXC): PoW – scrypt;
- Phonecoin (TEL): PoW – scrypt;
- Phooeycoin (HKP): PoS – x11;
- Photon (PHO): PoW – BLAKE;
- Photoncoin (PHO): PoW – quark;
- PHPcoin (PHP): PoS – scrypt;
- Phreakcoin (PHR): PoS – x11;
- Picoin (PCN): PoW – scrypt;
- PIcoin (PI): PoW – SHA2-256;
- Pigcoin (PIG): PoW – scrypt;
- Piggycoin (PIGGY): PoW – scrypt;
- Pikachu Coin (PIKACHU): PoW – scrypt;
- Pikacoin (PIKA): PoW – scrypt;

- Pimpcash (PIMP): PoS – scrypt;
- Pingas (PINGAS): PoW – scrypt-j;
- Piniumcoin (PCN): PoW – scrypt;
- PinkCoin (PINK): PoS – x11;
- PinkDiamond (PDC): PoS – x11;
- Pioneercoin (PER): PoW – x13;
- Pipshares (PIP): PoS – scrypt;
- Piratecoin (PC): PoS – scrypt;
- PirateCoin (PTE): PoW – SHA2-256;
- PirateCoin (PIR): PoW – scrypt;
- Pixcoin (PIX): PoW – scrypt;
- Pixxcoin (PIXX): PoS – scrypt;
- PizzaCoin (PIC): PoW – scrypt;
- PKRCoin (PKR): PoW – scrypt;
- Planecoin (AERO): PoW – scrypt;
- Planetcoin (PLANET): PoS – scrypt;
- Planetdollarcoin (PDR): PoW – scrypt-n;
- Plankton (FOOD): PoS – x13;
- Platinum (PTL): PoW – scrypt;
- Platinumcoin (PT): PoW – SHA2-256;
- PlatinumCoin (PNC): PoW – SHA2-256;
- Platinumtoken (PTKC): PoW – SHA2-256;
- Platonic (XPL): PoS – scrypt;
- PlayToken (PLT): PoW – scrypt;
- Plebeiancoin (PLEB): PoS – x13;
- Pleiadescoin (LEIA): PoW – SHA2-256;
- PLNcoin (PLNC): PoW – scrypt;
- PlusEVcoin (PEV): PoW – scrypt;
- Plutoniumcoin (RODS): PoS – x13;
- pNut (FTW): PoW – primechain;
- Podcoin (PDC): PoW – SHA2-256;
- Poison (PSN): PoS – x11;
- Poitin Coin (PTN): PoS – x11;
- Poker Chips (CPC): PoS – x11;
- Pokercoin (POK): PoW – scrypt;
- Polcoin (PLC): PoW – SHA2-256;
- PolishCoin (PCC): PoW – scrypt;
- PolishSexIndustry (PSI): PoS – x11;
- Polybit (POLY): PoW – scrypt;
- Ponycoin (PONY): PoW – SHA2-256;
- Ponycoin (PNC): PoW – scrypt;
- PoolStamp (XSP): PoW – x13;
- Poopcoin (POO): PoS – x11;
- POOSCoin (POOS): PoS – x13;
- Populacecoin (POC): PoW – quark;
- Popularcoin (POP): PoW – scrypt;
- PorkCoin (XPC): PoS – x11;
- Porncoin (PNC): PoW – scrypt;
- Portcoin (PORT): PoS – x13;
- POScoin (POS): PoS – x15;

- Posdigy (PDY): PoS – x13;
- PosEffectcoin (POSE): PoW – x13;
- Positron (TRON): PoW – SHA2-256;
- Potatocoin (SPUD): PoW – scrypt;
- PotCoin (POT): PoS – scrypt;
- Poundcoin (PND): PoW – scrypt;
- Poundkoin (PUK): PoW – SHA2-256;
- POWcoin (POW): PoS – scrypt;
- Powercoin (POW): PoW – scrypt;
- Powercoin (PWC): PoW – scrypt;
- Praisedong (PD): PoW – scrypt;
- Praycoin (JOSH): PoS – SHA2-256;
- Predatorcoin (PRDT): PoW – scrypt;
- Preiscoin (PRS): PoW – scrypt;
- Preminecoin (PMC): PoW – SHA2-256;
- PreminePlus (PMP): PoS – scrypt;
- Premium (PRE): PoW – scrypt;
- PresidentCoin (PSD): PoW – scrypt;
- PrimeChain (PRIME): PoS – SHA2-256;
- Primecoin (XPM): PoW – primechain;
- Prime-xicoin (PXI): PoW – x11;
- Primio (PRIMIO): PoW – JH;
- Prismacoin (PRISMA): PoS – x13;
- PRO (PRO): PoW – x15;
- Probe (PROBE): PoW – quark;
- Procoin (PCN): PoW – scrypt;
- Procomcoin (PCM): PoW – scrypt;
- Profitcoin (PRT): PoW – x11;
- ProfitCoin (PFC): PoS – x13;
- ProgressCoin (PSSC): PoS – x11;
- Prometheuscoin (PMC): PoS – x13;
- Prospercoin (PRC): PoW – scrypt;
- Proton (PRTO): PoS – scrypt;
- ProtoShares (PTS): PoW – momsha;
- Prototanium (PR): PoW – SHA2-256;
- Prototypecoin (PTY): PoS – x11;
- Prozcoin (PROZ): pow-pos – SHA2-256;
- PseudoCash (PSEUD): PoS – x13;
- Psilocybin (PSY): PoS – SHA2-256;
- Pugcoin (PUG): PoW – scrypt-n;
- Pulsar (PULSE): PoS – SHA2-256;
- Pulsarcoin (PSC): PoS – scrypt;
- PumpnDumpCoin (PND): PoW – scrypt;
- PunisherCoin (P666): PoW – scrypt;
- Purecoin (PURE): PoS – x11;
- PurePOS (POS): PoS – x11;
- Purplecoin (PC): PoS – scrypt;
- Pwnycoin (PWNY): PoW – SHA2-256;
- Pxlcoin (PXL): PoW – scrypt;
- PyongyangCoin (XPG): PoW – SHA2-256;

- Pyramids (PYRA): PoS – x11;
- Pythoncoin (PYBC): PoW – novel;
- Qcoin (QTC): PoS – scrypt;
- Qcoin (QTC): PoW – scrypt;
- Qibuckcoin (QBK): PoS – x13;
- QiwiCoin (QWC): PoS – x11;
- QixCoin (XQC): PoW – desconhecido;
- Qora (QORA): PoS – SHA2-256;
- QPScoin (QPS): PoW – x13;
- QQCoin (QQC): PoW – scrypt-j;
- Quantradilbry (Q1): PoW – scrypt;
- Quantum (QTM): PoS – scrypt;
- Quantum2 (QTM2): PoS – x13;
- Quantumcoin (QTC): PoW – scrypt;
- QuarkBar (QB): PoW – quark;
- QuarkCoin (QRK): PoW – quark;
- Quartz (QTZ): PoS – SHA2-256;
- Quatloo (QTL): PoW – scrypt;
- QuazarCoin (QCN): PoW – cryptonight;
- QubitCoin (Q2C): PoW – qubit;
- Québecoin (QBC): PoW – x11;
- Quedos (QDOS): PoW – x11;
- QuibitSphere (QBS): PoS – x11;
- Quickcoin (QWC): PoW – scrypt;
- Quicksilver (QSLV): PoS – x15;
- QuidCoin (QUID): PoS – x11;
- QuietCoin (SHH): PoS – x13;
- QuitDough (QUIT): PoS – x13;
- Quotient (XQN): PoS – scrypt;
- R3D (R3D): PoS – scrypt;
- RabbitCoin (RBBT): PoW – scrypt;
- Racecoin (RACE): PoS – x11;
- Radioactivecoin (RAD): PoW – scrypt-j;
- Radioshares (RDSH): PoW – scrypt-n;
- Radium (RADS): PoW – scrypt;
- Radix (RADIX): PoW – radix;
- Rainbowcoin (LGBT): PoW – SHA2-256;
- RainbowGoldCoin (RAIN): PoW – scrypt;
- Raincoin (RAIN): PoS – scrypt;
- Rambo coin (RBC): PoW – scrypt;
- Randomcoin (RND): PoW – x11;
- Randomquark (RQC): PoW – quark;
- RandPaulCoin (RPCD): dpos – momentum;
- Rapecoin (RAP): PoW – scrypt-n;
- RapidCoin (RPD): PoS – scrypt;
- Rastacoin (RTC): PoW – scrypt;
- Ratcoin (RATC): PoS – x11;
- Ratecoin (XRA): PoS – x11;
- Ratio (RATIO): PoS – x11;
- Raven (RVN): PoS – scrypt;

- Rawcoin (RAW): pow-pos – x15;
- Razor (RZR): PoW – BLAKE;
- RealCoin (REC): PoW – scrypt;
- Realpay (RPC): PoW – realpay;
- RealStackCoin (RSC): PoW – scrypt;
- Rebirthcoin (REB): PoW – SHA2-256;
- Recyclingcoin (REX): PoW – scrypt;
- RedCoin (RED): PoW – scrypt;
- Reddcoin (RDD): PoS – scrypt;
- Redditcoin (RDC): PoW – scrypt;
- RedDragonCoin (RDDC): PoS – x11;
- RedeemCoin (REM): PoS – scrypt;
- Redkoin (RKN): PoS – desconhecido;
- RedOakCoin (ROC): PoW – scrypt;
- RedWind (RD): PoW – cryptonight;
- Redwire (RW): PoS – x11;
- Refrigerator (FRIDGE): PoS – x15;
- RefrigeratorCoin (FRIDGE): PoS – x15;
- Reikicoin (RKC): PoS – SHA2-256;
- Rekt (REKT): PoS – scrypt;
- RenascenceCoin (RNC): PoS – SHA2-256;
- RepublicCoin (RC): PoW – SHA2-256;
- Republicoin (REP): PoS – x11;
- Republicoin (REP): PoW – quark;
- Rescuecoin (RSCC): PoW – scrypt;
- Reserved (RES): PoW – scrypt;
- ReserveShare (RSU): por – nxt;
- ResumeoShares (RMS): PoS – nist5;
- Retrocoin83 (R83): PoW – scrypt;
- Returncoin (RNC): PoS – x11;
- Revenu (REV): PoS – scrypt;
- RevoCoin (RVC): PoW – x15;
- RevolutionCoin (CHE): PoW – scrypt;
- Rewardcoin (RDC): PoW – momentum;
- RhinoCoin (XRC): PoS – scrypt;
- Rhinohorncoin (ROH): PoW – scrypt-n;
- Rhodiumcoin (RHO): PoW – scrypt;
- Ribbitrewards (RBR): PoW – SHA2-256;
- RiceCoin (RICE): PoS – x13;
- Richcoin (RCH): PoW – scrypt;
- Richcoin (RICHX): PoW – myriad;
- Riecoin (RIC): PoW – primeconstellation;
- Rightcoin (RTC): PoS – x11;
- Rimbit (RBT): PoS – scrypt;
- Ringo (RIN): PoS – scrypt;
- Riotcoin (RIOT): PoS – x13;
- Ripoffcoin (RIPO): PoS – scrypt;
- Ripple (XRP): PoW – ripple;
- RippleLite (XPL): PoS – scrypt;
- Riskcoin (RISK): PoS – scrypt;

- RivrCoin (RIVR): PoS – x13;
- RobotSexNickelscoin (RSN): PoW – scrypt;
- Rockcoin (RCK): PoW – x11;
- Rocket (RKT): PoW – scrypt;
- RocketCoin (ROC): PoW – scrypt;
- Romancoin (ROM): PoS – x11;
- RonBurgundyCoin (RBC): PoW – SHA2-256;
- RonPaulCoin (RPC): PoW – scrypt;
- Rootcoin (ROOT): PoS – scrypt;
- Roscoin (ROS): PoS – x11;
- Rosecoin (ROSE): PoW – scrypt;
- Roseonlycoin (RSC): PoW – x11;
- RossUlbrichtCoin (XRU): PoW – x11;
- Rotocoin (RT2): PoW – scrypt-n;
- Roulettecoin (RLT): PoW – roulette;
- ROXcoin (ROX): PoS – x11;
- RoyalCoin (RYC): PoW – scrypt;
- Rubberduckie (RBC): PoW – scrypt;
- Rubies (RBIES): PoS – scrypt;
- RubleBit (RUBIT): PoW – scrypt;
- Rublecoin (RU): PoS – x15;
- Rubycoin (RBY): PoW – scrypt;
- RuCoin (RUC): PoW – SHA2-256;
- Rumorscoin (RUM): PoS – x11;
- RupayaCoin (RUP): PoW – scrypt;
- Russiacoin (RC): PoS – scrypt;
- RVDCoin (RVD): PoW – quark;
- Safecoin (SAFE): por – SHA2-256;
- Saffroncoin (SFR): PoW – scrypt;
- Sailboatcoin (SBC): PoS – x15;
- SaintPatrickCoin (STP): PoW – scrypt;
- Sakuracoin (SKR): PoW – scrypt;
- Salus (SLS): PoS – SHA2-256;
- Sambacoin (SMB): PoW – scrypt;
- Samsaracoin (SMSR): PoW – qubit;
- Samurai (RONIN): PoS – qubit;
- Sapience (XAI): PoW – scrypt;
- Sapienta (SAP): PoW – x11;
- Sapphirecoin (SPH): PoW – scrypt;
- Sativacoin (STV): PoS – x13;
- Satoshifun (HIFUN): PoS – scrypt;
- Satoshimadness (MAD): PoS – x11;
- Saturn2coin (SAT2): PoS – scrypt;
- Saturncoin (SAT): PoW – scrypt;
- SauronRings (SAU): PoW – scrypt;
- Savecoin (SPC): PoW – SHA2-256;
- SavingCoin (SAV): PoW – scrypt;
- Sayacoin (SYC): PoW – SHA2-256;
- Scamcoin (SCAM): PoS – x13;
- ScarceCoin (SEC): PoW – scrypt;

- Scarfacecoin (SFC): PoW – scrypt;
- Scattercoin (STC): PoS – x11;
- SCitW (SCITW): PoS – x13;
- sCoin (SCO): PoW – scrypt;
- Scotcoin (SCOT): PoW – SHA2-256;
- Scrasic (SCR): PoW – SHA3-256;
- Scrolls (SCQ): PoW – scrypt;
- SDFcoin (SDF): PoW – SHA2-256;
- Sealandcoin (SEA): PoW – scrypt;
- Secondscoin (SEC): PoW – quark;
- Secretcoin (SCRT): PoS – x11;
- SecretsCoin (SCC): PoS – scrypt;
- Sectorcoin (SECT): PoW – x15;
- SecureCoin (SRC): PoW – quark;
- Securitysyscoin (SCSY): PoW – hefty1;
- Seedbit (SED): PoS – quark;
- Seedcoin (SEED): PoS – scrypt;
- Seedcoin (SDC): PoW – scrypt;
- SeedShares (SEEDS): PoS – SHA2-256;
- Selfiecoin (SLF): PoS – x13;
- Selfiecoin (SLFI): PoS – scrypt;
- SembroToken (SMBR): PoS – scrypt;
- Sendcoin (SEND): PoS – scrypt;
- Sentaro (SEN): PoS – scrypt;
- Serracoin (SRR): PoW – scrypt;
- ServX (XSX): PoW – scrypt;
- Sesame (SEED): PoW – scrypt;
- Sevencoin (SEVEN): PoW – scrypt;
- Sexcoin (SXC): PoW – scrypt;
- Sha1coin (SHA): PoW – SHA1-256;
- SHAcoin (SHA): PoS – SHA2-256;
- Shadecoin (SHADE): PoS – scrypt;
- ShadowCash (SDC): PoS – scrypt;
- Shadowcoin (SDC): PoS – nxt;
- Shapes (SPS): pow-pos – x15;
- Sharecoin (SHARE): PoS – myriad;
- Sharkcoin (SAK): PoW – quark;
- sharkfund0 (SF0): PoS – nxt;
- Sheckel (SKS): PoS – scrypt;
- Shekelcoin (SHE): PoW – SHA2-256;
- ShellCoin (SHELL): PoS – x11;
- Sherlockcoin (SHC): PoW – scrypt;
- ShibeCoin (SHIBE): PoS – scrypt;
- Shieldcoin (SHLD): PoS – x15;
- Shift (SHF): PoW – Dagger;
- Shillingcoin (SHI): PoW – SHA2-256;
- ShinyCoin (SHC): PoS – scrypt-n-r;
- Shirecoin (SCN): PoW – scrypt;
- Shitcoin (PTE): PoW – SHA2-256;
- SHITCoin (SHT): PoS – SHA2-256;

- ShitsandGiggles (SANDG): PoW – SHA2-256;
- Shoecoin (SHOE): PoW – x15;
- ShopCoin (SHOP): PoW – scrypt;
- ShopX (SHOPX): PoS – x13;
- Shrooms (SHRM): PoW – SHA2-256;
- Siacoin (SIA): PoW – BLAKE2b;
- Siamesecoin (SIS): PoS – x11;
- Sibcoin (SIB): PoW – x11gost;
- Sifcoin (SIC): PoW – nist6;
- Signaturecoin (SIGN): PoS – x11;
- SiliconValleyCoin (XSV): PoW – scrypt-n;
- Silkcoin (SC): PoS – scrypt;
- SilverBack (SBK): PoW – cryptonight;
- SilverBullet (SVB): PoS – x13;
- Simicoin (SIMI): PoW – scrypt;
- Sinecoin (SINE): PoW – scrypt-n;
- Singularcoin (SIN): PoS – scrypt;
- Singularity (SING): PoW – myriad;
- Siriuscoin (SSC): PoW – SHA2-256;
- SixAxis (SIX): PoS – x11;
- SJWcoin (SJW): PoW – scrypt;
- Skeincoin (SKC): PoW – Skein;
- SkullBuzz (SKB): PoS – SHA2-256;
- SkullCoin (SKULL): PoW – SHA2-256;
- Skycoin (SKY): PoW – Obelisk;
- SkyCoin (SYC): PoW – scrypt;
- Skynetcoin (SNET): PoS – x11;
- Slatecoin (SLATE): PoW – x11;
- Sleakcoin (SLK): PoW – scrypt;
- Slenderman (SMX): PoW – scrypt;
- Sletcoin (SLC): PoW – x11;
- Slimcoin (SLM): pob – dcrypt;
- Sling (SLING): PoS – SHA2-256;
- Slothcoin (SLOTH): PoW – SHA3-256;
- SMACoin (SMAC): PoS – x11;
- SmallChange (SMC): PoW – scrypt;
- Smartchips (SC): PoS – SHA2-256;
- SmartCoin (SMC): PoS – scrypt;
- SmartCoinv2 (SMC2): PoW – x11;
- Smileycoin (SMLY): pow-pos – scrypt;
- Smurfs coin (SMURF): PoS – scrypt;
- Snakecoin (SNAKE): PoW – scrypt-n;
- SnakeXcoin (SNCX): PoS – x13;
- Snapcoin (SNP): PoW – scrypt;
- Snowballs (BALLS): PoS – SHA2-256;
- Snowcoin (SNC): PoS – SHA2-256;
- Sobercoin (SOBER): PoW – scrypt;
- Soccercoin (SCC): PoW – scrypt;
- Soccercoin (SCC): PoS – scrypt;
- Sochicoin (SOCHI): PoW – scrypt;

- SocialCoin (SOC): PoW – scrypt;
- SocialKrypt (SOKRY): PoS – x13;
- Social media coin (SMAC): PoS – scrypt;
- SocialNetworkcoin (SNC): PoS – scrypt;
- SocialxBot (XBOT): PoS – scrypt;
- Softwarecoin (SOFT): PoW – scrypt;
- Soilcoin (SOIL): PoW – Dagger;
- Solace (SOLIS): PoW – cryptonight;
- Solarcoin (SLR): PoW – scrypt;
- Solcoin (SOL): PoW – scrypt;
- Solecoin (SOLE): pow-pos – x14;
- SolemnFuel (SOF): PoW – scrypt-n;
- SolemnShares (SOLEMN): PoS – scrypt-n;
- SolidCoin (SC): PoW – SHA2-256;
- SolidCoin2 (SC2): PoW – SHA2-256;
- Solocoin (SOLO): PoS – scrypt;
- Somacoin (SOMA): PoW – quark;
- Sonacoin (SNC): PoW – scrypt;
- Soncoin (SON): PoW – scrypt;
- SongCoin (SNG): PoW – scrypt;
- SonicScrewdrivercoin (SSD): PoS – SHA2-256;
- Sooncoin (SOON): PoW – SHA2-256;
- Soundbit (SND): PoW – x15;
- Soundcoin (SND): PoW – scrypt;
- Sourcecoin (SRC): PoS – scrypt;
- Sovereign (SOV): PoW – SHA2-256;
- Sovereigncoin (SOV): PoS – SHA2-256;
- Sovereigncoin (SVC): PoW – scrypt;
- Spacebucks (SBX): PoW – BLAKE;
- Spacecoin (SPACE): PoW – scrypt;
- Spacecredit (SPC): PoS – salsarg;
- SpainCoin (SPA): PoW – scrypt-n;
- Spamslayer (XSSX): PoS – x11;
- Spark (SPARK): PoS – x11;
- Spartacuscoin (SPATA): PoS – x15;
- Spartancoin (SPN): PoW – scrypt;
- Spec (SPEC): PoW – scrypt;
- SpecialCoin (SPE): pow-pos – x11;
- Specie (SPX): PoW – scrypt;
- Spectrumcoin (SPEC): PoW – myriad;
- Speedcoin (SPD): PoW – scrypt;
- SpeedCoin (SPC): PoW – SHA2-256;
- Sphere (SPH): PoW – scrypt;
- SpikesPrivateCoin (SPC): PoS – SHA2-256;
- SpinCoin (SPC): PoW – nist5;
- Spirecoin (SPIRE): PoW – scrypt;
- Spktr (SPKTR): PoS – SHA2-256;
- Spliffcoin (SPL): PoS – x11;
- Spoderman (SDM): PoW – scrypt;
- Sportcoin (SPCC): PoS – x11;

- Spots (SPOT): PoW – scrypt;
- Spots (SPT): PoW – scrypt;
- SpreadCoin (SPR): PoW – x11;
- Sprouts (SPRT): PoS – SHA2-256;
- SproutsExtreme (SPEX): PoS – SHA2-256;
- Spurdocoin (SPUR): PoW – x11;
- SquallCoin (SQL): PoS – x11;
- Square (SQ): PoW – scrypt;
- Squarebit (SBIT): PoS – x11;
- Squarerootcoin (ROOT): PoW – SHA2-256;
- SSVcoin (SSV): PoW – x13;
- Stabilityshares (XSS): PoW – scrypt;
- StabilityShares (XSI): PoS – scrypt;
- Stable (STAB): PoS – x15;
- StableCoin (SBC): PoW – scrypt;
- Stackcoin (STACK): PoW – scrypt;
- Stackedcoin (STKC): PoW – SHA2-256;
- Stacycoin (STCY): PoW – x11;
- Stag (STAG): PoS – nxt;
- StakeCoin (STK): PoS – scrypt;
- Stakerush (STHR): PoS – desconhecido;
- Stalwartbucks (SBX): PoW – scrypt;
- StandardCoin (STD): PoW – scrypt;
- StarBucks (STB): PoW – scrypt;
- StarbucksCoin (SUC): PoW – x11;
- Starcoin (STR): PoS – scrypt;
- StarCoin (STC): PoW – x11;
- Starkcoin (STK): PoW – stark;
- Starlightcoin (SLT): PoW – quark;
- Startcoin (START): PoW – scrypt;
- StashCoin (STA): PoW – SHA2-256;
- StealthCash (STX): PoS – scrypt;
- Stealthcoin (STH): PoW – x11;
- Stealthcoin (XST): PoW – x13;
- Stellar (STR): PoS – SHA2-256;
- Stemcoin (STEM): PoS – x15;
- Steps (STEPS): PoS – scrypt;
- Sterlingcoin (SLG): PoS – x13;
- Steroids (STOID): PoS – x13;
- Stlcoin (STL): PoW – SHA2-256;
- StockCoin (STC): PoW – scrypt;
- StoopidCoin (STP): PoW – scrypt;
- StopLosscoin (XSL): PoS – x11;
- Stories (STY): PoW – SHA2-256;
- Storjcoin X (SJCX): PoS – SHA2-256;
- Stormcoin (STC): PoW – scrypt;
- Streamcoin (STC): PoW – scrypt;
- Stress (STS): PoS – x13;
- Stripecoin (STRP): PoW – scrypt;
- StrongHands (SHND): PoW – SHA2-256;

- Suarezcoin (SRZ): PoW – x11;
- SuckCoin (SUC): PoW – scrypt;
- SUMcoin (SUM): PoS – x11;
- SummerCoin (SUM2): PoS – x13;
- SummerCoin (SUM): PoS – x11;
- Summitcoin (XMT): PoS – scrypt;
- Suncoin (SUN): PoW – scrypt;
- Sunflowercoin (SFC): PoS – scrypt;
- Sunnysideupcoin (SSU): PoW – scrypt;
- SunRiseCoin (SRC): PoW – scrypt;
- Supcoin (SUP): PoW – pluck-128;
- Supercoin (SUPER): PoS – x11;
- Supercoin (SPR): PoW – SHA2-256;
- SuperCoin (SPC): PoW – scrypt;
- SuperFastPOWsCrypt (SFPC): PoW – scrypt;
- Superherocoin (SHC): PoW – scrypt;
- Superiorcoin (SUPR): PoW – scrypt;
- SuperNET (TOKEN): PoS – nxt;
- SuperRandom (SRND): PoS – x11;
- SuperTurbostake (STRB): PoS – SHA2-256;
- SupplyShock (M1): PoS – x13;
- Surge Coin (SRG): PoW – scrypt;
- Survivorcoin (SVR): PoW – x11;
- Sutercoin (SUTC): PoW – scrypt;
- Swagbucks (BUCKS): PoW – scrypt;
- Swagcoin (SWAG): PoW – scrypt;
- SwansonCoin (RON): PoW – scrypt;
- Swarm (SWARM): PoS – SHA2-256;
- SweetStake (SWEET): PoS – x11;
- Swingcoin (SWING): PoS – SHA2-256;
- Swisscoin (SWC): PoS – x11;
- Switch Coin (SWITCH): PoW – scrypt;
- Switzerlandcoin (SWC): PoW – scrypt;
- Sydpakcoin (SDP): PoS – x13;
- Synapse (XSY): PoW – x11;
- Sync (SYNC): PoS – x11;
- SynCoin (SYN): PoW – scrypt;
- Synergy (SNRG): PoS – x11;
- SysCoin (SYS): PoW – scrypt;
- TacoCoin (TCO): PoW – scrypt;
- TagCoin (TAG): PoS – scrypt;
- Takeicoin (TAK): PoW – SHA2-256;
- Takeoutcoin (TOC): PoW – scrypt;
- Talkcoin (TAC): PoS – nist5;
- Tamaguccicoin (TAM): PoS – scrypt;
- Tanzanitecoin (TNZ): PoS – x11;
- TaoJingCoin (TJC): PoW – ocean;
- Tattoocoin (INK): PoW – scrypt;
- Tavos (XTV): PoW – cryptonight;
- Taxcoin (TXC): PoS – scrypt;

- Taxicoin (TAXI): PoW – scrypt;
- TaxiTokens (HACK): PoW – scrypt;
- Teacoin (TEA): PoS – SHA2-256;
- Techcoin (TECH): PoS – x13;
- Tecoin (TEC): PoW – hefty1;
- Teddycoin (TDY): PoS – x13;
- TeeleeCoin (TLEE): PoS – desconhecido;
- TEKcoin (TEK): PoS – SHA2-256;
- TeleBET (TB): PoW – scrypt;
- Templecoin (TPC): PoW – scrypt;
- Tenebrix (TBX): PoW – scrypt;
- TenFive Coin (10-5): PoW – scrypt-n;
- TenneT (TENNET): PoS – SHA2-256;
- TerraCoin (TRC): PoW – SHA2-256;
- TeslaCoin (TES): PoS – scrypt;
- Teslax3coin (TESLA): PoW – scrypt;
- Testcoin (TC): PoS – x11;
- Tetcoin (TET): PoW – scrypt;
- TexasCoin (TEX): PoW – x11;
- THcoin (TH): PoS – x11;
- TheballCoin (TBC): PoS – x13;
- Thebotcoin (TBN): PoW – scrypt;
- Thecoin (THC): PoW – scrypt;
- TheCoin (THE): PoW – scrypt;
- TheLastCoin (TLC): PoW – x15;
- Theoremcoin (THEO): PoS – x11;
- ThePandacoin (PANDA): PoW – scrypt-n;
- TheWeathercoin (TWC): PoW – scrypt;
- Thinkandgrowrich (TAGR): PoW – x15;
- ThinkTwice (TTC): PoW – scrypt;
- ThirdGenerationCoin (TGC): pob – dcrypt;
- Thorcoin (THOR): PoS – scrypt-j;
- ThunderStake (THUNDER): PoS – x11;
- Tianhe (TIA): PoW – lyra2re;
- Tianlongcoin (TLC): PoW – scrypt;
- Ticinocoin (TIC): PoW – SHA2-256;
- Tickcoin (TICK): PoW – x11;
- Ticketcoin (TKT): PoS – x11;
- Tigercoin (TGC): PoW – SHA2-256;
- TileCoin (XTC): PoS – SHA2-256;
- Time (TIME): PoW – SHA2-256;
- Timecoin (TMC): PoW – scrypt;
- Timekoin (TK): PoW – SHA2-256;
- Tincoin (TIN): PoW – scrypt;
- Tiplecoin (TPL): PoS – desconhecido;
- TippingRocks (TPRS): PoS – x15;
- Titanium (TTN): PoW – scrypt;
- Titcoin (TIT): PoW – SHA2-256;
- Tittiecoin (TTC): PoW – scrypt;
- Tjcoin (TJC): PoW – trisha;

- Tlascoin (TLS): PoW – Twister;
- Tokyocoin (TC): PoW – x11;
- Tomato (TOC): PoS – scrypt;
- Tomatocoin (TMC): PoW – x12;
- Tomatocoin (TMT): PoW – x11;
- TongYongCoin (TYC): PoW – quark;
- Toothfairycoin (TFC): PoS – x15;
- TopCoin (TOP): PoS – scrypt;
- Topcoin2 (TOP): PoS – scrypt;
- Torcoin (TOR): PoS – x11;
- Tornadocoin (TORN): PoS – x13;
- Torrentcoin (TC): PoW – x13;
- Torrentcoin (TCX): PoS – x11;
- TotalCoin (TOT): PoS – scrypt;
- Touchcoin (TOUCH): PoS – x11;
- Tournamentcoin (TC): PoW – SHA2-256;
- Tr011coin (TCN): PoW – scrypt;
- TradeCoin (TDC): PoW – scrypt;
- Tradercoin (TDC): PoW – scrypt;
- TraderCoin (TRDR): PoW – scrypt;
- Trafficcoin (TRFC): PoS – x15;
- TrailerParkCoin (TPC): PoS – scrypt;
- Traincoin (XTN): PoW – scrypt;
- Transactcoin (TXC): PoW – scrypt;
- Transactioncoin (TXC): PoW – myriad;
- Transcoin (TRN): PoW – scrypt;
- Transfercoin (TFC): PoW – scrypt-n;
- Transfercoin (TX): PoS – x11;
- Transformerscoin (TRANSF): PoW – qubit;
- Transitcoin (TNT): PoS – SHA2-256;
- TranslationCoin (TRLA): PoS – x11;
- Trash&Burn (TXB): PoS – SHA2-256;
- Travelcoin (TAC): PoW – scrypt;
- Travelcoin (TRV): PoS – x11;
- TreasureHuntCoin (BOOTY): PoS – x11;
- TrickyCoin (TRICK): PoS – x11;
- TrickyDickyFunBill (TDFB): PoS – SHA2-256;
- Tricoin (TRI): PoS – x11;
- Trinitycoin (TTY): PoW – myriad;
- TripCoin (TRIP): PoS – scrypt;
- Triskelecoin (TRS): PoS – x11;
- Triviacoin (QUIZ): PoS – SHA2-256;
- Trollcoin (TROLL): PoS – scrypt;
- Trollcoin (TRL): PoW – scrypt;
- Troptions (TRP): PoW – SHA2-256;
- Truckcoin (TRK): PoS – x11;
- Truecrave (TCRAVE): PoS – scrypt;
- Trumpcoin (TRUMP): PoW – x11;
- Trustcoin (TRUST): PoS – x11;
- Trustcoin (TRS): PoS – scrypt;

- Truthcoin (CSH): PoW – SHA2-256;
- T-StormCoin (TSTC): PoS – x15;
- TuHaocoin (THC): PoW – scrypt;
- Tulips (TLC): PoW – SHA2-256;
- Turbocoin (TBC): PoS – x11;
- Turbocoin (XTB): PoW – scrypt;
- Turbostake (TRBO): PoS – SHA2-256;
- Turing Currency (TNG): PoW – fresh;
- Turko (TRK): PoW – scrypt;
- Turroncoin (TUR): PoS – scrypt;
- TuxCoin (TUX): PoW – x11;
- Twecoin (TWE): PoW – twe;
- Twelve (TWLV): PoW – t-inside;
- Twenty15 (2015): PoS – x11;
- Twentyfour (XXIV): PoS – x13;
- Twerk (TWERK): PoS – SHA2-256;
- Twilight Coin (TWC): PoW – x11;
- Twipit (TWIP): PoW – scrypt;
- Twistercoin (TWIST): PoS – x11;
- Twocoin (TWO): PoS – x11;
- UberCoin (XBU): PoS – scrypt;
- UCIcoin (UCI): PoS – x13;
- Ucoin (U): pow-pos – x15;
- UFO Coin (UFO): PoW – scrypt;
- UKcoin (UKC): PoW – SHA2-256;
- Ukrainecoin (UC): PoW – SHA3-256;
- UkranianGirlGoin (UGG): PoS – scrypt-n;
- Ulicoin (ULI): PoW – scrypt;
- Ultimatecoin (UTLE): PoS – x11;
- UltimateCoin (ULT): PoW – scrypt;
- UltraCoin (UTC): PoS – scrypt-j;
- Umbrella-LTC (ULTC): PoW – scrypt;
- UnattainiumV2 (UNAT): PoW – myriad;
- Unattaniumcoin (UNAT): PoW – SHA2-256;
- UnbreakableCoin (UNB): PoW – SHA2-256;
- Uncoin (UNC): PoS – x11;
- UnfedCurrency (UNF): PoW – scrypt;
- Unicoin (UNIC): PoW – SHA2-256;
- Unioncoin (UNC): PoW – quark;
- UniteCoin (UNI): PoW – scrypt;
- United Federation of Planets Credit (UFC): PoW – BLAKE;
- UnitedScryptCoin (USC): PoW – scrypt;
- Unitus (UIS): PoW – myriad;
- UniversalCoin (UNV): PoS – scrypt;
- UniversalCurrency (UNIT): PoS – SHA2-256;
- UniversalMoleculecoin (UMO): PoW – BLAKE;
- Universecoin (UNVC): PoW – x11;
- UniversityCoin (UVC): PoS – scrypt;
- UniversityOfTexasCoin (UTC): PoW – SHA2-256;
- Unobtanium (UNO): PoW – SHA2-256;

- Unumcoin (UNU): PoW – scrypt;
- Upcoin (XUP): PoS – x13;
- UpCoin (UP): PoW – scrypt-n;
- Uranuscoin (URAN): PoW – SHA2-256;
- URCcoin (URC): PoW – scrypt;
- Uro coin (URO): PoW – x11;
- URObarkcoin (UROD): PoS – scrypt;
- USBcoin (USB): PoS – x11;
- UScoin (USC): PoW – scrypt;
- USDe (USDE): PoS – scrypt;
- Usecoin (USE): PoS – x13;
- UtilityCoin (UTIL): PoS – x13;
- V8coin (V8): PoS – x13;
- Vaginacoin (VAG): PoW – scrypt;
- Valorbit (VAL): PoS – scrypt;
- ValueCoin (VLC): PoW – scrypt;
- Vampirecoin (VMP): PoW – scrypt;
- VanadiumCoin (VAC): PoW – scrypt;
- Vanillacoin (VLD): PoW – quark;
- Vanillacoin (VNL): pow-pos - whirlpool;
- VapeCoin (VAPE): PoW – scrypt;
- VaporCoin (VPRC): PoS – SHA2-256;
- Variance (VARY): PoS – SHA2-256;
- Vastcoin (VAST): PoS – x11;
- Vaultcoin (VAULT): PoS – nist5;
- Vaultcoin (VLT): PoW – scrypt;
- Vcoin (VCN): PoW – SHA2-256;
- Vector (VEC): PoS – scrypt;
- Vectorcoin (VCT): PoW – scrypt;
- Vegancoin (VEGAN): PoW – SHA2-256;
- Vegascoin (VGC): PoW – scrypt;
- Veilcoin (VEIL): PoW – x13;
- VelocityCoin (VEL): PoS – scrypt-j;
- Vendettacoin (VAC): PoW – scrypt-j;
- VeniVidiVicicoin (VVV): PoS – x11;
- Venturecoin (VENT): PoW – x13;
- Venturenic (VTN): PoS – qubit;
- Verge (VERGE): PoW – scrypt;
- Vericoin (VRC): PoS – scrypt;
- Verncoin (VNC): PoW – scrypt;
- Versa (VERSA): PoS – x11;
- Version (V): PoS – SHA2-256;
- Vertcoin (VTC): PoW – scrypt-n;
- Vertex (VTX): PoW – scrypt;
- Vexcoin (VEX): PoS – x13;
- Viacoin (VIA): PoS – scrypt;
- Vibranium (XVI): PoS – scrypt;
- Vidioshare (VDO): PoS – scrypt;
- VikingCoin (VIK): PoW – SHA2-256;
- VindCoin (VIND): PoS – scrypt;

- Violetcoin (VLT): PoW – scrypt;
- Violincoin (VIO): PoW – scrypt-n;
- Viorcoin (VIOR): PoW – scrypt;
- VIPcoin (VIP): PoW – scrypt;
- VIPTokensClub (VIP): PoS – nist5;
- Viral (VIRAL): PoS – scrypt;
- Virocoin (VIRO): PoS – SHA2-256;
- Virtacoin (VTA): PoW – scrypt;
- VirtuaCash (VCS): PoS – x13;
- VirtualCoin (VC): PoW – x11;
- Virtualdibscoin (DIBS): PoW – scrypt;
- Virtual Mining Coin (VMC): PoW – scrypt-n;
- Virus (VIRUS): PoS – scrypt;
- Vita (VIT): PoS – x13;
- VMine (VMINE): PoS – x11;
- Vocal (VOCAL): PoS – x15;
- VodkaCoin (VDC): PoW – scrypt;
- Void (VOID): PoS – desconhecido;
- VolatilityCoin (VLT): PoS – x15;
- Volcanocoin (VOLC): PoS – x13;
- Volume (VOL): PoW – x11;
- Volume (VOL): PoW – scrypt;
- VootCoin (VOOT): PoS – x11;
- VorteX (VTX): PoS – x13;
- Votecoin (VOT): PoW – novel;
- Voxels (VOX): PoS – scrypt;
- Voxpopulicoin (VOXP): PoS – x13;
- Voyacoin (VOYA): PoW – pluck-128;
- VPNcoin (VPN): PoS – scrypt;
- vTorrent (VTR): PoS – scrypt;
- VvXxCoin (VVXX): PoS – x13;
- W2Coin (W2C): PoW – scrypt;
- Waccoin (WAC): PoW – scrypt;
- WaccoinGold (WACG): PoW – scrypt;
- WalletCoin (WTC): PoW – scrypt;
- Wampumcoin (WAM): PoW – scrypt;
- Wangminbi (WMB): PoW – scrypt;
- Wankcoin (WKC): PoW – SHA2-256;
- WanZhongcoin (WZC): PoS – x11;
- Warofcoins (WOC): PoS – SHA2-256;
- WarOfCoinsX (WOCX): PoS – x11;
- Warp (WARP): PoS – x11;
- Waspcoin (WASP): PoS – x13;
- Watcoin (WAT): PoW – x11;
- Waterpumpcoin (PUMP): PoS – scrypt;
- Wavecoin (WVS): PoS – x11;
- WCG Coin (WCG): PoW – ripple;
- Wealthcoin (WEALTH): PoS – scrypt;
- WeAreNakamotoCoin (WAN): PoW – SHA2-256;
- Wearesatoshi (WAS): PoW – SHA2-256;

- WeAreSatoshi (WSX): PoS – x11;
- Webcoin (WEB): PoW – x14;
- Wecoin (WC): PoW – SHA3-256;
- Weedcoin (WEC): PoW – scrypt;
- WeedTokens (WETK): PoS – x11;
- Wepcoin (WEP): PoW – scrypt;
- WFPcoin (WFP): PoW – quark;
- Whalecoin (WHAL): PoW – SHA2-256;
- Whalecoin (WHALE): PoS – x11;
- Whirlcoin (WHRL): PoW – Whirlpool;
- Whistlecoin (WSTL): pow-pos – x11;
- Whitecoin (WC): PoW – scrypt;
- Whitecoin (XWC): PoS – scrypt;
- Whycoin (WHY): PoW – scrypt;
- WifiCoin (WIFI): PoS – x11;
- WikiCoin (WIKI): PoW – quark;
- WildBeastBitcoin (WBB): PoW – scrypt;
- Wildfire (WF): PoW – scrypt;
- Wildwestcoin (WEST): PoS – x11;
- Wincoin (WIN): PoS – x11;
- Windcoin (WND): PoS – x11;
- Winecoin (WNC): PoS – scrypt;
- Wintercoin (WINTER): PoS – x11;
- WinterCoin (WINT): PoS – x11;
- Wisecoin (WISE): PoS – scrypt;
- Witchcoin (WITCH): PoS – x11;
- Wolfcoin (WLF): PoW – SHA3-256;
- WolongCoin (WOLONG): PoW – scrypt-n;
- Wonderful8Coin (W8): PoS – x13;
- Woodcoin (LOG): PoW – Skein;
- Woolfcoin (WOO): PoW – scrypt;
- WorldAidCoin (WAC): PoW – scrypt-n;
- WorldCoin (WDC): PoW – scrypt;
- WorldCupCcoin (WCC): PoW – x11;
- WorldCupcoin (WCUP): pow-pos – x11;
- World Football coin (WFC): PoS – scrypt;
- WorldLeadCurrency (WLC): PoW – SHA2-256;
- Worldpay (WOP): PoS – x11;
- WorldPeaceCoin (WPC): PoW – SHA2-256;
- WorldTopCoin (WTC): PoW – scrypt-j;
- WorldTradeFund (XWT): PoS – x15;
- Worldwidecoin (WWC): PoW – SHA2-256;
- Wotcoin (WOT): PoW – SHA3-256;
- WPcoin (WPC): PoW – scrypt;
- WTFcoin (WTF): PoS – x15;
- X11Bitcoin (XBTC): PoS – x11;
- X11coin (XC): PoW – x11;
- X13Coin (X13C): PoS – x13;
- X14coin (X14): PoW – x14;
- X15Coin (X15COIN): PoS – x15;

- X² (X2): PoS – x13;
- Xagon (XAGON): PoW – x11;
- Xanaxcoin (XNX): PoS – scrypt;
- XanonCoin (XAN): PoS – x11;
- Xaucoin (XAU): PoW – SHA2-256;
- Xcalibit (XBIT): PoW – SHA2-256;
- XCashcoin (XCASH): PoS – scrypt;
- XChildrencoin (CHILD): PoW – x11;
- XCloudcoin (XCLD): PoS – x11;
- Xcoin (XCO): PoW – scrypt;
- X-Coin (XCO): PoW – SHA2-256;
- Xcurrency (XC): PoS – x11;
- XDDcoin (XDD): PoS – x13;
- Xedoscoin (XDC): PoW – Skein;
- XenCoin (XNC): PoW – scrypt;
- Xenoncoin (XEC): PoW – myriad;
- XGcoin (XG): PoW – xg;
- XGeneration (XGEN): PoS – scrypt;
- Xiaomicoin (MI): PoS – scrypt;
- Xivra (XIV): PoS – scrypt;
- Xmascoin (XMAS): PoS – scrypt;
- Xquadron (QUAD): PoS – scrypt;
- xRadon (XRDN): PoS – scrypt;
- Xryptbitcoin (XBIT): PoW – qubit;
- Xtracoin (CX): PoS – SHA2-256;
- Xurocoin (XURO): PoS – x11;
- XXLcoin (XXL): PoW – scrypt;
- XXXcoin (XXX): PoS – scrypt;
- YACCoin (YACC): PoW – scrypt-j;
- Yacoin (YAC): PoS – scrypt-j;
- Yamashitacoin (YMC): PoS – x11;
- YangCoin (YANG): PoW – scrypt;
- YardSaleCoin (YSC): PoW – SHA2-256;
- YatYatLingcoin (YYL): PoW – SHA2-256;
- Yaycoin (YAY): PoW – SHA1-256;
- YbCoin (YBC): PoS – scrypt-j;
- YellowCoin (YC): pow-pos – scrypt;
- YellowLionCoin (YLC): PoW – SHA2-384;
- Yep (YEP): PoS – SHA2-256;
- YetCoin (YET): PoS – x11;
- YinCoin (YIN): PoW – scrypt;
- YinYangCoin (YINYANG): PoW – scrypt;
- Yocoin (YOC): PoW – scrypt;
- YoCoin (YOC): PoW – scrypt;
- Yolocoin (YOLO): PoW – scrypt;
- YoMama (MAMA): PoW – scrypt;
- Yovivirtualcoin (YOVI): PoS – SHA2-256;
- Ypcoin (YPC): PoW – scrypt;
- Yupcoin (YUP): PoW – scrypt;
- Zapcoin (ZAP): PoS – nist5;

- ZcCoin (ZCC): PoS – scrypt-j;
- Zebracoin (ZEB): PoS – x11;
- Zedcoin (ZED): PoW – scrypt;
- Zeitcoin (ZEIT): PoS – scrypt;
- ZenithCoin (ZTC): PoW – scrypt;
- Zerocoin (ZRO): PoW – SHA2-256;
- Zerovert (ZER): PoW – scrypt-n;
- Zestcoin (ZEST): PoW – scrypt;
- Zeta2coin (ZET2): PoW – quark;
- Zetacoin (ZET): PoW – SHA2-256;
- Zeuscoin (ZEU): PoW – scrypt;
- ZGCoin (ZGC): PoS – SHA2-256;
- ziftrCOIN (ZRC): PoS – zr5;
- Zimstake (ZS): PoW – SHA2-256;
- Zipcoin (ZIPC): PoS – x13;
- Zippercoin (ZIP): PoW – scrypt;
- Zirkcoin (ZIRK): PoS – scrypt;
- Zombiecoin (ZMB): PoW – scrypt;
- Zombiecoin (ZMC): PoS – SHA2-256;
- Zoom (ZOOM): PoW – lyra2re;
- Zurcoin (ZUR): PoW – quark.

MINERAÇÃO NA NUVEM

Minerar na nuvem (*cloud*) é quando se aluga um serviço de mineração online; ou seja, quando não se usa o próprio dispositivo (computador).

A *cloud mining* (mineração na nuvem) nada mais é do que servidores na nuvem ("cloud servers" ou VPS - "Virtual Private Server") que fornecem (alugam) seu poder se processamento remoto para o cliente minerar.

A mineração na nuvem, portanto, dispensa o software de mineração oficial e o gasto ou investimento com hardware de mineração e correlata refrigeração, eletricidade do equipamento minerador e de seu sistema de refrigeração e do consumo, alto e contínuo, de banda e de tráfego, de conexão com a Internet. Além disso, tem-se a comodidade de não ter que reservar um local para deixar o equipamento minerador funcionado, e fazendo barulho e calor, 24 (vinte e quatro) horas por dia.

Entretanto, muitos sites de *cloud mining* são *scam* (golpe ou fraude); ou seja, não são muitas as opções sérias ou confiáveis onde se possa investir com segurança na mineração na nuvem.

- http://g1.globo.com/tecnologia/blog/seguranca-digital/post/empresas-de-mineracao-de-bitcoin-sao-acusadas-de-fraude-nos-eua.html.

Em síntese, a pergunta que deve ser feita é a seguinte. Se uma pessoa, ou um grupo de pessoas, possui condições de poder montar um equipamento profissional de mineração, porque iria dividir isso com estranhos? A única justificativa plausível seria que parcelaram ou financiaram os equipamentos e que pretendem irem fazendo manutenção e *upgrade* (atualização) nos mesmos para poderem continuarem competitivos. Mas, mesmo assim, daria para desconfiar. Mas, se apenas uma parcela desse poder de processamento total é alugada, aí estar-se-ia sendo mais semelhante às empresas que negociam ações na bolsa de valores para conseguirem capital para a expansão da empresa. Por outras palavras, é, no mínimo, muito estranho a empresa alugar todo o seu potencial de mineração. Pior se a mineradora pagar retorno financeiro muito bom.

Em alguns sites de mineração na nuvem, além de poder pagar através de determinadas criptomoedas, também pode ocorrer do novo usuário receber algumas moedas para poderem ser trocadas pelo poder de processamento inicial; algo normal ao se saber que outras podem até dar uma mineração mínima ou simbólica de graça para que o novo usuário teste e confirme que a mineração realmente acontece. Também pode acontecer, tal como nas *faucets* (torneiras), do site de mineração na nuvem ter opção de poder indicar novos usuários e atribuir uma pequena comissão por isso; normalmente paga em aumento (melhora ou *upgrade*) de poder de processamento (*computational power*) na correlata mineração na nuvem. Por outras palavras, não pagam comissão em dinheiro, mas em prestação de serviço. Em sites de mineração na nuvem que minere mais de uma moeda digital, pode-se começar a mineração com a moeda mais fácil (e normalmente mais barata) de minerar e ir trocando o rendimento por poder ou potência de processador até que consiga um processamento adequado para mudar de moeda e assim sucessivamente.

Em existindo contas gratuitas na mineração em nuvem, uma pergunta lógica é quantas contas uma mesma pessoa pode fazer? Qual é o critério para saber que se trata da mesma pessoa? Se for o e-mail, basta a pessoa apresentar diferentes e-mails, um para cada nova conta.

No começo as falsas mineradas agem corretamente e pagam tudo e todos corretamente com a intenção de ganharem confiança dos usuários e credibilidade no mercado. Como está tudo funcionando "certinho" e estão pagando corretamente, muitos usuários fazem vídeos e os postam na Internet provando isso "de olho" na comissão pela indicação de novos membros. Em razão desses fatores, a quantidade de clientes vai aumentando cada vez mais e quanto mais tempo o cliente está no esquema, mais ele investe em poder de processamento ou de mineração (*has power*) porque tudo está funcionando conforme o prometido. Entretanto, assim que a falsa mineradora tiver uma boa quantidade de investimentos feitos ou quando a quantidade de solicitações de pagamentos (saída) superar o valor dos investimentos ou aplicações (entrada), começam a aparecer alguns *bugs* (falhas) repentinas no site dando erro nos pedidos de saques e atrasando os pagamentos. Falhas estas que no começo a falsa mineradora apresenta justificativas, desculpas, pedido de paciência e promessa de que tudo será resolvido e normalizado

em breve; inclusive prometendo uma gratificação como forma de compensação pelos transtornos, com o que muitos se animam e se acalmam. Entretanto, de repente, o site não funciona mais, não existe mais o site e ninguém tem notícias da empresa ou das pessoas responsáveis. Pronto, o golpe foi finalizado! O escalonamento do poder de processamento funcionou como hierarquia na pirâmide. As falhas nos sites e as explicações dadas, somadas ao prazo mínimo de tantos dias para o pagamento, somente tiveram a intenção de prolongar ainda as arrecadações. Exemplificando, digamos que a mineradora somente pagava todo 5º (quinto) dia útil; então ela já arrecadava por 30 (trinta) dias antes de pagar. Com as falsas falhas, esses 30 (trinta) dias podem ter se tornado 40, 50, 60... dias só recebendo e sem efetuar nenhum pagamento. E, assim, que os pagamentos pararem ou diminuírem drasticamente, o site é encerrado definitivamente. Desse modo, empresas sérias de mineração na nuvem (*cloud mining*), diariamente, de forma automática e direta, depositam nas contas (endereços públicos) dos clientes as suas cotas ou rendimentos do resultado da mineração. Por outras palavras, a existência de quantidade mínima para retirada e, ainda, a exigência do cliente ter que solicitar o pagamento, são sempre suspeitas. Algumas pessoas dizem que essas mineradoras falsas possuem apenas cerca de 6 (seis) meses de vida; ou seja, desde a criação até o encerramento. Entretanto, a HashOcean pagou os usuários continuamente por mais de 10 (dez) meses antes do grande final. Outro detalhe é que as falsas mineradoras normalmente não aceitam pagamentos através de meios convencionais; vez que tais procedimentos envolvem fornecerem uma conta bancária tradicional ou alguma outra forma de identificação do beneficiário dos pagamentos.

A Minerclound, por exemplo, aparentemente fechou “da noite para o dia” e deixou os clientes “a verem navios”. Já a Cloud mining simplesmente parou de funcionar e quando voltou, não era mais confiável. Outra que deixou os clientes "na mão" foi a HashOcean.

Outros exemplos são Ghsmine, Mixmine, Joltcorp, Profit-coin, Multi-coin, Fastmining, Bitminer, Onemine, Hash-line, Minerbitcoinsfree, Bitmine, Firebit, Hasheer, Investimentos.trade, Biteminer, Mixmine, Scurmrr, Upmcoins, Minerport, Aromine, Sky-hash, Xmine, Hash-capital.com, Hot-Coin, CLDMine, Topmine, Bitcoin Cloud Services, Cloudminr, etc.

- https://guiadobitcoin.com.br/hashocean-e-topmine-saem-do-ar-e-5-dicas-para-nao-cair-em-ciladas/.

Confira-se uma listagem de mineradoras *scam* (esquema fraudulento) ou esquema Ponzi:

- http://www.cmmonitor.com/;
- https://bitcointalk.org/index.php?topic=878387.msg14980900#msg14980900;
- http://www.badbitcoin.org/thebadlist/#TOP.

Algumas das considerações a serem feitas antes de contratar um serviço de mineração na nuvem:

1) Longevidade não é sinônimo de legalidade. Não é porque a empresa, site ou serviço existe a um determinado tempo que significaria seriedade ou legitimidade. Um esquema Ponzi ou de pirâmide, por exemplo, pode durar anos não se restringindo aqueles que possuem vida curta. O negócio mantém-se aberto ou ativo enquanto conseguir arranjar novos clientes que vão alimentando os mais antigos;

2) Qual é a razão social (nome comercial) da empresa? Deve pesquisar informações da empresa através do seu nome comercial e do seu CNPJ (ou identificação equivalente) com a finalidade de saber se existem protestos, ações judiciais, investigações policiais, etc. **Informalidade demais é muito suspeita**. Se a empresa ou minerador não fornece nenhuma **identificação** formal e nem sequer emite **nota fiscal ou recibo**, evidencia algo duvidoso. É inconcebível uma empresa não possuir instalações físicas e sequer ter um número de telefone fixo;

3) Quem é o proprietário da empresa? Deve-se conferir quem está por trás da empresa e saber seu histórico ou antecedentes; bem como se sofre ações judiciais ou se já foi condenado judicialmente antes. Na comunidade criptográfica essa pessoa já é conhecida? O que essa pessoa fazia antes de ter essa empresa?;

4) Avaliações de usuários podem ser simuladas. Os depoimentos, testemunhos e comentários favoráveis podem consistir em mentiras

feitas pelo próprio golpista. Deste modo não são críveis as avaliações positivas feitas no próprio site da empresa. Também é muito suspeito quando só existem depoimentos favoráveis ou com conteúdo exagerados. As avaliações mais confiáveis, portanto, são aquelas feitas em sites de terceiros, principalmente nos que se presume imparcialidade, independência ou inexistência de qualquer vínculo com a empresa de mineração na nuvem; preferencialmente os fóruns sobre as criptomoedas. Apesar de que também não estarão imunes a comentários falsos, a probabilidade de conterem comentários verdadeiros é bem alta. Ressalta-se que algumas empresas contratam pessoas para ficarem fazendo comentários positivos dela pela Internet. Em síntese, a regra é procurar e dar atenção aos comentários negativos, ao quais, também, podem ser mentirosos, mas tal incidência é bem menor do que as mentiras em comentários positivos;

5) Provas da existência física. Para pode operar, a empresa necessita de um espaço físico com equipamentos mineradores conectados à Internet e com refrigeração. Deve-se, portanto, conferir onde é esse local e quais são esses equipamentos. No site do Google é possível analisar fotos para saber se não foram copiadas da Internet; ou seja, se as fotos apresentadas são falsas. Confira como fazer: https://www.google.com/intl/pt-BR_ALL/insidesearch/features/images/searchbyimage.html;

6) Provas de mineração. As mineradoras na nuvem confiáveis, normalmente, informam os processadores ASIC's e as máquinas que estão utilizando; inclusive devem comprovar os blocos que foram minerados por elas e a *pool* (piscina) de mineração a qual estão minerando. Se a empresa realmente minera, ela possui uma identificação (endereço IP) dentro da rede P2P da criptomoeda; bem como em algum lugar deve aparecer listada como participante da rede P2P. Outro detalhe, obrigatoriamente, a empresa possui um endereço (chave) público da respectiva da criptomoeda, com o qual pode-se conferir os pagamentos recebidos e efetuados;

7) Limitação *Hashrate*. Cada máquina tem uma limitação de *hashrate* e supõe-se que cada empresa tenha uma limitação de máquinas para

oferta. É, no mínimo, estranho se não houver informações claras quanto a esse aspecto.

8) Relação de clientes. É de interesse da empresa, por alguma forma, divulgar ou provar quem são os seus clientes; vez que isso porque ajuda a promover as suas vendas. Além disso, a existência de um fórum ou comunidade dos clientes da empresa onde os clientes podem interagirem entre si, mas sem esquecer da regra de não se pode acreditar rápido em comentários positivos;

9) Desconfiar de descontos. Em razão de que toda empresa, comércio ou prestador de serviços possui custos, encargos e tributos a serem pagos e vivem dos lucros auferidos, os valores muito abaixo da concorrência são sempre suspeitos; bem como promoções ou descontos duradouros;

10) Aceitam pagamento com cartões de crédito? Para a empresa poder aceitar pagamentos com cartões de crédito, é necessário ter fornecido alguma identificação real para a instituição financeira, o que golpistas tendem a evitar de fazer. Além do que o cartão de crédito possui o recurso de contestação de pagamento;

11) Não existem garantias. Se uma empresa de mineração promete uma remuneração garantida está mentindo; vez que ninguém pode prever como vai evoluir a taxa de câmbio ou qual será a real lucratividade da mineração;

12) Bom demais para ser verdade. Essa é a principal regra ou regra de ouro; sempre desconfiar de propagandas onde tudo é maravilhoso, fantástico, perfeito ou excelente. Se parece um sonho é porque, normalmente, não passa disso, um mero sonho;

13) Pesquisar por vítimas da empresa. Se uma empresa aplicou golpe em muitas pessoas, provavelmente existem postagens, sites, blogs, grupos, comunidades ou fóruns nesse sentido;

14) As comissões serem o retorno do investimento. Programas de indicação ou de afiliados onde se paga, pelo menos, 10% (dez por cento) ou que dita comissão supera facilmente o retorno da própria mineração, tornando esta secundária, é evidência de pirâmide financeira. Mineração em nuvem não é MMN - Marketing Multinível;

15) Confisco. Se a empresa prende ou limita o saque dos ganhos, é um sinal de alerta;

16) Milagre da multiplicação. Se a mineradora usa o chavão de multiplicação de bitcoins e/ou altcoins, provavelmente é esquema Ponzi ou pirâmide financeira;

17) Consulte informações do site da mineradora em https://www.whois.net/ ou outro site de ***whois*** e confronte com as alegações (data de início das atividades, proprietários, local da empresa, etc.). Se alguma informação estiver oculta, restringida, sob sigilo ou não informada, é mal sinal;

18) A mineradora **é a própria piscina ou usa a piscina alheia?** As empresas golpistas costumam usar piscinas de mineração alheias enquanto que uma mineradora séria é a própria piscina de mineração.

As mineradoras na nuvem que mais possuem credibilidade são apenas https://www.genesis-mining.com/ e https://hashflare.io/. E, mesmo assim, há quem pense que são *scam*: https://bitcointalk.org/index.php?topic=1356688.0;all.

Sugere-se arriscar, no máximo, por um período de 3 (três) a 6 (seis) meses numa mineração na nuvem desconhecida e só voltar a arriscar de novo no mesmo site, após 6 (seis) meses.

Infra outros **sites de mineração na nuvem (*cloudmining*)** que estão pendentes de avaliação:

- https://scrypt.cc/;
- https://www.coinbr.net/mining;

- https://www.cryptopia.co.nz/Mineshaft;
- https://hasheer.com/;
- https://zeushash.com/;
- https://www.eobot.com/;
- https://www.hashnest.com/;
- https://www.miningsweden.se/;
- https://bitsrapid.com/;
- https://www.gigahash.org/;
- https://www.hashnest.com/;
- https://www.nicehash.com/;
- http://rent.mineoncloud.com/;
- https://www.miningrigrentals.com/;
- http://cryptomine.weebly.com/;
- http://coinomia.com/;
- http://spondoolies-tech.co/pages/cloud-mining.html.

MINERAÇÃO EM PISCINA (*POOL*)

É recomendável minerar bitcoins através de uma *pool* (piscina), como, por exemplos, a Bitclub Network (https://bitclubnetwork.com/) ou Eligius (http://eligius.st/). As *pools* de Mineração são grupos de mineradores de Bitcoin que trabalham juntos para encontrar a chave dos blocos e que partilham as recompensas. É muito mais conveniente partilhar o trabalho e dividir os lucros com um grupo maior de mineradores.

Normalmente nas próprias postagens de anúncio da moeda ou nos sites da mesma existem as indicações das piscinas de mineração.

Uma das formas de escolher uma *pool* é através da conferência do percentual de participação das *pools* na produção dos blocos; informações estas que estão disponíveis nos sites contendo a *Blockchain* (https://blockchain.info/pt/pools/ e https://bitcoinchain.com/pools). E, depois procurar por informações e comentários a respeito.

Outro procedimento é pesquisar nos fóruns; assim, por exemplo: https://bitcointalk.org/index.php?board=199.0.

Outra forma é através da comparação entre elas.

- https://en.bitcoin.it/wiki/Comparison_of_mining_pools.

EQUIPAMENTOS DE MINERAÇÃO

Existem vários fabricantes de *hardware* de mineração de criptomoedas (Bitcoins e altcoins), com diferentes sistemas e modelos (AntMiner, ASICMiner, Avalon, GekkoScience, TerraHash, Spondooliestech, RockMiner, NanoFury, HashBuster, HashFast, HashCoins, Butterflylabs, BTC-AM, BPMC, etc.).

- https://mybtcpool.com/.

Também nesse meio há casos de fraudes, como, por exemplo, empresas que não entregam o produto, equipamentos que não funcionam e empresas de encerram as atividades rapidamente.

Os equipamentos (*rigs*) **ASICs** (*Application Specific Integrated Circuits*) são pré-configurados para uma atividade e não podem ser reaproveitados, reconfigurados ou reprogramados para outra tarefa. Por outras palavras, se o equipamento (*rig*) foi configurado para minerar bitcoins, é praticamente impossível minerar outro tipo de criptomoeda; salvo, pela remota possibilidade do milagre do equipamento permitir pequenas configurações ou ajustes que o permitiria minerar outra moeda digital muito semelhante ao Bitcoin. Mas a possibilidade desse tipo de ajuste deve ser previamente conferida antes de comprar o equipamento. Outro detalhe importantíssimo, a evolução dos equipamentos de mineração é tão rápida que em pouquíssimo tempo (digamos, 5 anos) o equipamento se torna obsoleto ou inviável. Portanto, equipamentos ASIC possuem vida útil muito curta. Pelas mesmas razões não se recomenda a compra de um equipamento ASIC usado.

Desse modo, uma opção interessante é investir na mineração de alguma altcoin que não precise de um equipamento ASIC, mas que possa ser feita por um computador "normal" com configuração estilo de *gamer top* de linha; vez que, além de facilmente se mudar a moeda minerada (e existem várias opções), quando enfim o equipamento se tornar inútil para a mineração de criptomoedas, pode ser reaproveitado para várias outras atividades; além do que pode ser facilmente vendido. E, outro detalhe, em um computador desktop podem ser feitos *upgrades* (aprimoramentos) facilmente através da

simples substituição de componentes (processador, placa de vídeo, memória RAM, placa-mãe, disco rígido, modem, etc.), cujos itens substituídos podem ser vendidos. E, principalmente, considerando que muitos já possuem um computador, é possível fazer um teste prévio de mineração, sem gastar praticamente nada além da energia elétrica, para se ter uma noção de como é a mineração de determinadas altcoins.

Diante dessas considerações, antes de comprar um equipamento ASIC de mineração Bitcoin deve-se fazer uma previsão ou estimativa de todas os custos e despesas envolvidas, do rendimento teórico que o equipamento fará considerando o atual nível de dificuldade da moeda e da capacidade de mineração da concorrência; inclusive, levando-se em conta, o prazo teórico de um ano mantendo esse nível de rendimento e que a cada ano o nível de rendimento irá cair mais (digamos 20% ao ano), até que, em torno, de cinco anos o equipamento se tornará sucata. Ressalta-se que essas referências dadas para a elaboração de uma estimativa não são precisas, mas meramente teóricas para que a pessoa possa ter uma noção ou alguma referência para evitar de comprar "no escuro", na empolgação, sem nenhum critério, sem nenhuma noção ou desprovida de qualquer embasamento. Outro detalhe, mesmo que se use como referência os valores precisos de quais foram os percentuais de redução anual no passado, isso não significa que os mesmos percentuais se repetirão precisamente; vez que existem múltiplos fatores variáveis e imprevistos envolvidos. Desse modo, sugere-se que a pessoa interessada em comprar um equipamento de mineração, se informe qual é a atual potência máxima de processamento na rede da criptomoeda para que este valor seja a base (100%) para calcular uma previsão de queda de rendimento nos próximos anos. Se a pessoa pretender comprar um equipamento inferior a esse teto, já deve considerar que inicialmente ele será apenas uma fração do teto ou valor base atual; portanto, terá uma vida útil mais curta. De modo semelhante, se eventualmente o equipamento desejado possuir um valor de processamento superior ao atual da rede, dependendo da quantidade de outros mineradores que farão o mesmo, o grau de dificuldade será reajustado, com o que essa diferença a mais (*plus*) será perdida em determinado tempo; mas, mesmo assim, com a elevação da dificuldade, muitos mineradores serão retirados da competição antes do tempo. Se a estimativa de queda de 20% ao ano se demonstrar exagerada na prática (realidade), melhor será para o minerador que colherá rendimentos

maiores e por mais tempo. Mas nada impede que a pessoa aumente essa previsão para mais ou para menos; afinal o valor da aposta é definido pelo apostador.

Os equipamentos mais populares são Antminer, GH USB BitFury e Spondoolies, que possuem versões para Bitcoin e Litecoin e são encontrados facilmente pela Internet. Mas existem várias outras mineradoras no mercado:

- http://picclick.at/Bitcoin-Miner-Coincraft-800-GH-s-ASIC-BTC-Bitcoin-272449835751.html;
- http://www.ebay.at/itm/122209232799?clk_rvr_id=1128902228631&rmvSB=true;
- http://www.ebay.at/itm/381860680740?clk_rvr_id=1128868676521&rmvSB=true;
- http://anarcoin.org/product/sold-out-bitcoin-miner-antminer-s9-11-85th-asic-miner-newest-16nm-btc-miner-better-than-antminer-s7-with-psu/.

Como referência, citamos que em agosto de 2016, o fabricante de *hardware* de mineração Bitmain (https://bitmain.com/) anunciou o equipamento de mineração Antminer R4, com dois chips (BM1387 ASIC Chip de 16nm) de mineração de bitcoin mais eficientes do mundo (hashrate de 8,6 TH/s), consumindo apenas 845W de energia elétrica, pelo preço de $ 1.395,00. A empresa recomenda o uso da fonte de alimentação APW5 2600W. Cada Antminer R4 emprega 126 chips para entregar mais hashrate e eficiência do que qualquer *hardware* minerador bitcoin, exceto o Antminer S9.

- https://enshop.bitmain.com/productDetail.htm?pid=00020160829050856183dK8A4TFO0645.

Em sites como https://en.bitcoin.it/wiki/Mining_hardware_comparison e https://en.bitcoin.it/wiki/List_of_Bitcoin_mining_ASICs existem tabelas comparativas dos *hardwares* de mineração.

Infra uma lista de alguns dos **fabricantes** de *hardware* de mineração:

- Bitmain (https://bitmain.com/);

- Avalon da empresa Canaan (https://canaan.io/);
- Ufominers (http://www.ufominers.com/);
- Baikal-miner (http://baikal-miner.com/);
- Innosilicon (http://www.innosilicon.com/html/mining-asic/14.html);
- Spondoolies-tech (http://spondoolies-tech.co/collections/products.html);
- Sfards (http://sfards.com/pro/miner);
- KNC (http://www.kncminer.com/);
- Bitcrane (http://www.bitcrane.com).

Alguns locais **onde comprar** *hardware* de mineração:

- https://shop.bitmain.com/main.htm?lang=en;
- https://www.hobbymining.com/mining-hardware/;
- http://holybitcoin.com/;
- http://zoomhash.com/collections/bitcoin-asics;
- http://zoomhash.com/collections/asics;
- http://store.bitcoinrigs.org/;
- https://www.eastshore.xyz/;
- https://www.asicminermarket.com/;
- https://asic-miners.co.technology/;
- https://www.minerslab.com/;
- http://informatica.mercadolivre.com.br/asic-bitcoin;

- http://portuguese.alibaba.com/;
- http://www.ebay.com/;
- http://anarcoin.org/;
- http://www.espacoinfo.net/;
- http://www.ollasupply.collaborativeleaders.us/product-tag/asic-miner.olla.

Saiba mais sobre *hardware* de mineração:

- http://cryptomining-blog.com/;
- http://www.coinminingrigs.com/;
- http://www.bitcoinrigs.org/;
- http://www.cryptominingtalk.com/;
- http://www.topbitcoinmininghardware.com/blog/.

Outra opção, é **montar o próprio equipamento específico de mineração usando peças de computadores**.

O primeiro componente essencial que deve ser pensado é a **fonte de alimentação**. A fonte de alimentação é a responsável pelo fornecimento de eletricidade ao computador e todos os seus componentes, através da conversão da tensão (110 V ou 220 V) da corrente alternada (siglas, CA ou AC) fornecida pela rede elétrica (existente na tomada onde se liga a fonte) em tensões (+3,3 V, +5 V, +12 V e 12 V) de corrente contínua (siglas, CC ou DC). Portanto, não é possível ligar diretamente na tomada nenhum componente de computador sem existir uma fonte; recordando que os computadores prontos já veem com uma fonte interna. Se a fonte de alimentação não tem, pelo menos, um conector de alimentação de seis pinos para placas de vídeo, isso normalmente significa que ela é uma fonte de baixa qualidade e com potência rotulada falsa. Em resumo, deve-se procurar a fonte com a maior potência total ou real possível (exemplo 1600W) e que contenha a maior variedade e quantidade de conectores.

As três unidades mais básicas em eletricidade são tensão (V), corrente (I) e resistência (r). A tensão é medida em volts, a corrente é medida em

amperes e a resistência é medida em ohms. Voltagem é a forma coloquial de se dizer tensão. Amperagem é a intensidade da corrente. A potência (P) elétrica é igual à tensão (V) multiplicada pela corrente (I); já corrente (I) é igual à tensão (V) dividida pela resistência (r). Através da fórmula I = P / V pode-se calcular a quantidade de corrente em amperes necessária. 1 é a quantidade de carga elétrica carregada pela corrente de 1 ampere durante 1 segundo. Fazendo uma analogia a encanamento de água, a tensão é equivalente à pressão da água, a corrente é equivalente à taxa de fluxo e a resistência é como o tamanho do tubo. A tensão elétrica é como a velocidade da água passando no cano; já a amperagem é similar à bitola (espessura ou diâmetro) do cano. Um cano fino com água em grande velocidade dá o mesmo volume que um cano mais grosso com água com menos pressão. Do mesmo modo que ao aumentar a pressão da água num encanamento, mais água sairá por segundo da torneira ou da mangueira; aumentar a voltagem implica em aumento do fluxo de corrente elétrica. Do mesmo modo que aumentar o diâmetro (largura, espessura ou grossura) do cano ou tubo faz com que mais água seja transportada por segundo; em eletricidade a diminuição da resistência aumenta o fluxo de corrente. É semelhante a quantidade de pistas numa rodovia, quanto menos pistas, maior o congestionamento; já quanto mais pistas, melhor será o fluxo de veículos. E quanto maior a velocidade dos veículos, também maior será a quantidade de veículos movimentados por segundo. Portanto, existem duas formas de aumentar a quantidade trafegada por segundo, uma é aumentando a pressão (água), velocidade (automóveis) ou tensão (energia elétrica). A segunda é diminuindo a resistência (obstáculo) através do alargamento ou do aumento da via de transporte. Em um sistema elétrico, aumentando tanto a corrente ou a tensão resultará em maior potência. Entretanto, o ideal é usar menos corrente possível para poder fornecer a quantidade de energia elétrica necessária; vez que a resistência em fios elétricos consome energia e à medida que a corrente que passa pelos fios aumenta também o consumo pela resistência aumenta e quanto maior o consumo pela resistência, maior será o calor produzido. A resistência da corrente elétrica pode ser compreendida através do que acontece com um automóvel, com formato muito quadrado (nada aerodinâmico), que sofre a resistência do ar e quanto mais aumenta a velocidade, maior será a resistência do ar. Fato este que ocorre com as naves espaciais ao reentrarem na atmosfera terrestre em altíssima velocidade, com o que ocorre um superaquecimento. Mas os veículos

aerodinâmicos, por não sofrerem ou reduzirem a resistência do ar, conseguem um melhor desempenho. Recorda-se que os chuveiros elétricos aquecem a água através de resistência e que as lâmpadas comuns, chamadas de incandescentes, são radiadores térmicos. Consistem de um filamento de tungstênio pelo qual passa uma corrente elétrica de até 3000°C, que o aquece a tal ponto que a energia é transformada em forma de luz e calor. A equação V = I x R demonstra o poder em termos de resistência e corrente; já a fórmula P = V x I demonstra que a energia consumida pelos fios aumenta se a resistência dos fios também aumenta (por exemplo, se os fios ficam menores ou se são feitos de um material menos condutor). Mas aumenta dramaticamente se a corrente que passa pelos fios aumenta. Assim, utilizando uma tensão mais alta para reduzir a corrente elétrica pode tornar os sistemas mais eficiente. O aumento dos volts satisfaz a necessidade de maior eletricidade sem ter que aumentar o tamanho dos fios ou de fornecer maior corrente.

Baixe o Manual e catálogo do eletricista - Um guia prático para instalações residenciais e prediais no site http://www.voltimum.com.br/campanha/campanha-registos-atraves-facebook-1-2016.

Algumas marcas de fontes de alimentação são Corsair (http://www.corsair.com/pt-br), Xfx (http://xfxforce.com/) e Evga (http://br.evga.com/).

A fabricante **EVGA** (http://br.evga.com/) possui a linha SuperNOVA 1600 com 1600W, com processadores C6/C7 Idle Mode compatíveis com a 4º geração do Intel Core, garantia de 10 (dez) anos e inigualável suporte ao cliente. Seus capacitores japoneses (Nippon Chemi-Con) garantem melhor estabilidade, confiabilidade, *overclocking* e controle sem precedentes. A sua entrada de AC (corrente alternada) é de 115 - 240 VAC, 17-10A e 50 - 60 Hz. Possui saída de CC (corrente contínua) para as voltagens +3.3V, +5V, +12V, +5Vsb e -12V. Suas saídas máximas são 24A, 24A, 133.3A, 3A e 0.5A. Contam com os seguintes conectores: 9 (nove) VGA (Video Graphics Array), 2 (dois) CPU, 4 (quatro) SATA, 1 (uma) MB e 2 (duas) perfis. Possui a Certificação NVIDIA SLI, com o que permite que várias placas de vídeo NVIDIA estejam em execução. Um ventilador *dual-ball bearing*

(duplo balanceamento) de alta qualidade oferece um excelente perfil térmico e acústico (sem ruídos). A certificação 80 Plus garante que a fonte de alimentação não está desperdiçando energia e transformando isso em excesso de calor. O EVGA ECO *Thermal Control System* (Controle de Sistema Térmico) proporciona uma operação silenciosa com cargas baixas, maior eficiência e maior vida útil do ventilador; além disso reduz o ruído ambiente e os custos de energia com o funcionamento total com o sistema de controle térmico EVGA. Se sobrar saídas de energia elétrica da fonte de alimentação ou slots (encaixes para placas) na placa-mãe, deve-se comprar mais equipamentos para aproveitar ao máximo o potencial da mineradora; ou seja, montar outra placa-mãe com mais placas de vídeos para utilizar os watts sobrando ou comprar mais placas de vídeos (e, dependendo da necessidade, outra fonte de alimentação) para não deixar ociosos os slots da placa-mãe.

- http://br.evga.com/Products/ProductList.aspx?type=10&family=Power+Supplies&chipset=1600+Watts.

Existem **calculadoras** *on line* que auxiliam na verificação do **consumo de energia elétrica**:

- http://images10.newegg.com/BizIntell/tool/psucalc/index.html?name=Power-Supply-Wattage-Calculator;

- http://outervision.com/power-supply-calculator.

O segundo passo, para a mineração GPU (*Graphics Processing Unit* ou Unidade de Processamento Gráfico, também chamado de chip gráfico), é definir a **placa de vídeo** (*video board* ou *video card*). Deve-se preferir a placa de vídeo que use menos conectores de energia elétrica, que tenha o menor consumo de energia elétrica, que seja mais silenciosa, que seja mais bem refrigerada e que tenha o maior rendimento (processamento) possíveis. Deve-se optar pelas placas de vídeo com DDR5; já as com DDR3 devem ser evitadas, pois são antigas, consomem mais energia elétrica e possuem menos potência. Deve-se, ainda, preferir a que tenham melhor refrigeração; desse modo, deve-se rejeitar as que tiverem menor quantidade de *coolers* (ventoinhas ou ventiladorzinhos). O montante total da energia elétrica que uma placa gráfica consome é chamado de TDP - *Thermal Design Power* (Energia Térmica de Projeto). Normalmente esse valor é determinado em W

(Watts) e serve para indicar a quantidade máxima de energia que um sistema de refrigeração deve dissipar (espalhar e retirar). É aconselhável optar por um processador e uma placa de vídeo com o valor de TDP mais baixo; vez que quanto menor o TDP, menor será o aquecimento e, consequentemente, menor será a necessidade de refrigeração. ACP - *Average CPU Power* (Potência Razoável da CPU) é encontrada nas especificações de processadores AMD. Diferente do TDP, o valor do ACP serve para fornecer um valor médio da potência gerada pelo processador em uso no cotidiano. Esse valor serve para que o próprio processador monitore o quanto de energia está sendo dissipada para que, quando necessário, um *overclock* possa ser realizado. A verificação é realizada através de uma comparação entre o ACP e o TDP, o que possibilita à CPU aumentar a frequência sem que seja preciso medir a temperatura.

As **marcas de placas de vídeo** mais conceituadas são MSI (https://br.msi.com/), ASUS (https://www.asus.com/br/), Gigabyte (http://br.gigabyte.com/), Saphire (http://www.sapphiretech.com/), Powercolor (http://www.powercolor.com/br/), PNY (https://www.pny.com/), Zotac (https://www.zotac.com/br/pt) e XFX (http://xfxforce.com/).

A placa de vídeo AMD (http://www.amd.com/pt-br) possui uma arquitetura melhor que a NVIDIA (http://www.nvidia.com.br/); o que a torna a melhor opção para mineração GPU. Entretanto, apesar de que a placa de vídeo **Nvidia GeForce GTX 1050 Ti** (chip Pascal GP107, GPU clock 1290, GPU turbo 1392, 4 GB de memória GDDR5 e 7 Gbps de velocidade de memória) pode não ser a solução mais poderosa para a mineração, o interessante dela é seu menor consumo de energia elétrica (limite de TDP de 75W).

- http://www.nvidia.com.br/graphics-cards/geforce/pascal/br/gtx-1050.

Já a **EVGA GeForce GTX 1080 GAMING ACX 3.0** (http://br.evga.com/articles/01007/evga-geforce-gtx-1080/) possui o processador gráfico Pascal da NVIDIA, tecnologia de resfriamento EVGA ACX 3.0 e área de contato de cobre maiores para um funcionamento ainda mais frio. A ventoinha possui um rolamento esférico duplo num motor de

extremo baixo consumo, gerando maior fluxo de ar com menos energia e desbloqueando potência adicional à GPU; também possui curva e pás otimizadas para uma performance mais silenciosa. Possui processador com 2560 Núcleos CUDA, *clock* básico de 1607 MHz, *clock* aumentado de 1733 MHz, 8192 MB de memória GDDR5X, *clock* da memória de 10000 MHz e barramento PCI-E 3.0.

Outra opção, substitutiva ou complementar, é a utilização de **ASIC USB**. Existem vários modelos de equipamentos mineradores para serem conectados em portas USB: Sapphire Miner, The 21 Bitcoin Computer, Bitmain Antrouter R1, ASICMiner Block Erupter, GekkoScience Compac USB Stick Bitcoin Miner, Avalon Nano 3 Newest USB Asic Bitcoin Miner, X11 USB ASIC miner, NF1 Nano Fury Bitfury USB ASIC, Antminer USB, etc.

O terceiro elemento da mineração GPU é a **placa-mãe** (*motherboard*). Enquanto que o slot AGP (*Accelerated Graphics Port* ou porta gráfica acelerada) é usado exclusivamente por placas de vídeo, o slot PCI (*Peripheral Component Interconnect* ou interconexão de componentes periféricos) é usado tanto por placas de rede, placas de som, modems PCI, etc. Ainda mais, a tendência atual é que tanto o slot AGP como o slot PCI sejam substituídos pelo padrão PCI Express (*Peripheral Component Interconnect Express* ou Interconexão de Componentes Periféricos Expressa), que oferece mais recursos e possibilidades.

O slot PCI-X é uma evolução do PCI de 64 bit e não se confunde com o slot PCI Express (PCIe ou PCI-EX), que está disponível em vários segmentos: 1x, 2x, 4x, 8x, 16x, 32x, etc. Quanto maior esse número antes da letra x, maior é a taxa de transferência de dados. Enquanto o PCI é um barramento (caminho para transferência de dados onde se pode conectar vários dispositivos ao mesmo tempo, compartilhando este caminho), o PCI Express é uma conexão ponto-a-ponto; isto é, utiliza um caminho exclusivo para se comunicar com o *chipset* da placa-mãe. Por outras palavras, ele não compartilha esta conexão com outro dispositivo. Desse modo, numa placa-mãe com slots PCI padrão, todos esses slots são conectados ao mesmo barramento e, assim, todos eles compartilham o mesmo caminho de dados, causando redução no desempenho caso mais de um dispositivo queira

transmitir dados ao mesmo tempo. Já numa placa-mãe com slots PCI Express, cada slot PCI Express é conectado ao *chipset* da placa-mãe usando uma um caminho dedicado (privativo ou exclusivo); ou seja, que não é compartilhado com os outros slots PCI Express. Controladores de rede, SATA e USB estão normalmente conectados ao *chipset* da placa-mãe através de conexões PCI Express dedicadas. Outro detalhe, o PCI e os outros tipos de slots de expansão utilizam comunicações em paralelo enquanto que o PCI Express é baseado em comunicações em série de alta velocidade. Explica-se. O PCI Express conta com um recurso que permite o uso de uma ou mais conexões seriais (lanes ou caminhos) bidirecionais (pode receber e enviar dados) para transferência de dados. O "x" que segue a descrição do PCI Express se refere ao número de pistas que a conexão usa. Assim, por exemplo, se um determinado dispositivo usa apenas um caminho, então trata-se do barramento PCI Express 1X. Se usa 4 conexões, é o PCI Express 4X e assim por diante. Por fim, as pistas individuais dos slots PCI Express podem ser agrupadas para criar uma conexão mais rápida.

Desse modo, a placa-mãe indicada é aquela com vários slots PCI-E (onde conectar as placas de vídeo), como, por exemplo, a **AsRock H81 Pro BTC da AsRock** (http://www.asrock.com/mb/intel/h81%20pro%20btc/) ou com várias portas USB para usar equipamentos como o USB BitFury e, ainda, se possível, com mais de um soquete para processador. A placa-mãe Asrock H81 Pro BTC possui 6 (seis) slots GPU e 2 (dois) plugs Molex extras para a unidade de fonte de alimentação. Normalmente esse tipo de placa-mãe são as especialmente projetadas para *gamers* (jogadores), *workstations* (equipamentos direcionados a aplicações que exigem muito poder de processamento) ou para computadores servidores ou industriais. Detalhe, slots PCIe x16 são muito mais capazes de transferir grandes volumes de dados por segundo do que slots PCIe x1 e, ainda, exige-se conferir a compatibilidade de encaixe e funcionamento das placas de vídeos pretendidas. Uma observação importante é que as placas mães são pré projetadas para funcionarem apenas com determinados processadores através da especificação (quantidade, formato, espessura e localização) dos furos de encaixe (*socket* ou soquete) para os pinos do processador. Simplificando, ou a placa-mãe utiliza um processador da fabricante Intel ou da AMD. Mas não é só a marca que é restringida, mas também os modelos. Portanto, quanto mais novos os modelos das placas mães, mais novos serão

os processadores compatíveis com elas. E, normalmente, cada vez que se lança um novo modelo de processador, muda-se o formato de seus pinos de encaixe para que só possam ser usados em placas mães novas. Desse modo, o processador usado pode até não ser o mais moderno, mas a placa-mãe deve ser a mais moderna possível (exceto em caso de placa-mãe de servidor ou industrial com vários slots e soquetes, que compensariam o risco); vez que é muito mais fácil substituir o processador do que a placa-mãe com todos os seus encaixes para o monte de periféricos. Detalhe, os novos processadores da Intel e da AMD terão suporte apenas no Windows 10. Os processadores atuais da AMD são da linha FX, todos com soquete AM3+ e TDP de 125w, que não devem ser usados em placas mães com TDP inferior; pois placas mães com TDP inferior ao do processador limitam o seu desempenho.

A placa-**mãe X99 OC Formula/3.1** da ASRock possui 5 slots PCI-E 3.0 x16 e 1 W mini-PCIe, suporta memória máxima de 128 GB (Quad-Channel de 8 slots com 16GB DIMM DDR4 em cada) e é compatível com as placas de vídeo NVIDIA 4-Way SLI e AMD 4-Way CrossFirex. O soquete M.2 Socket suporta módulos M.2 SATA3 de 6Gb/s e M.2 PCI Express módulos até Gen2 x2 10Gb/s. Possui 10 SATA3, 1 SATA Express, 1 Ultra M2 (PCIe Gen3 x4), 1 M2 (PCIe Gen2 x2 & SATA3), 1 USB 3.1 Type-C de 10 Gb/s, 2 USB 3.1 Type-A de 10 Gb/s (suportados pelo pacote ASRock USB 3.1 Card / A+A), 11 USB 3.0 e 6 USB. O soquete do processador LGA2011-3 (X Series OC Socket) adiciona mais pinos para impulsionar o desempenho da CPU e da memória; compatível com os processadores Intel i7 e Xeon 18-Core. Limite de energia elétrica de 1300W. Os processadores AMD com soquete 2011-3, são os seguintes modelos da série G incorporada eBrazos: GET24LFQB12GVE, GET40NFPB22GVE, GET40RFSB12GVE, GET44RFPB12GVE, GET48NGBB22GVE, GET52RGBB12GVE, GET56NGBB22GVE e 100-CG2293.

- http://www.intel.com.br/content/www/br/pt/processors/xeon/xeon-technical-resources.html?wapkw=xeon.

A placa-mãe da **MSI** (https://br.msi.com/Motherboards/), no formato **ATX estendida** (E-ATX - *Extended ATX* [*Advanced Technology Extended*]), nos modelos **X99**A Gaming 9 ACK, X99A Godlike Gaming, X99S Gaming 9 ACK e X99A Xpower Gaming Titanium possuem 5 slots PCI-Ex16 para

placas de vídeo (VIDIA SLI e AMD Crossfire de 4 vias). Suportam processadores Intel Core i7 Extreme Edition para socket LGA 2011-3.

A **MS-98A9 industrial ATX** (http://adek.com/product/ms-98a9-industrial-atx-motherboard/), com *chipset* Intel Q77 Expresso e soquete LGA 1155 (suporta Geração 3 do Intel Core i3, i5 e i7), possui 5 slots PCI de 32 bits, 1 slot ISA e 1 slot PCIe x16, 1 slots PCIe x4, 5 controladores SATA (2 x SATA 3, 3 x SATA 2), 4 x USB 3.0, 8 x USB 2.0, 6 portas COM (5 x RS-232, 1 x RS232 / 422/485), 1 LPT, PS / 2 e 1 x slot ISA (Sem suporte DMA para ISA).

A **placa-mãe industrial AIMB-705 da XYZ Informática LTDA** (http://xyzinformatica.com.br/), com soquete LGA 1151 e *chipset* H110 (no i3-6100 tem 3.7 Ghz), possui 5 slots PCI, 1 slot PCIe x4 Gen 2 e 1 slot PCIe x16 Gen 3.

As placas-mães **X9DRG-OTF-CPU e X9DRG-O-PCIE** da Supermicro (https://www.supermicro.com/index.cfm) com soquete LGA 2011, possuem os seguintes slots (X9DRG-O-PCIE): 8 PCI-E 3.0 x16, 2 PCI-E 3.0 x8 (no slot x16) e 1 PCI-E 2.0 x4 (no slot x16). Possuem 9x portas USB 2.0 e 8 portas SATA3, SATA2 e 2x.

A **S7079 GM 2 NR do Server Barebones**, linha 4U Rackmount, modelo FT 77 CB 7079 (B 7079 F 77 C V 10 HR) da Tyan (http://www.tyan.com/), possui 8 PCI-E Gen 3 x 16 slots, 2 PCI-E Gen 3 x 8 e 3 PCI-E Gen 2 x 1.

- http://www.tyan.com/cn/Barebones_FT77CB7079_B7079F77CV10HR.

A **GA-990FXA-UD3** AM3+ da Gigabyte, possui 7 slots PCI, 4 slots de memória e 8 conexões SATA (http://br.gigabyte.com/products/product-page.aspx?pid=3894#ov).

A **Crosshair V Formula-Z** da ASUS possui 6 slots PCI, 4 slots de memória e 10 conexões SATA (https://www.asus.com/br/Motherboards/CROSSHAIR_V_FORMULAZ/).

A **P8Z77-V LX** da ASUS possui 7 slots PCI, 4 slots de memória e 6 conexões SATA.

- https://www.asus.com/br/Motherboards/P8Z77V_LX/specifications/.

As **North Bridge AMD 970 e South Bridge AMD SB950** da MSI Computer (https://br.msi.com/) fornecem 6 slots PCI, 4 slots de memória e 6 conexões SATA.

A **placa-mãe de servidor S2600CP2** da Intel suporta dois processadores Intel Xeon E5-2600 e 16 DIMMs com 6 slots PCIe Gen3 x8, 8 portas SCU, 2 portas SATA 6Gb e 4 portas SATA 3 GB.

- http://www.intel.com.br/buy/br/pt/product/components/intel-server-board-s2600cp2-403299.

A **Z9PE-D8WS** da ASUS suporta 2 processadores (*Dual Intel Socket*) Xeon E5-2600 e/ou E5-2600 (https://www.asus.com/Motherboards/Z9PED8_WS/specifications/).

A **placa-mãe de servidor S2600WT** da Intel possui dois soquetes de processadores e suporta dois processadores Intel Xeon E5-2600 v4.

- http://www.intel.com.br/content/www/br/pt/motherboards/server-motherboards/server-board-s2600wt.html;
- http://www.intel.com.br/content/www/br/pt/servers/server-board-s2600wt-brief.html;
- http://www.intel.com/content/dam/support/us/en/documents/server-products/server-boards/S2600WT_TPS_R1_4.pdf.

A **Gigabyte** Dual Intel Xeon Haswell Extreme **MD30-RS0** Server Motherboard também possui soquete 2011-3 x2.

- http://b2b.gigabyte.com/products/product-page.aspx?pid=5147&kw=MD30-RS0#ov.

A **X9QRi-F+ da Supermicro** é *quad socket*; ou seja, comporta 4 processadores LGA 2011: suporta os processadores **Intel Xeon E5-4600 v2**

ou E5-4600 (https://www.supermicro.com/products/motherboard/Xeon/C600/X9QRi-F_.cfm).

As placas-mães **Intel Server Board S4600LH2 e S4600LT2** são 4-Socket; ou seja, possuem 4 soquetes de processadores (http://ark.intel.com/pt-br/products/family/43717/4-Socket-Server-Boards).

O *rack* de servidor **RH2288H V3 2U 2CPU da Huawei** (http://thesyn.co.kr/wp/?page_id=12912&ckattempt=1), suporta 2 Intel Xeon E5-2600 e possui até 9 slot PCIe.

- http://e.huawei.com/br/products/cloud-computing-dc/servers/rh-series/rh2288h-v3.

O **servidor HP Proliant Ml350 Gen9** suporta até 2 processadores Intel Xeon E5-2600 v3 ou v4 e possui 9 x PCIe.

- https://www.hpe.com/br/pt/product-catalog/servers/proliant-servers/pip.7271259.html.

O **supercomputador DGX-1 da Nvidia** (http://www.nvidia.com/object/deep-learning-system.html#source=gss) vem com 2 processadores Intel Xeon e com 8 unidades da placa de vídeo Tesla P100 (http://www.nvidia.com/object/tesla-p100.html). Isso tudo resulta em 170 TFLOP/s de performance FP16. No total, o supercomputador consome 3200W.

Sites como http://adrenaline.uol.com.br/produtos/categoria/placa-mae/ permitem comparar diferentes placas-mães. Veja, ainda, o site de pesquisa da Intel: http://ark.intel.com/pt-br/Search/SearchServerSystems?_ga=1.25266872.466984200.1479928559.

A quem prefira, por serem mais baratas, usar várias **pequenas placas-mães Raspberry Pi 3 Modelo B** (https://www.modmypi.com/) conectadas a placa de vídeo e/ou mineradoras USB (USB ASIC Miner) como a BitFury. Mas o processador da Raspberry é pouco potente para minerar Bitcoins. Provavelmente será necessário o uso de adaptadores de PCI para a placa

Raspberry, tal como, por exemplo, o EXP GDC, que é um notebook built-in interface PCI-E X16.

- https://computers.tutsplus.com/tutorials/how-to-create-a-raspberry-pi-bitcoin-miner--cms-20353;
- How to make a Raspberry Pi Bitcoin Mining Rig: https://www.youtube.com/watch?v=kqfj4U9LDMw.

Em quarto são os **conectores**. Um problema comum é o espaçamento entre os slots PCI Express da placa-mãe; ou seja, normalmente não cabem todas placas gráficas juntas nos locais destinados na placa-mãe. Como solução pode-se usar um riser GPU (por exemplo, PCI-E [PCI Express] 16X Riser Card Extender Flex Flexible Extension), que é basicamente um cabo de extensão para um slot PCI Express.

O conector principal da placa-mãe usa um plugue de 24 pinos (o maior plugue encontrado na fonte de alimentação). A maioria das fontes de alimentação permite converter este plugue de 24 pinos em um de 20 pinos (normalmente removendo os pinos extras). O conector EPS12V (de 4 pinos) é usado para fornecer energia elétrica para o processador na placa-mãe, mas pode ser substituído pelo conector EPS12V (de 8 pinos). Pelo fato do EPS12V ter 8 pinos em vez de apenas 4 como o ATX12V, ele é capaz de fornecer mais energia elétrica. Mas nem todas as fontes de alimentação e placas-mães possuem este conector. Portanto, se a placa-mãe e a fonte de alimentação possuírem o EPS12V, este deve ser usado ao invés do EPS12V. Em alguns casos, o conector EPS12V pode ser obtido juntando-se dois conectores ATX12V. As placas-mães que vêm com o conector EPS12V, normalmente estão com metade dele coberto por uma etiqueta adesiva ou uma proteção plástica, induzindo e permitindo usar o conector ATX12V (de 4 pinos) da fonte de alimentação no conector EPS12V (de 8 pinos), apesar de não ser este procedimento recomendado. O uso de compartilhamentos da fiação de fonte energética envolve a análise do tipo de material e bitola do fio utilizado para saber se é o adequado para o caso específico e, ainda, se a demanda (necessidade ou consumo) dos equipamentos estará em conformidade com a respectiva fonte energética compartilhada; ou seja, se não irá ocorrer queda de tensão, de potência ou de amperagem. Numa resistência constante, se aumentar a voltagem a corrente também aumentará.

Já numa potência constante, se aumentar a voltagem a corrente diminuirá. Para que haja a possibilidade de um aumento de potência no equipamento, o material condutor deve ter uma diminuição de resistência; ou seja, aumentar a sua condutância, para que o material empregado consiga suportar, caso contrário ele simplesmente vai derreter. Exemplificando, recorda-se que quando ocorre queda na tensão ou na potência na corrente elétrica ou quando se liga o chuveiro elétrico, as lâmpadas comuns de iluminação sofrem redução de seu brilho; bem como quando há algum vazamento na tubulação ou encanamento, a torneira ou a mangueira d'água sofre queda de pressão e de volume. Portanto, o uso de lâmpadas como teste prévio é uma forma simples para saber se ocorre algum comprometimento (queda) na corrente elétrica (para quem não tem um multímetro ou não saiba usar um). Por óbvio a lâmpada deve ser adequada à voltagem (12v, 5v, etc.) da fiação elétrica que se quer testar, primeiramente com uma, depois com duas, depois com três e depois com quatro lâmpadas. A melhor forma de distribuição (divisão) da corrente elétrica é através de fios paralelos (separados) da mesma fonte; vez que a ligação em série (sequência) compromete a qualidade da corrente elétrica. Um circuito em paralelo tem resistência menor do que um circuito em série; por isso, no primeiro caso a corrente sobre cada componente é maior, bem como a dissipação de energia. Num circuito em série, apesar da corrente ser a mesma, a tensão total se divide entre todos os componentes, ficando mais fraca em todos; já num circuito em paralelo a tensão é a mesma, mas a corrente se divide.

- http://www.pontociencia.org.br/experimentos/visualizar/lampadas-em-serie-e-paralelo/727.

Antes de surgir o conector PEG, as placas de vídeo top de linha usavam conectores periféricos (para alimentar discos rígidos, unidades ópticas, ventoinhas, sistemas de iluminação, etc.) de quatro pinos (conhecidos por Molex) para a alimentação extra; ou seja, além das placas de vídeo estarem conectadas (encaixadas ou espetadas) na placa-mãe e recebendo energia elétrica desta, ainda precisam de uma ligação ou fonte externa de energia elétrica adicional. Atualmente os discos rígidos (HDs) e unidades ópticas usam plugues de alimentação SATA (15 pinos); ou seja, os utilizados nos dispositivos Serial ATA (SATA). É possível converter qualquer plugue de alimentação para periféricos em um plugue de alimentação SATA mediante a utilização de um adaptador. Os conectores de

alimentação auxiliar PCI Express (contendo seis ou oito pinos) são usados para fornecerem mais corrente elétrica para os dispositivos PCI Express, especialmente as placas de vídeo que necessitam de energia extra (algumas exigem dois, três ou quatro cabos conectores de energia elétrica adicional), com o que são conhecidos como PEG - *PCI Express Graphics* (conectores de alimentação para placas de vídeo). Por exemplo, existe o cabo flexível adaptador extensor da Riser.

Cada placa GPU deve ser alocada na placa independente das outras. Com o uso de um adaptador bridge, apesar de perder um pouco de desempenho em mineração, é possível usar placas de diferentes modelos na mesma placa-mãe. Existem os adaptadores de alimentação Add2Psu e Add2Psu-D (http://www.add2psu.com/). Também é possível transformar um plugue de alimentação para periférico em um conector de alimentação para placa de vídeo com a utilização de um adaptador (peça com um padrão ou formato de entrada e outro de saída). Por exemplo, o conector SATA power fornece energia elétrica ao disco rígido, podendo ser de 3,3, 5 ou 12 V. Detalhe, somente não se pode confundir o conector EPS12V com o conector PCI de 8 pinos usado em placas de vídeo top de linha. Também não é recomendável utilizar cabos e adaptadores de tráfego de dados, de vídeo ou de áudio para fins de condução de energia elétrica; vez que o material interno e a espessura do mesmo não são projetados para o tráfego de energia elétrica. Desse modo, dependendo da energia elétrica necessária pela placa de vídeo pode-se utilizar outras saídas adaptadas da fonte elétrica e/ou da placa-mãe; claro que também vai depender da capacidade de *slots* (encaixes fêmeas similares a tomadas onde os plugues de periféricos ou de PCI são conectados) e dos limites tráfego de dados e de energia elétrica da placa-mãe. O problema com conectores de alimentação de 4 pinos Molex não são os próprios conectores, mas os cabos que estão sendo usados, pois eles costumam possuir pouca potência máxima em razão da fina espessura (bitola) ou do material do fio.

O slot x16 PCI-E (PCI Express), que é normalmente utilizado para conectar as placas de vídeo na placa-mãe, é projetado para fornecer até 75 W (Watts) de energia elétrica para a placa de vídeo, embora a maior parte do consumo vem da linha de 12V e a potência máxima normalmente é de até 66W. Por outras palavras, o slot PCI Express 2.0 só fornece até 75 W de energia elétrica para a placa de vídeo, com isso as placas que precisem de

mais energia do que 75 W, irão precisar de conectores especiais de fonte de energia elétrica. Os conectores de 8 pinos dobram essa capacidade; ou seja, fornecem 150 W. Desse modo, se o consumo máximo de energia elétrica da placa de vídeo sobre 12V de um slot PCI-E de 5.5A (66 W), um cabo conetor com fio de bitola 22 AWG (*American Wire Gauge*) e 6 Amps deve ser o suficiente. Mas, quanto mais grosso o fio de energia elétrica, melhor será a condução e menor será o aquecimento. Em caso de dúvida, para conferir se não está sobrecarregando qualquer uma das linhas de fornecimento de energia, o modo mais fácil de verificar é tocar nos cabos e verificar se estão ficando quentes; se não estiverem quentes está tudo bem, mas se estiverem quentes, no mínimo, a bitola e/ou o material da fiação está inferior ao necessário ou está sendo transmitida mais corrente elétrica do que deveria. Similar aos conectores 6 pinos PCI Express, o 6+2 PCI-E (PCI Express) consegue levar até 150 W de energia elétrica para as placas de vídeo. Como os dois pinos adicionais são separados, pode ser usado também em modelos mais antigos. Os pinos adicionais do pino 6+2 conectores PCI-E são os dois são terra e não cabos +12V como normalmente se pensa por aí.

Já se a pessoa pretende realizar mineração CPU, pode-se dispensar os segundo, terceiro e quarto elementos ou acrescentar os *hardwares* infra elencados em combinação aos da mineração GPU.

Na mineração CPU, além da fonte de energia elétrica, deve-se pensar no **processador** (*processor*) com a maior quantidade de núcleos, maior potência (frequência ou velocidade) possível, maior número de *threads* e a maior possibilidade de *overclock*. Entretanto, o que determina a performance do processador é o IPC (Instruções Por Clock ou Instruções Processadas por Ciclo); ou seja, a quantidade de cálculos matemáticos que o processador realiza por ciclo de *clock*. Deste modo, o que importa ou faz a diferença é o resultado da arquitetura do processador. O conjunto (núcleos, cache, *clock*, barramento, etc.) ajudam a melhorar o desempenho, mas não o determinam. Exemplo, o Pentium G4520, que é Dual-Core, é muito mais potente do que o Athlon 5150, que é Quad-Core. Na maioria das vezes, a Intel possui um *design* de chips muito melhor do que a AMD. A Intel possui tecnologias que melhoram o IPC, o consumo e o aquecimento enquanto que os processadores AMD possuem a fama de aquecerem muito mais.

É necessário verificar quais são os processadores que a placa-mãe suporta; ou seja, através da identificação do tipo de *socket* (padrão de pinos de encaixe). Exemplificando, placa-mãe com soquete LGA 1155 só aceita processadores LGA 1155 e placa-mãe de soquete LGA 1150 só aceita processadores LGA 1150. Outros processadores podem até encaixar na placa-mãe, mas não significa que são compatíveis. Não existe uma equivalência ou padrão entre os pinos dos processadores Intel e AMD.

Em sites como o http://br.gigabyte.com/products/main.aspx?s=42 é possível conferir quais são as placas-mães com determinado tipo de *socket* (ou soquete). Além do soquete existe o *chipset* que identifica a placa-mãe; assim um mesmo soquete pode ter vários *chipsets*. Por exemplo, o soquete 1155 da Intel possui os *chipsets* Z77, H77, B75, Z68, Q67, P67, H67, H61 e B65. Nas descrições dos processadores costumam ter os *chipsets* compatíveis.

- http://www.intermedia.pt/processadores.htm;
- http://www.techtudo.com.br/listas/noticia/2016/03/conheca-todos-os-soquetes-e-os-processadores-compativeis-da-intel-e-amd.html.

No site http://br.gigabyte.com/products/main.aspx?s=42 é possível pesquisar placas-mães de acordo com o soquete e o *chipset*.

Os **processadores com 4.00 GHz** (Gigahertz) são o Intel Core i7-4790K com Socket LGA 1150 (e no turbo são, 4.4 Ghz) e o AMD FX-8350 com socket AM3+ (no turbo são 4.2 Ghz). Já na função turbo, o AMD FX-8370E (com *socket* AM3+) alcança 4.3 GHz e o Intel Core I7-6700k (com *socket* LGA 1151) 4.2 GHz. O Intel Core i7-4790K atinge 4.4 Ghz com o Max Turbo; já o AMD FX-9590 Octa Core Black Edition (exige *socket* AM3+) atinge 5.0 GHz no TurboCore (dispensando assim *overclock*) enquanto o AMD FX-9370 Octa Core Black Edition (com *socket* AM3+) atinge 4.7GHz no Max Turbo. O Intel Core i7-6950X (com 10 núcleos, 20 *threads* e *socket* LGA 2011-v3) já atingiu 5.7 GHz no *overclock*. Já o Intel Xeon E5-2602 v4 consegue 5.1 GHZ no *clock* normal; mas estará disponível apenas através de certos OEMs - *Originals Equipment Manufacturers* (Fabricantes Originais do Equipamento). Cada processador traz um sensor que mede o consumo de

energia do chip em tempo real, pode até não ser um dado extremamente correto, mas é bem aproximado do consumo real. *Softwares* de diagnóstico de *hardware* (como o HWiNFO - https://www.hwinfo.com/) conseguem extrair essa informação. O programa CPUZ (http://www.cpuid.com/softwares/cpu-z.html), um pouco inferior que o HWiNFO, fornece informações sobre processador, placa mãe, memória e placa de vídeo. Também existe o *software* Aida64 (https://www.aida64.com/).

- https://versus.com/es/intel-core-i7-4790k-vs-amd-fx-8350-black-edition;
- https://versus.com/es/amd-fx-8350-vs-intel-core-i7-4770k;
- https://versus.com/es/amd-a4-3400-vs-intel-core-i3-3220;
- https://versus.com/es/amd-fx-9590-vs-intel-core-i7-4770k;
- https://versus.com/es/amd-fx-9590-vs-intel-core-i7-4790k;
- https://versus.com/es/amd-fx-9590-vs-intel-core-i7-5960x;
- https://versus.com/es/intel-xeon-e5-2609-vs-intel-core-i7-3770;
- https://versus.com/es/intel-core-i7-3770-vs-intel-core-i7-2600k;
- http://adrenaline.uol.com.br/2016/07/15/44437/analise-processador-intel-core-i7-6950x/;
- http://ark.intel.com/pt-br/products/family/79318/Intel-High-End-Desktop-Processors#@Desktop.

Sabendo fazer o *overclock*, o aumento da potência pode ser fabuloso:

"No ano passado noticiamos que um *overclocker* chinês tinha alcançado 5.2 GHz com o processador Core i7-6700K da arquitetura Skylake, utilizando um sistema de nitrogênio líquido (LN2) e uma configuração baseada em uma placa-mãe MSI Gaming Z170 e memórias DDR4. Lembrando que por padrão o *clock* base do Core i7-6700K é de 4 GHz podendo chegar a 4.2 GHz graças ao Turbo Boost. Pois bem, agora outro chinês está envolvido em um novo *overclock* com esse processador, porém com ganhos ainda mais expressivos. O *overclocker* Chi Kui Lam conseguiu através de uma bela dose de nitrogénio líquido e uma configuração com uma placa-mãe ASRock Z170, 4 GB de RAM G-

Skill DRR4 (Trident Z), SSD Plextor de 256 GB e uma fonte Antec de 1300 Watts, elevar a frequência do 6700K para a casa dos 7 GHz, mais precisamente 7025,66 Mhz. Durante os testes Lam desabilitou três dos quatro núcleos da CPU. Esse recorde acabou por superar a dupla alemã Dancop e Der8auer que tinham conseguido 7007,85 MHz com este mesmo processador." (http://www.hardware.com.br/noticias/2016-02/chines-supera-os-ghz-em-overclock-com-processador-core-i7-6700.html).

Saiba mais sobre os últimos lançamentos de processadores:

- http://olhardigital.uol.com.br/noticia/intel-anuncia-novos-processadores-para-pcs-veja-o-que-muda/65048;
- https://www.windowsteam.com.br/intel-anuncia-seus-novos-processadores-de-7a-geracao-para-computadores/;
- https://tecnoblog.net/205679/intel-core-kaby-lake-anuncio/;
- http://www.techtudo.com.br/listas/noticia/2016/12/veja-quais-foram-os-melhores-processadores-de-2016.html.

A **memória RAM** (ou temporária) é outro item a ser considerado. Enquanto que a mineração do Bitcoin não exige nada de memória RAM, a mineração do Litecoin exige muita memória RAM (ou VRAM). Deste modo, deve-se preferir uma placa-mãe que suporte o máximo possível de memória RAM. Deste modo, a placa-mãe escolhida é que vai definir o tipo de memória RAM a ser comprada.

Por fim, como existe moedas que utilizam a quantidade de **espaço no disco rígido** (ou HD - *hard disk*), este é outro item a ser considerado. A Burst (https://www.burst-team.us/), por exemplo, utiliza o algoritmo de prova de capacidade (espaço em disco rígido). A Seagate (http://www.seagate.com/br/pt/), por exemplo, fornece HD interno de até 10 TB (Terabyte). Já os modelos de 8 TB são: Enterprise Capacity 3.5 HDD 8 TB 4Kn SATA SED-FIPS ST8000NM0145, Enterprise Capacity 3.5 HDD 8 TB 4Kn SAS ST8000NM0065 e Enterprise Capacity 3.5 HDD 8 TB 4Kn SAS SED-FIPS ST8000NM0125. Já como HD externo (*Expansion Desktop*), a Seagate possui até 5 TB.

- http://www.seagate.com/br/pt/enterprise-storage/hard-disk-drives/enterprise-capacity-3-5-hdd-10tb/.

Outro detalhe é a **refrigeração**. Geralmente os processadores já vêm com *coolers* para ficarem em cima deles na placa-mãe; mas estes normalmente não são adequados para *overclock*. Ainda mais, geralmente a Intel possui melhor resfriamento do que a AMD. Desse modo, a utilização de um watercooler pode ser necessária. Se o watercooler estiver fora do orçamento, uma possibilidade inferior e mais barata é o AIR cooler; mas não dão conta de *overclock* extremamente forte. No site http://www.frostytech.com/top5_lowprofile_heatsinks.cfm existe uma relação de dissipadores de calor (*heatsink*) de acordo com o processador.

Não se pode esquecer da **placa de rede** se esta não for *onboard* (vir na placa-mãe) ou se a existente na placa-mãe não tiver boa velocidade de conexão. Não se recomenda o uso de Wi-Fi porque a velocidade de conexão deste e limitada e está sujeita a várias interferências e intermitências (oscilações). Por óbvio que a conexão à Internet deve ser de banda larga; ainda mais que algumas moedas utilizam a largura de banda como um fator determinante para permitir a mineração ou para determinar o peso do "voto" na rede.

Em relação aos *softwares* necessários e suas respectivas configurações, tais informações são adquiridas dos sites e dos anúncios de divulgação das moedas digitais. E, ainda, existem os fóruns correlatos para pesquisar orientações adicionais ou perguntar mesmo.

INTRODUÇÃO ÀS ALTCOINS

Para a maioria das pessoas, o mercado de moedas criptografadas se resume ao Bitcoin. Mas o Bitcoin é apenas uma das centenas, senão milhares, de moedas matemáticas que podem ser usadas em transações digitais.

Altcoins é a denominação empregada para designar as demais moedas digitais ou criptográficas além do Bitcoin; que é considerado o primeiro experimento que deu certo (mas não a primeira moeda digital ou eletrônica), servindo, portanto, de marco histórico, divisor de águas ou referência. Em razão do sucesso do Bitcoin, muitas pessoas não só tentam copiar, imitar ou repetir o sucesso obtido pelo Bitcoin, mas, também, tentam aprimorá-lo ou aperfeiçoá-lo. Desse modo, muitas altcoins utilizam o código fonte do Bitcoin (ou de alguma altcoin) com algumas pequenas alterações ou simples ajustes, tais como, por exemplos, aumentando a velocidade da confirmação da transação, aumentando o anonimato (sigilo ou privacidade), melhorando a segurança, alterando o mecanismo de consenso, mudando o algoritmo de hash (criptografia), alterando o tamanho dos blocos, modificando a quantidade máxima de moedas a serem emitidas, modificando as recompensas dos mineiros, implementando funções e utilidades novas, etc. Entretanto, existem outras que são totalmente feitas do zero; ou seja, não se aproveitaram do código fonte do Bitcoin e nem de alguma altcoin.

Em resumo, as altcoins são milhares de alternativas existentes ao Bitcoin. Aliás esse é o significado de seu nome. A palavra altcoin é uma abreviação da expressão "alternative to bitcoin" (alternativa ao bitcoin).

Quando Henry Ford lançou, em 1927, o automóvel Ford T não foi o primeiro automóvel, mas foi o primeiro que se popularizou. Mas o fato de Henry Ford ter sido o primeiro industriário a aplicar a montagem em série de forma a produzir em massa automóveis em menos tempo e a um menor custo, não eternizou seu veículo Ford T como o automóvel perfeito e eterno; nem sua linha de montagem ficou congelada no tempo. Por outras palavras, muitas outras empresas se basearam na linha de montagem e no automóvel de Henry Ford para desenvolverem procedimentos e veículos cada vez melhores. Com as criptomoedas não pode ser diferente. Não se pode ficar

preso ao passado. O Bitcoin não foi a primeira moeda digital, mas tão somente foi a primeira delas a ser popular. De igual modo, muitos profissionais estudaram o Bitcoin e o aperfeiçoaram cada vez mais. Portanto, tal como quando a Apple lança nova versão do Iphone, as altcoins sérias foram lançadas em contínuo aperfeiçoamento daquilo que a rede Bitcoin não pode proporcionar.

A maioria das altcoins são praticamente clones ou bifurcações (*forks*) do bitcoin com pequenas mudanças, tais como, por exemplos, quantidade de unidades da moeda a serem emitidas, tamanho do bloco, quantidade de transações por bloco, tempo de confirmação ou velocidade de validação, grau de dificuldade, algoritmo de hash (*hashing algorithm*) ou algoritmo de criptografia (*encryption algorithm*), método de consenso ou prova de sistema (*system proof*), recompensa dos mineiros, taxas, etc.

Tal como as ações nas bolsas de valores, as moedas criptográficas possuem um código ou sigla para facilitar sua identificação e distinção das outras moedas digitais.

Outras altcoins foram e são desenvolvidas totalmente do zero; ou seja, não são derivadas do bitcoin e nem baseadas nela.

Nos sites http://cryptocoin.cc/, http://saldigi.info/coins/, https://coinmarketcap.com/, http://com-http.us/ e http://coinwik.org/Main_Page é possível conseguir rapidamente as informações básicas ou essenciais das altcoins ("Cryptocoin" ou "Crypto-Currency").

No site https://minkiz.co/coin/ constam 2.681 altcoins listadas.

Com o *CoinMarketCap* (http://coinmarketcap.com/all/views/all/), é possível acompanhar em tempo real, várias criptomoedas mais movimentadas nas últimas 24 horas. Confira, ainda: http://www.coinwarz.com/cryptocurrency.

Confira mais cotações em:

- http://coinmarketcap.com/currencies/;
- http://coincap.io/#/;
- http://cryptoindex.com/#/;
- https://chainz.cryptoid.info/;
- http://www.cryptocoinrank.com/ ou https://www.cryptopia.co.nz/Exchange;
- http://cryptmarketcap.com/;
- https://www.cryptojam.com;
- https://www.cryptocoincharts.info/coins/info.

Obviamente existem aplicativos para *smartphones* e *tablets* com essa função, como, por exemplo, o *Bitcoin Checker*.

- http://www.bitcoinnews.com.br/bitcoinbrasil/como-acompanhar-a-cotacao-do-bitcoin-e-de-outras-altcoins-pelo-seu-celular/.

Uma altcoin pode tanto usar a *Blockchain* do Bitcoin como possuir seu próprio livro de registro das cadeias de blocos:

- https://chainz.cryptoid.info/ltc/;
- http://cryptochainer.com/dir/;
- https://bchain.info/coins/;
- http://ltc.blockr.io/.

O site https://chainz.cryptoid.info/ monitora as *blockchains* das moedas: 1CR - 1CRedit, 2FLAV - FlavorCoin V2, 2GIVE, 42 - 42 coin, 808 - 808 coin, AC - AsiaCoin, ARCO - AquariusCoin, ARCH - ARCHcoin, ARG - Argentum, ATX - Atomic Coin, B3 - B3Coin, BAY - BitBay, BCR - Bitcredit, BEE2 - Beecoin v2, BITB - BitBean, BLITZ - Blitzcash, BLK - BlackCoin, BLOCK - BlockNet, BLZ - BlazeCoin, BOLI - BolivarCoin, BSD - BitSend, BSTY - GlobalBoost-Y, BTA - BATA, BTCR - BitCurrency, BVC - BeaverCoin, BXT - BitToken, BYC - Bytecent, CANN - CannabisCoin, CARBON - CarbonCoin, CBX - CryptoBullion, CCN - CannaCoin, CLUB - ClubCoin, CNO - Coino, CPAY - ColoradoPay, CPC -

Capricoin, CRYPT - CryptCoin, CRW - CROWN, CSH - Cashout, CURE - CureCoin, DASH - Dash, DBG - Digital Bullion Gold, DGC - DigitalCoin, DIME - Dimecoin, DMD - Diamond, DOT - Dotcoin, DRZ - Droidz, EC - Eclipse, EFL - e-Gulden, EMD - Emerald, ENRG - EnergyCoin, ENT - Eternity, ERC - Europecoin, ETHS - Ethereumscrypt, FAIL - FailCoin, FIRE - FireCoin, FLT - FlutterCoin, FSX - Frost, FUEL - Fuelcoin, FUNK - The Cypherfunks, GAM - Gambit, GAP - GapCoin, GBT - GameBet Coin, GCR - Global Currency Reserve, GLC - GlobalCoin, GLD - GoldCoin, GOLF - Golfcoin, GRE - GreenCoin, GRN - Granite, GRS - Groestlcoin, GRT - Grantcoin, GUN - Guncoin, HIRE - Bithire, HYPER - Hyper, I0C - I0Coin, ICN - iCoin, INFX - Influx, IOC - I/O Coin, ION - Ion, IXC - iXcoin, J - JoinCoin, JBS - Jumbucks, JWL - Jewels, KARM - Karma, LANA - Lanacoin, LEA - LeaCoin, LIR - LetItRide, LTC - Litecoin, LXC - Librexcoin, MND - MindCoin, MOJO - Mojocoin, MOON - Mooncoin, MPC - MobilePayCoin, MST - MustangCoin, MTR - MasterTraderCoin, MUE - MonetaryUnit, NAV - NavCoin, NBX - NetBit, NCL - Nucleus, NEOS - Neoscoin, NEVA - Nevacoin, NOBL - Noblecoin, NXC - Nexxus Coin, OCTO - OctoCoin, OK - OKCash, OMC - Omicron, OPAL - OpalCoin, PAK - PakCoin, PEX - PosEx, PIGGY - Piggycoin, PIN - Piron, PINK - PinkCoin, PKB - ParkByte, PND - PandaCoin, POT - PotCoin, PPC - PeerCoin, PR - Prototanium, PSB - Pesobit, PX, RADS - Radium, RBY - Rubycoin, REGA - REGA, RIC - Riecoin, RUB - Rubblecoin, SAR - SARcoin, SCRT - SecretCoin, SDC - ShadowCash, SHA - SHACoin, SILK2 - SilkCoin2, SLR - SolarCoin, SMBR - Sembro Token, SNRG - Synergy, SPR - SpreadCoin, STK - Stakecoin, STRAT - Stratis, STV - SativaCoin, SWIFT - BitSwift, SWING - Swing, SYS - SysCoin 2.0, TAJ - TajCoin, TALK - BTCTalkCoin, TECH - TechCoin, TES - Teslacoin, TROLL - Trollcoin, TRUMP - TrumpCoin, TRUST - TRUSTplus, TUBE TubeCoin, TX - Transfercoin, UNIQ - UniQredit, UNO - Unobtanium, URO - UroCoin, VCN - Vcoin, VIA - ViaCoin, etc.

Em sites de cotações, como, por exemplo, o CoinMarketCap (http://coinmarketcap.com/), é possível conferir as altcoins que estão sendo valorizadas. O site https://cryptolization.com/ também traz a cotação de várias altcoins; já o site https://https://bx.in.th/ permite a comparação da cotação do Bitcoin com algumas altcoins e o http://bravenewcoin.com/bitcoin#Trading-Pairs permite comparar a cotação

do Bitcoin nas *exchanges* pelo mundo. Pelo site https://chainz.cryptoid.info/ é possível verificar o valor de mercado (*market cap*) da criptomoeda. Veja, ainda, o site https://www.cryptopia.co.nz/Exchange?market=POP_LTC.

Existem cerca de 3.000 (três mil) moedas criptográficas. Muitas delas foram abandonadas, encerradas, extintas ou estão inativas. Muitas nem sequer chegaram a ser lançadas (inauguradas). Outras tantas foram criadas por pura diversão. Centenas foram feitas precipitadamente ou sem muito critério, estando fadadas ao fracasso. Portanto, dessas milhares de moedas digitais, apenas algumas dezenas ou, no máximo, somente cerca de uma centena pode ser considerada ou levada em conta.

Quando consultamos o site http://cryptodatabase.net/coins-all haviam 1.623 criptomoedas catalogadas. Já no site http://abc.20coin.com/ constavam 1.206 moedas enquanto que no site http://coinmarketcap.com/all/views/all/ haviam apenas 709 moedas. http://com-http.us/, por sua vez, possui apenas 468 moedas digitais no seu acervo. O site http://altcoindb.com/ possui a descrição sumária de 362 criptomoedas. Nos sites http://listofaltcoins.com/ e https://cryptofolio.info/ também existem algumas dezenas catalogadas.

Através do site http://cryptocoin.cc/search.php e possível pesquisar altcoins através dos critérios ano de lançamento (*year launched*), bifurcação de determinada moeda criptográfica (*forked from*), número total de moedas (*total number of coins*), mecanismo de consenso (*consensus mechanism*), algoritmo de hash (*hashing algorithm*), plataforma (*platform*) e situação (*status*). Ressalta-se que o site não possui todas as altcoins catalogadas. Já o site https://www.cryptopia.co.nz/CoinInfo/?coin=DOT possui uma tabela dinâmica de classificação e avaliação de algumas dezenas de criptomoedas através da classificação ou avaliação (*rating*), algoritmo de hash (*algo*), método de consenso (*network*), situação (*status*), etc.

Sites como http://cryptocoin.cc/, http://saldigi.info/coins/ e https://minkiz.co/coin/ apresentam as descrições resumidas de várias moedas digitais.

Das criptomoedas consideráveis falaremos em outros capítulos, por ora, infra discorreremos das que não são sérias, não interessam para

investimentos, foram mal elaboradas, fracassaram ou estão destinadas ou ao fracasso ou a serem restritas a um pequeno grupo de aficionados.

Para chamar a atenção de determinadas comunidades, algumas moedas estão ligadas a locais reais; tais como, por exemplos, alguns **países**, nações ou continentes: AmericanCoin, Amsterdamcoin, Antarctic, Arcticcoin, Argcoin, AsiaCoin, AustraliaCoin, Bolivarcoin, CaliforniaCoin, Canadacoin, CanadaEcoin, Dubaicoin, EmiratesCoin, EuroCoin, Eurasiancoin, 020Londoncoin, Britcoin, eUK, FIFAWCcoin, Floripacoin, Sambacoin, Floridacoin, Guarany, GermanyCoin, Galleon, Hawaiicoin, Hongkongcoin, Incakoin, ItalyCoin, iTcoin, Latinocoin, Lusocoin, MalibuCoin, Mazacoin, Navajocoin, NewYorkCoin, Nigeria Coin, Palestinecoin, CryptoEscudo, Russiacoin, SpainCoin, TexasCoin, VegasCoin, VikingCoin, Unitary Status Dollar eCoin, KlondikeCoin, Quebecoin, etc. De modo semelhante, ao utilizar nomes de localidades, é fazer **referência a alguma moeda física** (Pennies, Doubloons, Florin, PesetaCoin, BitPeso, Dollarpounds, Benjamins, Unitary Status Dollar eCoin, etc.).

Algumas criptomoedas são direcionadas a **grupos específicos**. Assim, por exemplos, a HamRadioCoin foi criada especificamente para os radialistas amadores (https://bitcointalk.org/index.php?topic=675564.0); para os amantes de tacos de todo o mundo, a TacoCoin (https://bitcointalk.org/index.php?topic=601960 e http://tacocoin.net/); para os fãs de ficção científica, em especial a franquia Jornada nas Estrelas, a SciFiCoin (https://cryptocointalk.com/topic/1062-startrek-new-coins/), denominado Sistema de Crédito GPL (*Gold Pressed Latinum*) da Federação dos Planetas Unidos (*Empire Darsek UFC - United Federation of Planets Credit System*) e do Império Klingon (*KED - Klingon Empire Darsek*). E até mesmo uma moeda chamada BumbaCoin (http://bumbacoin.com/), distribuída automaticamente entre os *trolls* que postam xingamentos jamaicanos em fóruns de Bitcoin.

De modo semelhante, vendedores de drogas, maconha, sexo, armas, negociantes no mercado negro e criminosos em geral, por possuírem dificuldades ou problemas com os sistemas tradicionais de pagamento, podem contar com moedas destinadas aos seus objetivos ou grupos:

HempCoin, PotCoin, Cannacoin, CannabisCoin, GroinCoin, TitCoin, WankCoin, Sexcoin, Cannacoin, CannabisCoin, CannabisDarkcoin, CocaineCoin, Fetishcoin, Porncoin, PolishSexIndustry, Stripecoin, TittieCoin, Vaginacoin, etc.

Sobre as referências à maconha, confira o verbete 420 do Glossário.

Exemplos de altcoins de fãs de **animais** são: Albatrosscoin, Beecoin, Birdcoin, Blackdragoncoin, Butterflycoin, CatCoin, CateDoge, Cheetahcoin, CorgiCoin, CowCoin, CrimeaCoin, ElephantCoin, EagleCoin, Fishcoin, FoxCoin, GorillaBucks, Hamstercoin, Jaguarcoin, Kittehcoin, Koalacoin, Lioncoin, Mammothcoin, Mouse, Pigcoin, NewPiggycoin, Orcacoin, Pandacoin, Penguincoin, Ponycoin, PorkCoin, RabbitCoin, Rhinohorncoin, Sharkcoin, Slothcoin, Snakecoin, Tigercoin, Waspcoin, Whalecoin, Wolfcoin, Zebracoin, etc.

Algumas altcoins **exóticas** são: MemeCoin, Zombiecoin, Vampirecoin, TheSmurfsCoin, HODOR, RobotSex Nickels, 007Coin, 666Coin, Evilcoin, Aliencoin, AnaLCoin, AngryBirdCoin, Antibeebacoin, BananaBits, Choclatecoin, Coca-ColaCoin, ComedyGold, CrimeCoin, DraculaCoin, Ebolacoin, FacebookCoin, FailCoin, FakeCoin, Fairbytecoin, Flashcoin, Football2014coin, Fuckcoin, Frycoin, Gabencoin, GhostCoin, Godzillacoin, Gollumcoin, Hamburgercoin, Homocoin, Hodorcoin, Starkcoin, ILoveYoucoin, Klingon Empire Darsek, Federation Credits, Kiwicoin, LadyCoin, Lemoncoin, Lemurcoin, Leprocoin, Lycancoin, MadCowCoin, MetalMusiccoin, MothManCoin, Mugatucoin, Ninja Doge, Nosferatu, Nuggets, OhMyGod, Pikachu Coin, Piratecoin, Potatocoin, Predatorcoin, PunisherCoin, Rambo coin, Norris Coin, Scamcoin, Scarfacecoin, ShitsandGiggles, Skynetcoin, Spoderman, Steroids, StoopidCoin, Superherocoin, Teddycoin, Tomato, Trafficcoin, Transformerscoin, Trollcoin, VodkaCoin, Watcoin, Baconbits, BatCoin, Beercoin, Caponecoin, etc. Existem muitas moedas satíricas pelo fato de muitas querer imitar o sucesso que a Dogecoin fez ao ser uma moeda de diversão; bem como pequenos grupos fazerem por pura diversão mesmo.

Algumas são feitas em **homenagens ou sátiras a artistas ou celebridades** (Biebercoin, MileyCyruscoin, Murraycoin, Gangnamstylecoin,

CoinyeCoin, Einsteinium, EdisonX3, TeslaCoin, etc.) e outras para **fins políticos ou eleitorais**, como as moedas para o Aécio Neves (Aeciocoin), Dilma Rousseff (Dilmacoin), Donald Trump (Trumpcoin), JFK (JFKcoin), Obama (Obamacoin), Won (CryptoWon), Kim (Kimcoin e KimJonguncoin), etc.

Também existem as ideias mirabolantes ou surreais. SpaceBIT anunciou ao mundo, no final de 2014, a sua ambição de ser a primeira empresa espaço descentralizado através do lançamento de vários nano-satélites em órbita. Entretanto, após os primeiros dois meses de 2015, não se ouviu mais sobre a SpaceBIT. A equipe por trás da SpaceBIT começou uma nova empresa *blockchain*, a BlockVerify (http://www.blockverify.io/), na qual todos os esforços foram focados e, assim, o projeto SpaceBIT foi totalmente engavetado desde março de 2015.

Outras altcoins foram feitas com **temas religiosos** ou em forma de tributo, oferenda, louvor ou adoração a divindades: Godcoin, Jesuscoin, B1bl3Coin, Praycoin, IsisCoin, Aegiscoin, Bitraam, Cthulhu Offerings, Demonic, Freemasoncoin, Masoncoin, Illuminati, Goat, Horuscoin, IslaCoin, Ottomancoin, JupiterCoin, Kraken, Witchcoin, Thorcoin, Zeuscoin, Buddhacoin, Atheistcoin, BeastCoin, etc.

A ConfessionCoin (https://bitcointalk.org/index.php?topic=606996.0) é uma espécie de confissão online de pecados com a consequente venda de indulgência (perdão dos pecados).

O que se pretendeu com as citações desses exemplos acima é demonstrar que é um erro transmitir a ideia contrária a universalidade. O dinheiro deve ser algo internacional, sem fronteiras e sem acepção de pessoas; ou seja, não pode ter etnia, sexo, religião, time de futebol, zoação, etc. Alguns exemplos de moedas digitais que utilizaram expressões sinônimas para dinheiro, mas sem dar interpretação restritiva são: Gold Coin, Diamond, Emerald, Graincoin, ValueCoin e CREDS. E alguns nomes simples, mas criativos que dão ênfase na universalidade são Terracoin, SolarCoin e Union Coin. Já GPUCoin e PowerCoin utilizaram expressões que simplificam e resumem o que é uma moeda digital.

Uma forma didática de compreender as altcoins é fazendo uma analogia com as denominações ou instituições religiosas da Cristandade ou do Cristianismo. Comparemos o Bitcoin com a igreja Católica e as altcoins com as igrejas evangélicas ou protestantes. Deste modo, ante as falhas, erros, corrupção, máfia, desvirtuamento e adulterações no projeto da primeira denominação ou entidade, reformistas deixaram a organização para criarem outras objetivando expurgar essas máculas, defeitos, problemas, burocracia, elitização e corrupção; e, assim, sucessivamente o processo se repete dano origem a milhares de novos grupos onde, teoricamente, cada vez mais evoluem, se adaptam, se aperfeiçoam e se modernizam. De modo similar também pode-se usar os partidos políticos com exemplo; vez que devido a divergências, insatisfações ou escândalos, correligionários deixam partidos para criarem um novo partido. Diante disso, não adianta simplesmente saber que existe algo lá fora em algum lugar; tem que saber quais são. E, para isto, não basta somente saber os nomes; é necessário saber sua doutrina, credo, filosofia e objetivos. Explica-se. O nome pode ser bonito, sugestivo, atrativo, comovente, agradável, carismático, sedutor e enganador, com o que pode dar uma falsa ideia, impressão ou compreensão do que se trata de fato. E, inclusive, conferir se seus ideais são realmente cumpridos ou se trata de um engodo, estelionato, fraude, enganação, hipocrisia ou armadilha. Por outras palavras, em razão de que, na maioria das vezes, a teoria é muito diferente da prática e existe muita hipocrisia no mundo, deve-se analisar se a pessoa por trás da entidade, grupo, movimento, instituição, entidade, organização, associação, fundação ou empresa é alguém sincero aos seus ideais e se dedica à teoria que professa ou se trata de um golpista. Urge, portanto, distinguir os lobos, falsos profetas, falsos messias, falsos cristos (ungidos), falsos santos, falsos deuses... das pessoas com o Espírito Santo (portadores e praticantes da verdade).

Diante disso, em teoria nas criptomoedas, quanto mais nova ela for, mais moderna, avançada, eficiente, prática, segura, rápida e multitarefa será; vez que a tecnologia envolvida está em constante aprimoramento.

Entretanto, não se pode confundir uma moeda criptográfica avançada, moderna ou de última geração como sendo sinônimo de sucesso ou de aceitação popular. Tal como os produtos, serviços, ideias e políticos em geral, normalmente não é o melhor que prevalece, mas sim o que consegue a

preferência, aprovação ou gosto popular. Por outras palavras, o fato de algo ter grande conhecimento, aceitação, aprovação ou uso popular não significa que seja o melhor, correto ou mais moderno. E, para conseguir a aceitação popular, não basta simplesmente fazer propaganda (divulgar, anunciar ou fazer campanha). A propaganda não é algo simples, pois deve-se analisar o veículo (meio, forma, instrumento ou local) utilizado, os horários envolvidos nessa divulgação, as pessoas (quantidade e tipo) atingidas por esses anúncios, o linguajar utilizado (deve ser facilmente assimilado pelos destinatários, mas sem insinuar que são idiotas ou analfabetos), o conteúdo (se as ideias, conceitos, objetivos, imagens, desenhos, símbolos, cores, sons, música, pessoas, animais, atores, artistas... são atrativos, chamativos, carismáticos, convincentes, comoventes, cativadores ou sedutores), a quantidade de vezes em que se repete (reitera, reforça, recorda, relembra, etc.) a propaganda, etc.

Para sermos mais claros, como em qualquer propaganda, muitas vezes o que mais importa é quem é o “garoto propaganda”; ou seja, quem é a pessoa que apresenta o produto ou serviço ao público. Outro fator bastante decisivo é quem são as pessoas, empresas, marcas, entidades e/ou instituições por trás e quais são as que usam, patrocinam, recomendam e/ou fazem parte. Em terceiro, a questão de poder exibir-se em público (ostentar, chamar a atenção ou causar inveja) ou dar conotação de ser um VIP (*Very Important Person* ou "pessoa muito importante") também pode ser algo determinante; vez que a maioria das pessoas gosta de exibir aos outros o que possui (veículos de luxo, joias, roupas de grife, etc.). Desse modo, se determinado produto, serviço ou evento (show, festa, jogo de futebol, boate, clube, restaurante, barzinho, excursão, parque de diversões, viagem, roupa, calçado, bolsa, mochila, boné, caneta, chaveiro, brinquedo, game, etc.) somente pode ser pago através de uma criptomoeda específica, isso dá a conotação de exclusividade, seletividade ou elitização que agrada ao ego, a vaidade e o fetiche de muitas pessoas. Por fim, a adoção de certas filosofias, conceitos, credos, valores, princípios e estilos de vida também ajuda a arregimentar muitos adeptos. Assim, por exemplo, a promessa de que parcela dos rendimentos serão revertidas em prol (benefício) de determinada causa, pesquisa ou entidade pode cativar determinados grupos. Entretanto, também pode ocorrer o efeito inverso; ou seja, pode causar repulsa, aversão,

indignação ou reprovação social generalizada (exemplos: pedofilia, estupro, racismo, etc.).

Especificadamente sobre tecnologia e informática, normalmente para se conseguir conquistar as pessoas, em razão da maioria delas não entenderem praticamente nada do assunto, deve traduzir a informação para o linguajar dessas pessoas. Por outras palavras, deve-se utilizar um linguajar mais simples e acessível sem evidenciar ou transparecer que as está tratando como se fossem crianças ou retardados mentais. Explica-se. Se empregar um linguajar simples demais, além das pessoas não entenderem direito, acabará ofendendo essas pessoas. Portanto, deve-se usar uma linguagem mediana (da pessoa média ou comum). Mas somente fazer a pessoa saber da existência, conhecer e entender do produto ou serviço não é o suficiente. É necessário que a pessoa não só veja utilidade, proveito, comodidade, satisfação, prazer e/ou valor naquilo, mas que tenha a concepção que aquilo é importante, prioritário, essencial, vital, indispensável, viciante e/ou valioso. Em resumo, deve-se coexistirem ambos requisitos para que o produto ou serviço se viralize (vire febre, moda ou mania) entre a sociedade. Desse modo, por exemplo, apesar de muitas pessoas saberem que investir em bolsa de valores dá muito dinheiro, por acharem complicado, muitos não investem e nem sequer procuram pesquisar (estudar) a respeito. Já, por outro lado, produtos ou serviços que proporcionam prazer, diversão, vício ou ostentação social por si mesmos, conseguem despertar o interesse a tal ponto que as pessoas pesquisam, estudam e se informam a respeito. Mas criptomoedas não possuem esse efeito sobre a maioria das pessoas.

Deste modo, em síntese, tanto para criar uma altcoin, como para analisar qual criptomoeda pode prosperar ou "cair no gosto popular" ou, ainda, simplesmente para poder convencer as pessoas sobre determinada criptomoeda, deve-se abordar sobre:

- O **nome** dado à moeda desperta interesse, simpatia ou atração ou, pelo contrário, resulta em reprovação, rejeição, aversão, discórdia ou polêmica? É um termo simples demais, infantil, imbecil, criminoso, zombador, popular ou elitista? O nome dá a ideia de ser algo universal ou restringe-se à uma determinada comunidade, povo, grupo específico, minoria, fãs, adeptos de

alguma crença ou filosofia, ativistas, continente, país, idioma, etnia, sexo, religião, partido político ou time de futebol? Trata-se de um nome sério ou alguma brincadeira, zombaria, homenagem, propaganda, adoração ou fã clube? Por exemplo, a moeda Gaycoin (http://www.gaycoin.online/) é destinada aos gays, lésbicas, bissexuais, transexuais e simpatizantes da comunidade GLBT.

- O **logotipo** (símbolo gráfico) é bem elaborado e trabalhado ou aparenta ser um trabalho rudimentar ou infantil? O emblema denota seriedade, inspira credibilidade ou sugere tratar-se de brincadeira, diversão, golpe ou um trabalho mal feito?

- Os **objetivos e/ou ideais** (causas, filosofias, intenções, etc.) pretendidos e/ou defendidos podem agradar ou desagradar grande parcela das pessoas?

- A **tecnologia** empregada possui alguma inovação, evolução ou aprimoramento ou não passa de mero e simples clone de outra altcoin sem qualquer diferencial, qualidade ou vantagem? Trata-se de um simples *fork* (bifurcação) de outra altcoin ou possui implementos consideráveis?

- A **segurança** existente no aplicativo e nas suas interações e transações realizadas;

- A **proteção** contra manipulações, conluios, fraudes e estelionatos;

- O grau de **anonimidade, privacidade ou sigilo** envolvidos, os quais variam de pessoa para pessoa de acordo com o uso que se faz e/ou as intenções que se tem;

- A possibilidade de realizar atos e/ou de adquirir determinados bens, produtos e/ou serviços que **não são disponíveis ou possíveis de outra forma**;

- Os **idiomas** utilizados; ou seja, em termos globais deve-se, no mínimo, empregar o inglês norte americano e, em questão regional, deve também utilizar o português brasileiro, pois a enorme maioria dos brasileiros não sabem inglês. Parece óbvio, mas existem altcoins que usam somente o chinês ou o russo. Portanto, quanto mais idiomas a moeda utilizar, melhor será;

- A **apresentação gráfica** (aparência) é de suma importância para poder cativar as pessoas; principalmente as leigas em informática e/ou tecnologia;

- O **grau de dificuldade ou de facilidade do manuseio** do software e/ou do sistema. Deste modo, quanto mais uma pessoa simples e leiga poder usar facilmente, melhor será;

- Existência, ou não, de uma **comunidade de desenvolvedores**. Algum tempo depois do lançamento, deve haver uma comunidade ativa de pessoas não só de apoio à moeda, mas em desenvolvimento de serviços relevantes para ela. Um exemplo, disso foi a EZCoin;

- A existência, ou não, e a respectiva qualidade do **suporte técnico** disponibilizado aos usuários, vez que muitos irão ter dúvidas e dificuldades por mais que existam manuais, tutoriais e vídeo aulas. Inclusive existem altcoins que nem sequer wikis ou FAQs possuem;

- O **país de origem ou da sede** do sistema e/ou software, pois pode ser um país de grande rejeição ou descrédito internacional;

- O idioma ou idiomas nos quais foi feito o **anúncio de divulgação** da moeda, bem como os locais onde foi divulgada;

- A existência, ou não, de ***exchanges*** **no país**;

- Quais são os **sistemas operacionais** utilizados, pois urge utilizar, no mínimo, sistemas populares como, por exemplos, o Android e o Windows em suas várias versões, sob pena de se "tornar uma ilha" ou "uma panelinha"; ou seja, um grupinho fechado, exclusivo e elitizado. Deste modo, altcoins que somente funcionam ou mineram em diferentes sistemas não tendem a prosperar;

- Os **equipamentos** que podem executar (rodar) o software e/ou sistema. Quanto mais os aparelhos poderem ser domésticos, simples e/ou velhos, melhor será para fins de popularização;

- Existir, ou não, **mineração** e se o garimpo é democraticamente acessível ou privilegia os ricos;

- Ocorrência, ou não, de **escândalos** envolvendo os proprietários, promotores, coordenadores, desenvolvedores, colaboradores e demais envolvidos na criação ou administração da criptomoeda;

- **Quem são as pessoas**, empresas, marcas, entidades e/ou instituições **por trás** e quais são as que usam, patrocinam, recomendam e/ou fazem parte;

- **A moeda é tão boa quanto o desenvolvedor**. O desenvolvedor é ativo e experiente? Ele parece ter uma boa noção de como o sistema funciona? Os parâmetros escolhidos para a sua moeda são realistas? Exemplos: Fastcoin possuía parâmetros insustentáveis; Gamecoin foi lançada com logotipo e abreviatura de outra moeda; Megacoin teve o cliente inicial liberado usando as mesmas portas do Litecoin;

- A **idoneidade e/ou credibilidade** das pessoas envolvidas no projeto;

- A existência, ou não, de **prévio debate e/ou desenvolvimento comunitário**;

- O **grau de repercussão** do anúncio do lançamento da moeda nos fóruns correlatos e quais foram as críticas feitas. Além de anúncios de novas moedas, os fóruns específicos (exemplos: https://bitcointalk.org/, https://cryptocointalk.com/, https://bitcointalk4.com/, https://freebitcointalk.org/, https://www.cryptopia.co.nz, https://www.reddit.com/, http://www.talkgold.com/forum/, https://forum.gethashing.com/, https://bitco.in/forum/, https://allcryptotalk.com/index.php, https://nxtforum.org/, etc.), contêm avisos sobre fraudes e moedas mal planejadas, conhecidas como “shitcoins” (moedas de merda);

- A existência, ou não, de um **site**;

- A **comodidade e/ou praticidade** proporcionada(s) ante a falta de tempo, aversão a burocracia e, até mesmo, a preguiça da maioria das pessoas somada a operatividade em qualquer lugar e a qualquer instante por 24 (vinte e quatro) horas por dia em todos os dias da semana, sem sábados, domingos ou feriados;

- A **economia** envolvida ao não ter que pagar tributos, tarifas bancárias, taxas de *exchanges*, emolumentos de cartórios, honorários de intermediários, etc.;

- Configurar uma **fonte de renda extra** que não possui dias, horários, tempo, velocidade, quantidade e/ou valores mínimos pré-estabelecidos para poder ser realizada;

- Consistir numa **rede social** onde qualquer um pode fazer parte, sem necessitar dispender de algum valor significativo ou de comprar algo de valor considerável, e sendo possível se relacionar com qualquer outra pessoa do mundo e de qualquer classe social;

- Possibilitar com enorme facilidade, rapidez e eficácia a união de esforços para a realização de **atividades sociais**, assistenciais, beneficentes, filantrópicas, humanitárias, institucionais, ideológicas e de caridade;

- Representar uma **revolução empresarial** semelhante a revolução industrial (transição dos processos artesanais e de manufatura para os maquinários) e à implantação da linha de montagem ou de produção nas fábricas (fabricação maciça através do procedimento de cada trabalhador fazer apenas um parte do processo ao invés de todos os trabalhadores fazerem o processo por completo) pelo fato de desburocratizar, aprimorar, agilizar, dinamizar, acelerar e economizar em diversas rotinas, trabalhos e procedimentos nas indústrias, empresas e comércios em geral;

- Tratar-se de uma **tendência evolutiva** em constante e rápida implantação, com o que, em questão de tempo, se tornará algo comum e que não a compreender ou utilizar será equivalente a um analfabeto, tal como hoje quem não sabe usar um computador ou um caixa eletrônico.

Além da questão da viabilidade ou possibilidade de prosperidade da altcoin, deve-se também considerar a possibilidade de tratar-se de um golpe. Assim, por exemplo, a *Premine* (mineração prévia) injustificada ou exagerada é sempre suspeita; principalmente quando o beneficiário é o desenvolvedor ou a conta destinatário é de seu controle. Na Phenixcoin, por exemplo, ocorre uma *premine* com uma explicação nada convincente. Já na ZenithCoin, metade de todas as recompensas do bloco vão para o desenvolvedor sem qualquer explicação ou justificativa. Outro fator suspeito é a quantidade desproporcional de moedas geradas no lançamento; fato denominado de *instamining*. Essa prática permite que, depois de lançada, o desenvolvedor extraia rapidamente uma enorme quantidade de moedas, antes mesmo das outras pessoas começarem a minerar. O Feathercoin, por exemplo, teve 3 milhões de moedas gerados durante as primeiras 24 horas. Já a Mincoin teve 868.000 moedas minadas durante as primeiras três horas e a Bitbar, 2000 moedas minadas durante as 3 primeiras horas. O GoldCoin, por sua vez, teve uma enorme quantidade de moedas geradas durante as primeiras poucas horas. Aliadas a essa prática pode ocorrer do software ou das configurações disponibilizadas aos demais mineradores darem erro; ou pior, nem sequer ser disponibilizado o software e suas configurações. Um exemplo disso foi o Mincoin, que não teve nenhum cliente após semanas do

lançamento. Outra técnica é o lançamento da moeda em algum canto remoto da Internet, que também possibilita a mineração prévia e exclusiva (sem concorrência ou competição) por seus desenvolvedores, para somente depois divulgar em outro site mais popular como, por exemplo, o BitcoinTalk (fórum oficial). Exemplo disso, foi a Pennies, que foi liberada num site desconhecido antes de fazer uma publicação no fórum BitcoinTalk.

TabTrader (https://play.google.com/store/apps/details?id=com.tabtrader.android) é um terminal de negociação gratuito para bitcoins e altcoins nas bolsas: Mercado Bitcoin, Coinbase, Bitstamp, ANXPRO, HitBtc, BTC-E, BTCChina, Huobi, Kraken, ItBit, Bitbay, Cryptsy, Bter, Bitfinex, Clevercoin, Bitmarket, Gatecoin, Bleutrade, QUOINE, Bittrex, BL3P (Bitonic), Poloniex, Bitcurex, EXMO, CEX.IO, Vaultoro, Mercado Bitcoin (Brasil). O app negocia várias moedas criptografadas: Bitcoin (BTC), Litecoin (LTC), Dogecoin (Ducal), Ripple (XRP), Namecoin (NMC), Stellar (STR), Ethereum (ETH), Lisk (LSK) e outras. Gráficos rápidos de preços, com indicadores técnicos e negociação diretamente a partir dos gráficos. Inclui um *widget* (ferramenta). Alertas de preços por meio notificações. *Feed* (alimentação) de notícias do Reddit, Coindesk, Bitcoin Magazine e outras fontes de notícias sobre moedas digitais.

Bitcoin Ticker Widget (https://play.google.com/store/apps/details?id=st.brothas.mtgoxwidget) exibe e monitora as atuais taxas de câmbio de Australian BTC Markets (Mercados BTC australianos), Bit2c, Bitbay, Bitcashout, Bitcoin Indonesia, Bitcoin.co.id, Bitcoin.de, Bitcurex, Bitex, Bitfinex, bitFlyer Lightning, Bitkonan, bitmarket.pl, Bitmex, Bitonic, Bitpay, Bitstamp, bitstar, Bitx, Bl3p, BTC China, BTC-e, Canadianbitcoins, Cex.io, Clevercoin, Coinbase, CoinBR, Coindesk, Coinfloor, FoxBit, GDAX, Gemini, Gocelery, Hitbtc, Huobi, Igot, ItBit, Kraken, Lakebtc, Localbitcoins, Okcoin, Paymium, Poloniex, Quadrigacx, Quoine, SatoshiTango, Therocktrading e Zyado.

O Bitcoin & Altcoin Trader (https://play.google.com/store/apps/details?id=com.coinigy.app), por sua vez, realiza o câmbio com mais de 50 criptomoedas. Já o Bitcoin Checker (https://play.google.com/store/apps/details?id=com.mobnetic.coinguardian) monitora os preços de mais de 80 criptomoedas. O aplicativo Altcoin Price

Ticker (Bitcoin) (https://play.google.com/store/apps/details?id=com.ericturnerdev.Altcoin) informa o preço atual e outras informações para mais de 200 criptomoedas. O Blockfolio Bitcoin/Altcoin App (https://play.google.com/store/apps/details?id=com.blockfolio.blockfolio), por sua vez, oferece gerenciamento completo para mais de 800 criptomoedas. Através dele, além das cotações, sabe-se demais informações sobre o mercado de moedas digitais. Possui o recurso de alerta de quando ocorre alterações no preço. CoinWatch - Crypto Coin Prices (https://play.google.com/store/apps/details?id=com.papenam.coinwatch) fornece o preço de mais de 1000 moedas.

Já o também aplicativo para smartphone, zTrader Altcoin/Bitcoin Trader (https://play.google.com/store/apps/details?id=co.bandicoot.ztrader) efetua troca de centenas de moedas digitais em 17 bolsas diferentes. O aplicativo Crypto Prices All-in-One (https://play.google.com/store/apps/details?id=com.coinprices.allexchanges), por sua vez, trabalha com 24 intercâmbios de criptomoedas. Já o Boilr (https://play.google.com/store/apps/details?id=mobi.boilr.boilr) suporta mais de 70 bolsas.

O App (aplicativo) para celular, Crypto Currency converter (https://play.google.com/store/apps/details?id=com.squids.converter) é um conversor de mais de 350 moedas. Já o BitCoin Free Converter (https://play.google.com/store/apps/details?id=es.cryptoexchange.account) realiza a conversão das 100 melhores criptomoedas e dezenas de moedas convencionais. Também possui recurso de alarme. O Cryptonator (https://play.google.com/store/apps/details?id=com.aev.cryptonator), por sua vez, é uma calculadora de taxa de câmbio e conversão de mais de 500 moedas digitais e moedas fiduciárias. Por fim, o Digital Currency Widget (https://play.google.com/store/apps/details?id=org.phauna.litecoinwidget) fornece os preços para mais de 17 moedas de troca e mais 500 moedas digitais.

LISTA DE ALTCOINS: ANÚNCIOS

A lista infra não é exaustiva (completa), mas meramente exemplificativa e visa fornecer além dos detalhes de cada moeda, de como foi apresentada ou lançada e quais foram as reações e críticas do seu lançamento; também fornece os únicos links que costumam existir mesmo depois que a moeda foi encerrada, extinta, descontinuada, desativada ou morta. Por padrão (em regra ou na maioria das vezes) nesta listagem não se informam os endereços ou sites oficiais em razão da volatilidade, instabilidade e efemeridade dos mesmos. Deste modo, esta relação visa dar conhecimento dos nomes e siglas das moedas já existentes e que já existiram; bem como dos links para maiores informações para fins de estudos prévios para o lançamento de uma nova altcoin, para fins de prevenção contra *scams* e de análises de viabilidade das moedas atuais ante o estudo de quais foram os erros, falhas e defeitos das altcoins que fracassaram. Esta listagem, ainda, serve para complementar as demais citações das altcoins existentes e que já existiram; mas, nem assim, esgotamos a citação de todas as altcoins. Detalhe, para fins de estudo ou uso de códigos fontes, deve-se consultar repositórios como o GitHub (https://github.com/).

- 0NE (0NE): https://bitcointalk.org/index.php?topic=637108.0 e https://cryptocointalk.com/topic/12670-0ne-0ne-information/;
- 1Coin (ONE): https://bitcointalk.org/index.php?topic=820302.0 e https://cryptocointalk.com/topic/20085-1coin-one-information/;
- 1Credit (1CR): https://bitcointalk.org/index.php?topic=645124.0 e https://cryptocointalk.com/topic/10515-1credit-1cr-information/;
- 2chcoin (2CH): https://bitcointalk.org/index.php?topic=398100.0;
- 13Coin (13): https://bitcointalk.org/index.php?topic=519705.0 e https://cryptocointalk.com/topic/8399-3-27pre-ann1313coin-anti-asic-1-premine-safe-ipo-scrypt-jane-nfactor-rare/;
- 21coin (21): https://bitcointalk.org/index.php?topic=426853.0 e https://cryptocointalk.com/topic/3564-21coin-21-

information/;

- 23 Skidoo (CHAO): https://bitcointalk.org/index.php?topic=526224.0 e https://cryptocointalk.com/topic/8154-23-skidoo-chao-information/;
- 42 Coin (42): https://bitcointalk.org/index.php?topic=399658.0, https://bitcointalk.org/index.php?topic=1502028.0 e https://cryptocointalk.com/topic/2874-42-information/;
- 66coin (66): https://bitcointalk.org/index.php?topic=431696.0 e https://cryptocointalk.com/topic/3699-66coin-66-information/;
- 84 Coin (84): https://bitcointalk.org/index.php?topic=421286.0 e https://cryptocointalk.com/topic/3458-84-information/;
- 365Coin (365): https://bitcointalk.org/index.php?topic=492311.0 e https://cryptocointalk.com/topic/6893-365coin-365-information/;
- 500Coin ou FiveHundredCoin (FHC): https://cryptocointalk.com/topic/10629-500coin-fhc-information/;
- 666coin (666): https://bitcointalk.org/index.php?topic=585912.0 e https://cryptocointalk.com/topic/10743-666coin-666-information/;
- ÆØÅ (AEOA): https://bitcointalk.org/index.php?topic=767759.0;
- Abundance (ABC2): https://bitcointalk.org/index.php?topic=682939.0 e https://github.com/AbundanceSource;
- AceCoin (ACE): https://bitcointalk.org/index.php?topic=714025.0 e https://cryptocointalk.com/topic/13776-acecoin-ace-information/;
- Aces: https://bitcointalk.org/index.php?topic=1568436.0;
- AchillesCoin: https://bitcointalk.org/index.php?topic=712128.0 e https://cryptocointalk.com/topic/13769-achillescoin-ach-information/;
- ACoin: https://bitcointalk.org/index.php?topic=761818.0 e https://github.com/acoin-project/acoin;
- Acros: https://bitcointalk.org/index.php?topic=415829.0;
- ActiveCoin: https://bitcointalk.org/index.php?topic=602982.0;

- AditiCoin (XAD): https://bitcointalk.org/index.php?topic=635232.0 e https://cryptocointalk.com/topic/12283-aditicoin-xad-information/;
- Adzcoin (ADZ): https://bitcointalk.org/index.php?topic=1292875.0 e http://adzcoin.org/;
- AecioCoin: https://bitcointalk.org/index.php?topic=575797.0 e https://minkiz.co/coin/3581/;
- Aegis (AGS): https://bitcointalk.org/index.php?topic=679580.0 e https://cryptocointalk.com/topic/13129-aegis-ags-information/;
- Aeoncoin: https://bitcointalk.org/index.php?topic=641696.0 e http://www.aeoncoin.org/;
- Aerocoin: https://bitcointalk.org/index.php?topic=660938.0, https://github.com/aeromasterdev/AeroCoin e http://www.aerocoin.io/;
- AeroME (AM): https://bitcointalk.org/index.php?topic=955204.0 e https://minkiz.co/coin/5106/;
- AidBit (AID): https://bitcointalk.org/index.php?topic=683317.0 e https://cryptocointalk.com/topic/13520-aidbit-aid-information/;
- AidCoin (AID): https://bitcointalk.org/index.php?topic=637962.0;
- Aiden (ADN): https://bitcointalk.org/index.php?topic=558414.0, https://cryptocointalk.com/topic/10682-aiden-adn-information/ e http://aidencoin.github.io/;
- Aimcoin (AIM): https://bitcointalk.org/index.php?topic=635015.0 e https://github.com/Aimcoin;
- AirCoin (AIR): https://bitcointalk.org/index.php?topic=476383.0 e https://cryptocointalk.com/topic/5886-aircoin-air-information/;
- AirDropCoin: https://bitcointalk.org/index.php?topic=518662.140 e https://bitcointalk.org/index.php?topic=518662.0;
- AlboCoin (ALB): https://cryptocointalk.com/topic/12157-albocoin-alb-information/ e https://github.com/albocoin/albocoin;
- AlcoHoin (ALC): https://bitcointalk.org/index.php?topic=426299.0 e https://cryptocointalk.com/topic/3536-alcohoin-

alc-information/;

- AlexiumCoin: https://bitcointalk.org/index.php?topic=1148013.0 e https://github.com/ALEXIUMCOIN;
- AliCoin: https://bitcointa.lk/threads/pre-ann-ali-alicoin-im-not-the-greatest-im-the-double-greatest.260129/;
- Aliencoin (ALN): https://bitcointalk.org/index.php?topic=407460.0 e https://cryptocointalk.com/topic/3108-aliencoin-aln-information/;
- Alipaycoin (ALI): https://bitcointalk.org/index.php?topic=868675.0 e https://cryptocointalk.com/topic/25997-annalialipaycoinx142015happy-new-year/;
- AllAgesCoin: https://bitcointalk.org/index.php?topic=386973.0;
- AllahCoin: https://cryptocointalk.com/topic/829-allahcoin-the-islamic-cryptocoin/;
- AllianceCoin (AAC): https://bitcointalk.org/index.php?topic=647376.0 e https://cryptocointalk.com/topic/12251-alliancecoin-aac-information/;
- Alphacoin (ALF): https://bitcointalk.org/index.php?topic=230868.0, https://cryptocointalk.com/topic/560-alphacoin-alf-information/ e https://alphacoin.wordpress.com/;
- AlphaOmegaCoin (AOC): https://bitcointalk.org/index.php?topic=407285.0 e https://cryptocointalk.com/topic/2039-alphaomegacoin-aoc-information/;
- Altcoin (ATC): https://cryptocointalk.com/topic/5104-altcoin-alt-information/;
- AlterEgoCoin: https://bitcointalk.org/index.php?topic=528925.0;
- AltroCoin: https://bitcointalk.org/index.php?topic=434209.0;
- AmazoniaCoin (AMZ): https://bitcointalk.org/index.php?topic=663285.0 e https://minkiz.co/coin/4352/;
- AmberCoin: https://bitcointalk.org/index.php?topic=944408.0, https://cryptocointalk.com/topic/14851-ambercoin-amber-information/ e http://ambercoin.info/;

- AmericanCoin (AMC): https://bitcointalk.org/index.php?topic=219165.0 e https://cryptocointalk.com/topic/388-americancoin-amc-information/;
- AmigaCoin (AGA): https://bitcointalk.org/index.php?topic=539974.0 e https://cryptocointalk.com/topic/12040-amigacoin-aga-information/;
- AmKoin (AMK): https://bitcointalk.org/index.php?topic=464885.0 e https://cryptocointalk.com/topic/4692-amkoin-amk-information/;
- Android Token (ADT): https://bitcointalk.org/index.php?topic=440353.0 e https://cryptocointalk.com/topic/1039-android-tokens-adt-20-updated-information/;
- AngelCoin (ANG): https://bitcointalk.org/index.php?topic=681111.0 e https://cryptocointalk.com/topic/13165-angelcoin-ang-information/;
- AngryBirdsCoin: https://bitcointalk.org/index.php?topic=634850.0 e https://bitcointalk.org/index.php?topic=634850.msg7075202#msg7075202;
- Anherocoin (AHC): https://bitcointalk.org/index.php?topic=393546.5 e https://cryptocointalk.com/topic/2698-anherocoin-ahc-information/;
- Animecoin (ANI): https://bitcointalk.org/index.php?topic=423339.0 e https://cryptocointalk.com/topic/3707-animecoin-ani-information/;
- Anoncoin (ANC): https://bitcointalk.org/index.php?topic=227287.0, https://cryptocointalk.com/topic/522-anoncoin-anc-information/ e https://anoncoin.net/;
- AnonymousCoin (XAC): https://bitcointalk.org/index.php?topic=648489.0 e https://cryptocointalk.com/topic/11814-anonymouscoin-xac-information/;
- AntarcticCoin (ACC): https://bitcointalk.org/index.php?topic=610049.0 e https://cryptocointalk.com/topic/11486-antarcticcoin-acc-information/;
- Antimatter (ANT): https://bitcointalk.org/index.php?topic=460112.0 e https://cryptocointalk.com/topic/4920-antimatter-ant-information/;

- ApeCoin (APE): https://bitcointalk.org/index.php?topic=375938.0 e https://cryptocointalk.com/topic/2265-apecoin-ape-information/;
- ApexCoin (APEX): https://bitcointalk.org/index.php?topic=686403.0 e https://cryptocointalk.com/topic/13274-apexcoin-apex-information/;
- AphroditeCoin (APH): https://bitcointalk.org/index.php?topic=511160.0 e https://cryptocointalk.com/topic/8012-aphroditecoin-aph-information/;
- ApolloCoin: https://bitcointalk.org/index.php?topic=744924.0 e https://github.com/apollocoin/apollocoin;
- AppCoin (APP): https://bitcointalk.org/index.php?topic=475160.0 e https://cryptocointalk.com/topic/6121-appcoin-app-information/;
- Applecoin (APC): https://bitcointalk.org/index.php?topic=337782.0 e https://cryptocointalk.com/topic/1577-applecoin-apc-information/;
- AptCoin (APT): https://bitcointalk.org/index.php?topic=743731.0 e https://cryptocointalk.com/topic/14319-aptcoin-apt-information/;
- ARCHcoin - https://bitcointalk.org/index.php?topic=831777.0 e https://www.archcoin.co/;
- Arcoin (AR): https://bitcointalk.org/index.php?topic=696243.0 e https://cryptocointalk.com/topic/13425-arcoin-ar-information/;
- ArgCoin (ARC): https://bitcointalk.org/index.php?topic=278452.0 e https://cryptocointalk.com/topic/1048-argcoin-arc-information/;
- Argentum: https://bitcointalk.org/index.php?topic=231524.0 e https://cryptocointalk.com/topic/50052-argentum-arg/#entry226415;
- Arkcoin (ARK): https://bitcointalk.org/index.php?topic=518299.0 e https://cryptocointalk.com/topic/8198-arkcoin-ark-information/;
- Arkenstone (ARS): https://bitcointalk.org/index.php?topic=608482.0 e https://cryptocointalk.com/topic/11269-arkenstone-ars-information/;

- ArmoredCoin: https://bitcointalk.org/index.php?topic=474788.0;
- ArtsyCoin: https://bitcointalk.org/index.php?topic=956061.0 e https://bitcointa.lk/threads/ann-contest-artsycoin-coin-icon-design-challenge-with-prizes.420055/;
- AsapCoin (ASAP): https://bitcointalk.org/index.php?topic=705494.0 e https://cryptocointalk.com/topic/13894-asapcoin-asap-information/;
- Ascentcoin (ASCE): https://bitcointalk.org/index.php?topic=611790.0 e https://cryptocointalk.com/topic/11336-ascentcoin-asce-information-added-anon/;
- ASDCoin (ASD): https://bitcointalk.org/index.php?topic=724181.0 e https://cryptocointalk.com/topic/13986-asdcoin-asd-information/;
- Asiacoin (AC): https://bitcointalk.org/index.php?topic=595999.0 e https://cryptocointalk.com/topic/10458-asiacoin-ac-information/;
- Asiccoin (ASC): https://bitcointalk.org/index.php?topic=292501.0 e https://cryptocointalk.com/topic/1183-asiccoin-asc-information/;
- AssPennies: https://bitcointalk.org/index.php?topic=554718.0 e https://cryptocointalk.com/topic/9574-ann-asspennies-now-youve-got-the-upper-hand-no-premine/;
- Astrocoin (ASR): https://bitcointalk.org/index.php?topic=425367.0 e https://cryptocointalk.com/topic/3496-astrocoin-asr-information/;
- Atheistcoin (ATH): https://bitcointalk.org/index.php?topic=654656.0 e https://cryptocointalk.com/topic/12219-atheistcoin-ath-information/;
- AtomCoin: https://cryptocointalk.com/topic/2372-atom-ato-information/ e https://github.com/zombo/atomcoin-new;
- Atomic Trade: https://bitcointalk.org/index.php?topic=395192.0;
- Auroracoin (AUR): https://en.wikipedia.org/wiki/Auroracoin;
- AurumCoin (AU): https://bitcointalk.org/index.php?topic=793502.0 e https://cryptocointalk.com/topic/18228-

aurumcoin-au-information/;

- AustraliaCoin: https://bitcointalk.org/index.php?topic=550198.0, https://bitcointalk.org/index.php?topic=538580.0 e https://github.com/auscoins/AustraliaCoin;
- AustroCoin: https://bitcointalk.org/index.php?topic=629175;
- AVCoin (AV): https://bitcointalk.org/index.php?topic=613049.0 e https://cryptocointalk.com/topic/11395-avcoin-av-information/;
- AxioCoin: https://bitcointalk.org/index.php?topic=670286.0;
- AxisCoin: https://bitcointalk.org/index.php?topic=632818.0 e https://cryptocointalk.com/topic/12134-axiscoin-axis-information/;
- Axron (AXR): https://bitcointalk.org/index.php?topic=738534.0 e https://cryptocointalk.com/topic/14458-axron-axr-information/;
- B1bl3Coin: https://bitcointalk.org/index.php?topic=827734.0 e https://cryptocointalk.com/topic/20100-b1bl3coin-powpos-to-be-released-on-november-1-2014/;
- BackPackersCoin (BACK): https://bitcointalk.org/index.php?topic=693973.0 e https://cryptocointalk.com/topic/13383-backpackerscoin-back-information/;
- BaconBits (YUM): https://bitcointalk.org/index.php?topic=400667.0 e https://cryptocointalk.com/topic/2914-baconbits-yum-information/;
- BadCoin: https://bitcointalk.org/index.php?topic=844023.0 e https://cryptocointalk.com/topic/21184-badcoin-bad-information/;
- Badgercoin (BDG): https://bitcointalk.org/index.php?topic=585796.0 e https://cryptocointalk.com/topic/10537-badgercoin-bdg-information/;
- Bancorcoin (BNCR): https://cryptocointalk.com/topic/7859-bancorcoin-bncr-information/ e https://github.com/bancor/bancorcoin;

- Bankcoin (BANK): https://bitcointalk.org/index.php?topic=606388.0 e https://cryptocointalk.com/topic/11248-bankcoin-bank-information/;
- BankNote (BN): https://bitcointalk.org/index.php?topic=633466.0;
- Banksycoin (BSY): https://bitcointalk.org/index.php?topic=684008.0;
- Banx (BANX): https://bitcointalk.org/index.php?topic=813191.0;
- BaseCoin (BAC): https://bitcointalk.org/index.php?topic=289959.0 e https://cryptocointalk.com/topic/1164-basecoin-bac-information/;
- Batcoin (BAT): https://bitcointalk.org/index.php?topic=400753.0 e https://cryptocointalk.com/topic/2943-batcoin-bat-information/;
- BattleCoin (BCX): https://bitcointalk.org/index.php?topic=354612.0 e https://cryptocointalk.com/topic/3081-battlecoin-bcx-information/;
- BawbeeCoin (BAW): https://bitcointalk.org/index.php?topic=520729.0, https://github.com/Bawbeecoin e http://bawbeecoin.org/;
- Bbqcoin (BQC): https://bitcointalk.org/index.php?topic=93437.0 e https://cryptocointalk.com/topic/116-bbqcoin-bqc-information/;
- BctCoin: https://bitcointalk.org/index.php?topic=569997.0 e https://github.com/bctc;
- BDSM: https://bitcointalk.org/index.php?topic=789338.0 e https://cryptocointalk.com/topic/17325-?-?-?-bdsm-fetish-?-?-?/;
- Beaocoin (BEC): https://bitcointalk.org/index.php?topic=300523.0 e https://cryptocointalk.com/topic/1227-beaocoin-bec-information/;
- BeatleCoin (BEA): https://bitcointalk.org/index.php?topic=511571.0 e https://cryptocointalk.com/topic/8525-beatlecoin-bea-information/;
- BeaverCoin (BVC): https://bitcointalk.org/index.php?topic=761269.0 e https://cryptocointalk.com/topic/14774-beavercoin-bvc-information/;

- BeeCoin (BEE e BEE2): https://bitcointalk.org/index.php?topic=601247.0 e https://cryptocointalk.com/topic/5199-beecoin-bee-information/;
- BeerCoin: https://bitcointalk.org/index.php?topic=436419.0 e https://cryptocointalk.com/topic/3728-beercoin-beer-information-2xexchanges-new-ver-643-checkpoints/;
- Belicoin (BELI): https://bitcointalk.org/index.php?topic=460810.0 e https://cryptocointalk.com/topic/5784-belicoin-beli-information/;
- Bellacoin (BELA): https://bitcointalk.org/index.php?topic=437825.0 e https://cryptocointalk.com/topic/3861-bellacoin-bela-information/;
- Bellscoin (BEL): https://bitcointalk.org/index.php?topic=349695.0 e https://cryptocointalk.com/topic/1678-bells-bel-information/;
- Benjamins (BEN): https://bitcointalk.org/index.php?topic=444543.0 e https://cryptocointalk.com/topic/4173-benjamins-ben-information/;
- BernanKoin: https://bitcointalk.org/index.php?topic=375010.0 e https://cryptocointalk.com/topic/2364-bernankoin-a-virtual-virtual-non-digital-coin-being-sold-on-ebay/;
- BestCoin: https://bitcointalk.org/index.php?topic=266439.0 e https://cryptocointalk.com/topic/930-bestcoin-best-information/;
- BetaCoin (BET): https://bitcointalk.org/index.php?topic=321266.0 e https://cryptocointalk.com/topic/1443-betacoin-bet-information/;
- BieberCoin (BRC): https://bitcointalk.org/index.php?topic=636530.0 e https://cryptocointalk.com/topic/11985-biebercoin-brc-information/;
- Bigbangcoin (BBC): https://bitcointalk.org/index.php?topic=716901.0 e https://cryptocointalk.com/topic/14164-bigbangcoin-bbc-information/;
- BigBullion (BIG): https://bitcointalk.org/index.php?topic=715904.0 e https://cryptocointalk.com/topic/14255-bigbullion-big-information/;

- Billaume (BLL): https://bitcointalk.org/index.php?topic=448528.0 e https://cryptocointalk.com/topic/3912-billaume-bll-information/;
- BillionCoin (BIL): https://bitcointalk.org/index.php?topic=374073.0 e https://cryptocointalk.com/topic/2237-billioncoin-bil-information/;
- BilShares (BILS): https://bitcointalk.org/index.php?topic=729068.0;
- BinaryCoin (BIC): https://bitcointalk.org/index.php?topic=383604.0 e https://cryptocointalk.com/topic/2425-binarycoin-announcement/;
- BirdCoin (BRD): https://bitcointalk.org/index.php?topic=496363.0 e https://cryptocointalk.com/topic/6968-birdcoin-brd-information/;
- Bitbar (BTB): https://bitcointalk.org/index.php?topic=196125.0 e https://cryptocointalk.com/topic/112-bitbar-btb-information/;
- BitBay (BAY): https://bitcointalk.org/index.php?topic=850267.0 e https://cryptocointalk.com/topic/21458-annbay-bitbay-decentralized-marketplacesmart-contractsiot-techico-on-bter/;
- BitBean: https://bitcointalk.org/index.php?topic=915650.0 e http://www.bitbean.org/;
- BitBlock (BBL): https://bitcointalk.org/index.php?topic=665159.0 e https://cryptocointalk.com/topic/12777-bitblock-bbl-information/;
- BitBurst (BTB): https://bitcointalk.org/index.php?topic=599570.0 e https://cryptocointalk.com/topic/12665-bitburst-btb-information/;
- BitCash (BCSH): https://bitcointalk.org/index.php?topic=737857.0 e https://cryptocointalk.com/topic/14540-bitcash-bcsh-information/;
- BitCentavo (NBE): https://bitcointalk.org/index.php?topic=636934.0 e https://cryptocointalk.com/topic/11946-bitcentavo-nbe-information/;
- BitcoinDark (BTCD): https://bitcointalk.org/index.php?topic=684090.0 e https://cryptocointalk.com/topic/13343-

bitcoindark-btcd-information/;

- BitCoinFast (BCF): https://bitcointalk.org/index.php?topic=881774.0 e https://cryptocointalk.com/topic/23789-ann-bitcoinfast-bcf-scrypt-powpos-33-million-pow-coins-25-annual-stake/;
- BitCoinNEW (BTN): https://bitcointalk.org/index.php?topic=610673.0 e https://cryptocointalk.com/topic/11332-bitcoinnew-btn-information/;
- BitcoinPlus (XBC): https://bitcointalk.org/index.php?topic=549485.0 e https://cryptocointalk.com/topic/12758-bitcoinplus-xbc-information/;
- Bitcoinscrypt (BTCS): https://bitcointalk.org/index.php?topic=318253.0 e https://cryptocointalk.com/topic/1169-bitcoin-scrypt-btcs-information/;
- BitCoinX11 (BTCX): https://bitcointalk.org/index.php?topic=625769.0 e https://cryptocointalk.com/topic/11714-bitcoinx11-btcx-information/;
- BitDrachma (DRA): https://bitcointalk.org/index.php?topic=729956.0 e https://cryptocointalk.com/topic/14320-bitdrachma-dra-information/;
- Bitgem (BTG): https://bitcointalk.org/index.php?topic=207008.0 e https://cryptocointalk.com/topic/186-bitgem-btg-information/;
- Bitinum (BTN): https://bitcointalk.org/index.php?topic=501676.0 e https://cryptocointalk.com/topic/7388-bitinum-btn-information/;
- BitLand: https://bitcointalk.org/index.php?topic=1434155.0 e http://landing.bitland.world/;
- Bitleu (BTL): https://bitcointalk.org/index.php?topic=510353.0 e https://cryptocointalk.com/topic/7835-bitleu-btl-information/;
- BitLionCoin (XBL): https://bitcointalk.org/index.php?topic=660737.0 e https://cryptocointalk.com/topic/12693-bitlioncoin-xbl-information/;
- BitLits (BTLS): https://cryptocointalk.com/topic/16386-bitlits-btls-information/ e https://github.com/BitLitS-BTLS;

- Bitmark (BTM): https://bitcointalk.org/index.php?topic=660544.0 e https://cryptocointalk.com/topic/13341-bitmark-btm-information/;
- BitMo (XMB): https://bitcointalk.org/index.php?topic=772235.0 e https://cryptocointalk.com/topic/14609-bitmo-xbm-information/;
- BitMoney (BMY): https://bitcointalk.org/index.php?topic=689881.0 e https://cryptocointalk.com/topic/13583-bitmoney-bmy-information/;
- BitOre (BTO): https://bitcointalk.org/index.php?topic=714852.0;
- BitPagar: https://github.com/bitpagar e https://minkiz.co/coin/3990/;
- BitPeso (BTP): https://bitcointalk.org/index.php?topic=502918.0 e https://cryptocointalk.com/topic/7398-bitpeso-btp-information/;
- BitPopCoin (BPC): https://bitcointalk.org/index.php?topic=665896.0 e https://cryptocointalk.com/topic/13296-bitpopcoin-bpc-information/;
- BitPug: https://bitcointalk4.com/project-development/bitpug-btcxbt-pricing/;
- BitQuark (BTQ): https://bitcointalk.org/index.php?topic=468018.0 e https://cryptocointalk.com/topic/5233-annbtq-bitquark-cpu-mined-super-secure/;
- BitRaam (BRM): https://bitcointalk.org/index.php?topic=623124.0 e https://cryptocointalk.com/topic/11166-bitraam-brm-information/;
- BitReplica (BITR): https://bitcointalk.org/index.php?topic=846163.0 e https://cryptocointalk.com/topic/21068-bitreplica-bitr-information/;
- BitShares (BTS): https://bitcointalk.org/index.php?topic=1084460.0, https://github.com/bitshares e https://bitshares.org/;
- BitSharesPTS (PTS): https://bitcointalk.org/index.php?topic=325261.0 e https://cryptocointalk.com/topic/1492-bitshares-pts-information/;

- BitSlap: https://bitcointalk.org/index.php?topic=622985.0;
- Bitstar (BITS): https://bitcointalk.org/index.php?topic=748045 e https://cryptocointalk.com/topic/10459-bitstar-bits-information/;
- BitSwift: https://bitcointalk.org/index.php?topic=807557.0 e http://bitswift.io/;
- BitTor (BT): https://bitcointalk.org/index.php?topic=711590 e https://cryptocointalk.com/topic/13882-bittor-bt-information/;
- Bitz: https://bitcointalk.org/index.php?topic=954125.0 e https://cryptocointalk.com/topic/34613-ann-bitz-x11-powpos-hybrid-hard-fork-block-70000-mandatory-update/;
- BizCoin (BIZ): https://bitcointalk.org/index.php?topic=733070.0 e https://cryptocointalk.com/topic/13990-bizcoin-biz-information/;
- BlackCatCoin (BCAT): https://bitcointalk.org/index.php?topic=635920.0 e https://cryptocointalk.com/topic/11941-blackcatcoin-bcat-information/;
- BlackCoin (BLK/BC): https://bitcointalk.org/index.php?topic=469640.0, https://cryptocointalk.com/topic/6156-blackcoin-bc-information/ e http://blackcoin.co/;
- BlackDogCoin (BDOG): https://bitcointalk.org/index.php?topic=710920.0 e https://cryptocointalk.com/topic/13766-blackdogcoin-bdog-information/;
- BlackDogeCoin (XBD): https://bitcointalk.org/index.php?topic=677671.0 e https://cryptocointalk.com/topic/13166-blackdogecoin-xbd-information/;
- BlackDragonCoin (BDC): https://bitcointalk.org/index.php?topic=597006.0 e https://cryptocointalk.com/topic/11070-black-dragon-coin-bdc-information/;
- Blacktoken (BLKT): https://bitcointalk.org/index.php?topic=734339.0 e https://cryptocointalk.com/topic/14141-blacktoken-blkt-information/;

- Blade (BLA): https://bitcointalk.org/index.php?topic=452956.0 e https://cryptocointalk.com/topic/4178-blade-bla-information/;
- Blakebitcoin (BBTC): https://bitcointalk.org/index.php?topic=606037.0 e https://github.com/BlakeBitcoin/BlakeBitcoin;
- Blakecoin (BLC): https://bitcointalk.org/index.php?topic=306894.0 e https://cryptocointalk.com/topic/1357-blakecoin-blc-information/;
- Blazecoin (BLZ): https://bitcointalk.org/index.php?topic=624778.0 e https://cryptocointalk.com/topic/11607-blazecoin-blz-information/;
- BlessCoin (BLS): https://bitcointalk.org/index.php?topic=391793.0 e https://cryptocointalk.com/topic/2653-blesscoin-bls-information/;
- BlitzCoin (BLTZ): https://bitcointalk.org/index.php?topic=509173.0 e https://cryptocointalk.com/topic/9148-blitzcoin-bltz-information/;
- Blocknet (BLOCK): https://bitcointalk.org/index.php?topic=829576.0 e http://blocknet.co/;
- BluCoin (BLU): https://bitcointalk.org/index.php?topic=436511.0 e https://cryptocointalk.com/topic/3857-ann-blucoin-blu-new-social-media-cryptocurrency-1-million-free-coin-giveaway/;
- Bluechip (BCH): https://bitcointalk.org/index.php?topic=647938.0 e https://cryptocointalk.com/topic/12316-bluechip-bch-information/;
- Bluecoin (BLU): https://bitcointalk.org/index.php?topic=580639.0 e https://cryptocointalk.com/topic/10505-bluecoin-blu-information/;
- BluePlanetCoin (BLP): https://bitcointalk.org/index.php?topic=736114.0;
- Bones: https://bitcointalk.org/index.php?topic=521270.0 e https://cryptocointalk.com/topic/8383-bones-bones-information/;
- Bongger (BGR): https://bitcointalk.org/index.php?topic=634701.0;
- BonusCoin (BNS): https://bitcointalk.org/index.php?topic=524212.0 e https://cryptocointalk.com/topic/8568-bonuscoin-

bns-information/;

- BoolBerry (BBR): https://bitcointalk.org/index.php?topic=577267.0 e https://cryptocointalk.com/topic/11954-boolberry-bbr-information/;
- Boomcoin: https://bitcointalk.org/index.php?topic=716699.0 e https://cryptocointalk.com/topic/13844-boomcoin-boom-information/;
- BoostCoin: https://bitcointalk.org/index.php?topic=601965.0 e https://cryptocointalk.com/topic/11297-boostcoin-bost-information/;
- BoschiCoin (BCC): https://bitcointalk.org/index.php?topic=498976.0 e https://cryptocointalk.com/topic/7047-boschicoin-bcc-information/;
- BossCoin (BSS): https://bitcointalk.org/index.php?topic=355729.0 e https://cryptocointalk.com/topic/2196-bosscoin-bos-information/;
- Bottlecaps (CAP): https://bitcointalk.org/index.php?topic=241445.0 e https://cryptocointalk.com/topic/1117-bottlecaps-cap-information/;
- BountyCoin (BOC/BOUN): https://bitcointalk.org/index.php?topic=271729.0 e https://cryptocointalk.com/topic/1001-bountycoin-boc-information/;
- BoxCoin: https://bitcointalk.org/index.php?topic=599218.0;
- BoyCoin: https://cryptocointalk.com/topic/10492-boycoin-boy-information/ e https://github.com/bgcoin/BoyCoin;
- BrCoin: https://bitcointalk.org/index.php?topic=514869.0 e https://cryptocointalk.com/topic/12082-brcoin-brc-information/;
- BrigadeCoin (BRIG): https://bitcointalk.org/index.php?topic=657840.15 e https://cryptocointalk.com/topic/12663-brigadecoin-brig-information/;
- BrightCoin (BRI): https://bitcointalk.org/index.php?topic=507590.0 e https://cryptocointalk.com/topic/8075-brightcoin-bri-information/;
- Britcoin (BRIT): https://bitcointalk.org/index.php?topic=1463367.0 e https://cryptocointalk.com/topic/12854-britcoin-brit-information/;

- BtcTalkCoin (BCT): https://bitcointalk.org/index.php?topic=570750.0;
- BulbaCoin (BULB): https://bitcointalk.org/index.php?topic=676992.0 e https://cryptocointalk.com/topic/12900-bulbacoin-bulb-information/;
- Bumbacoin (CLOT): https://bitcointalk.org/index.php?topic=592679.0 e http://bumbacoin.com/;
- BunnyCoin (BUN): https://bitcointalk.org/index.php?topic=589180.0 e https://cryptocointalk.com/topic/10671-bunnycoin-bun-information/;
- BurbuCoin (BUR): https://bitcointalk.org/index.php?topic=442021.0 e https://cryptocointalk.com/topic/4122-burbucoin-bur-information/;
- Burnercoin (BURN): https://bitcointalk.org/index.php?topic=645753.0 e https://cryptocointalk.com/topic/12237-burnercoin-burn-information/;
- Burst: https://bitcointalk.org/index.php?topic=731923.0 e https://cryptocointalk.com/topic/28465-ann-burst-hard-disk-mining-crowdfunding-press-release/;
- ButterflyCoin (BFC): https://cryptocointalk.com/topic/1113-ann-butterflycoin-bfc-announcement/;
- BuyCoin (BUY): https://bitcointalk.org/index.php?topic=734708.0 e https://cryptocointalk.com/topic/14578-buycoin-buy-information/;
- Bytecoin (BCN): https://bitcointalk.org/index.php?topic=512747.0, https://cryptocointalk.com/topic/11158-bytecoin-bcn-information/ e https://bytecoin.org/;
- C-Note (CNT): https://bitcointalk.org/index.php?topic=397916.0 e https://cryptocointalk.com/topic/3010-c-note-cnt-information/;
- Cachecoin (CACH): https://bitcointalk.org/index.php?topic=400389.0 e https://cryptocointalk.com/topic/2873-cachecoin-cach-information/;
- CageCoin (CAGE): https://bitcointalk.org/index.php?topic=394958.0 e https://cryptocointalk.com/topic/2728-cagecoin-cage-information/;

- CaiShen (CAIx): https://bitcointalk.org/index.php?topic=513613.0 e https://cryptocointalk.com/topic/9305-caishencoin-caix-information/;
- Californiacoin (CAC): https://bitcointalk.org/index.php?topic=589672.0 e https://cryptocointalk.com/topic/10632-californiacoin-cac-information/;
- CamCoin (CAM): https://bitcointalk.org/index.php?topic=683355.0 e https://cryptocointalk.com/topic/13194-camcoin-cam-information/;
- CamorraCoin: https://bitcointalk.org/index.php?topic=827956.0 e https://cryptocointalk.com/topic/20373-ann-camorracoin-cam-scrypt-stealth-addresses-encrypted-messaging/;
- CanadaCoin (CDA): https://bitcointalk.org/index.php?topic=599784.0;
- Canadaecoin (CDN): https://bitcointalk.org/index.php?topic=545675.0 e https://cryptocointalk.com/topic/9053-canadaecoin-cdn-information/;
- CannabisCoin (CANN): https://bitcointalk.org/index.php?topic=661885.0 e http://cannabiscoin.net/;
- Cannacoin (CCN): https://bitcointalk.org/index.php?topic=740903.0;
- CantorCoin (EIC): https://cryptocointalk.com/topic/12727-cantorcoin-eic-information/;
- CapitalCoin (CPTL): https://bitcointalk.org/index.php?topic=589930.0 e https://cryptocointalk.com/topic/10755-capitalcoin-cptl-information/;
- CaptCoin (CAPT): https://bitcointalk.org/index.php?topic=684167.0 e https://cryptocointalk.com/topic/13731-captcoin-capt-information/;
- Carboncoin (CARB): https://bitcointalk.org/index.php?topic=465364.0 e https://cryptocointalk.com/topic/5229-carboncoin-carb-information/;
- CarCoin (V8): https://cryptocointalk.com/topic/12934-carcoin-v8-information/;
- CarpeDiemCoin (DIEM): https://bitcointalk.org/index.php?topic=513599.0 e

https://cryptocointalk.com/topic/7991-carpediemcoin-diem-information/;

- Cashcoin (CASH): https://bitcointalk.org/index.php?topic=424421.0 e https://cryptocointalk.com/topic/3442-cashcoin-cash-information/;
- Cashtag: https://bitcointalk.org/index.php?topic=577348.0;
- CasinoCoin (CSC): https://bitcointalk.org/index.php?topic=258090.0, https://cryptocointalk.com/topic/851-casinocoin-csc-information/ e http://casinocoin.org/;
- CassubianDetk (CDT): https://bitcointalk.org/index.php?topic=688311.0 e https://cryptocointalk.com/topic/13319-cassubian-detk-cdt-information/;
- Cataloniacoin (CATC): https://bitcointalk.org/index.php?topic=518418.0 e https://cryptocointalk.com/topic/9374-cataloniacoin-catc-information/;
- Catcoin (CAT): https://bitcointalk.org/index.php?topic=380130.0 e https://cryptocointalk.com/topic/2391-catcoin-cat-information/;
- CateDoge: (CTD): https://bitcointalk.org/index.php?topic=528453.0 e https://cryptocointalk.com/topic/10415-catedoge-ctd-information/;
- CCoin (CC): https://cryptocointalk.com/topic/3083-ccoin-cc-information/;
- CetusCoin (CETI): https://bitcointalk.org/index.php?topic=790782.0, https://cryptocointalk.com/topic/17223-ceti-cetus-coin-scryptpowpos1-year-pow/ e https://github.com/CetusCoin/Ceti;
- Cganomaly (CGA): https://bitcointalk.org/index.php?topic=771830.0 e https://cryptocointalk.com/topic/4141-cryptographic-anomaly-cga-information/;
- ChainCoin (CHC): https://bitcointalk.org/index.php?topic=422149.0 e https://cryptocointalk.com/topic/3382-chaincoin-chc-information/;
- ChanceCoin (CHA): https://bitcointalk.org/index.php?topic=528023.0 e https://cryptocointalk.com/topic/13603-gryf-gryfencoin-x15-powpos-gpu-1trillion-coins-gryfx-options-trading/;

- CharityCoin: https://bitcointalk.org/index.php?topic=448269.0 e https://cryptocointalk.com/topic/4572-charitycoin-cha-information/;
- Chatcoin (CHAT): https://bitcointalk.org/index.php?topic=675803.0 e https://cryptocointalk.com/topic/13074-chatcoin-chat-information/;
- Chccoin (CHCC): https://bitcointalk.org/index.php?topic=603992.0 e https://cryptocointalk.com/topic/12135-chccoin-chcc-information/;
- CheckCoin (CKC): https://bitcointalk.org/index.php?topic=715563.0 e https://cryptocointalk.com/topic/16725-checkcoin-ckc-information/;
- CheckOutCoin (CXC): https://bitcointalk.org/index.php?topic=840437;
- CherryNote (CRR): https://bitcointalk.org/index.php?topic=695608.0 e https://cryptocointalk.com/topic/13398-cherrynote-crr-information/;
- ChiCoin (CHI): https://bitcointalk.org/index.php?topic=423620.0 e https://cryptocointalk.com/topic/2440-chicoin-chi-information/;
- ChiKun (KUN): https://bitcointalk.org/index.php?topic=507614.0 e https://cryptocointalk.com/topic/7745-chikun-kun-information/;
- ChinaCoin/CHNcoin (CNC): https://bitcointalk.org/index.php?topic=192969.0 e https://cryptocointalk.com/topic/1484-chncoin-cnc-information-resurrection/;
- ChocoCoin (CCC): https://bitcointalk.org/index.php?topic=353864 e https://cryptocointalk.com/topic/2208-chococoin-ccc-information/;
- CinnamonCoin CIN): https://bitcointalk.org/index.php?topic=299221.0 e https://cryptocointalk.com/topic/1220-cinnamoncoin-cin-141-proof-of-stake-only/;
- Cinni (CINNI): https://bitcointalk.org/index.php?topic=573232.0 e https://cryptocointalk.com/topic/10590-cinnicoin-cinni-information/;

- CitizenCoin (CTZ): https://bitcointalk.org/index.php?topic=526076.0 e https://cryptocointalk.com/topic/11427-citizencoin-ctz-information/;
- CityCoin (CITY): https://bitcointalk.org/index.php?topic=704271.0;
- CivilizationCoin (CIV): https://bitcointalk.org/index.php?topic=796591.0 e https://cryptocointalk.com/topic/11560-civilizationcoin-civ-information/;
- CkCoin (CK): https://bitcointalk.org/index.php?topic=726101.0 e https://cryptocointalk.com/topic/13989-ckcoin-ck-information/;
- Clams: https://bitcointalk.org/index.php?topic=623147.0 e http://clamclient.com/;
- CleanCoin (CLN): https://bitcointalk.org/index.php?topic=705533.0 e https://cryptocointalk.com/topic/13695-cleancoin-cln-information/;
- Clean Water Coin (WATER): https://bitcointalk.org/index.php?topic=526513.0 e https://cryptocointalk.com/topic/9375-cleanwatercoin-water-information/;
- CloakCoin (CLOAK): https://bitcointalk.org/index.php?topic=637704.0, https://cryptocointalk.com/topic/12025-cloakcoin-cloak-information/ e http://www.cloakcoin.com/;
- ClockCoin (CKC): https://bitcointalk.org/index.php?topic=400477.0 e https://cryptocointalk.com/topic/2879-clockcoin-ckc-information/;
- CloudCoin (CDC): https://bitcointalk.org/index.php?topic=256120.0 e https://cryptocointalk.com/topic/884-cloudcoin-cdc-information/;
- CloverCoin: https://bitcointalk.org/index.php?topic=596917.0;
- ClusterCoin (CLSTR): https://bitcointalk.org/index.php?topic=737636.0 e https://cryptocointalk.com/topic/14535-clustercoin-clstr-information/;
- CoCoCoin (COCO): https://bitcointalk.org/index.php?topic=646781.0 e https://cryptocointalk.com/topic/12791-cococoin-coco-information/;

- Coffeecoin (CFC/CFC2): https://bitcointalk.org/index.php?topic=596562.0 e https://cryptocointalk.com/topic/11061-coffeecoin-cfc-information/;
- CoiledCoin (CLC): https://bitcointalk.org/index.php?topic=56675.0;
- Coin2 (NC2): https://bitcointalk.org/index.php?topic=483847.0 e https://cryptocointalk.com/topic/9056-coin2-nc2-information/;
- Coinaaa: https://bitcointalk.org/index.php?topic=525345.0;
- Coino (COINO): https://bitcointalk.org/index.php?topic=419873.0 e https://cryptocointalk.com/topic/3367-coino-con-information/;
- CoinShield: https://bitcointalk.org/index.php?topic=816600.0 e https://cryptocointalk.com/topic/19201-ann-coinshield-sk-1024-11-new-features-cpu-launched-gpu-launch-date-set/;
- Coinsy (CSY): https://bitcointalk.org/index.php?topic=606006.0 e https://cryptocointalk.com/topic/11183-coinsy-csy-information/;
- Coinye (KOI / COYE): https://bitcointalk.org/index.php?topic=396068.0 e https://en.wikipedia.org/wiki/Coinye;
- ColaCoin (COLA): https://bitcointalk.org/index.php?topic=443776.0 e https://cryptocointalk.com/topic/4073-colacoin-cola-information-new-ver-chkpoints-mandatory-update/;
- ColbertCoin (CC): https://bitcointalk.org/index.php?topic=567491.0;
- ColossusCoin (COL): https://bitcointalk.org/index.php?topic=279601.0 e https://cryptocointalk.com/topic/1146-colossuscoin-col-information/;
- ComedyGold: https://bitcointalk.org/index.php?topic=549303.0;
- Communitycoin (COMM): https://bitcointalk.org/index.php?topic=558319.0 e https://cryptocointalk.com/topic/9028-communitycoin-comm-information/;

- CompassCoin (CPC): https://bitcointalk.org/index.php?topic=553127.0 e https://cryptocointalk.com/topic/10915-compasscoin-cpc-information/;
- ComputerCoin (CMPT): https://bitcointalk.org/index.php?topic=684562.0 e https://cryptocointalk.com/topic/13883-computercoin-cmpt-information/;
- ConcealCoin (CNL): https://bitcointalk.org/index.php?topic=700289.0 e https://cryptocointalk.com/topic/13513-concealcoin-cnl-information/;
- ConfessionCoin (CFN): https://bitcointalk.org/index.php?topic=606996.0 e https://cryptocointalk.com/topic/11696-confessioncoin-cfn-information/;
- ConspiracyCoin (CYC): https://bitcointalk.org/index.php?topic=590841.0 e https://cryptocointalk.com/topic/11563-conspiracycoin-cyc-information/;
- Continuumcoin (CTM): https://bitcointalk.org/index.php?topic=440515.0 e https://cryptocointalk.com/topic/3795-continuumcoin-ctm-information/;
- Coolcoin: https://bitcointalk.org/index.php?topic=601045.0 e https://cryptocointalk.com/topic/13344-coolcoin-cool-information/;
- Compasscoin (CPC): https://bitcointalk.org/index.php?topic=553127.0 e https://cryptocointalk.com/topic/10915-compasscoin-cpc-information/;
- Conspiracycoin (CYC): https://bitcointalk.org/index.php?topic=590841.0 e https://cryptocointalk.com/topic/11563-conspiracycoin-cyc-information/;
- CopperBars (CPR): https://bitcointalk.org/index.php?topic=272170.0 e https://cryptocointalk.com/topic/1006-copperbars-cpr-information/;
- Copperlark (CL): https://bitcointalk.org/index.php?topic=227252.0 e https://cryptocointalk.com/topic/519-copperlark-cl-information/;
- Corgicoin (CORG): https://bitcointalk.org/index.php?topic=444700.0, https://bitcointalk.org/index.php?topic=1373179 e https://cryptocointalk.com/topic/4183-corgicoin-corg-information/;

- CornerstoneCoin (CCX): https://bitcointalk.org/index.php?topic=584550.0 e https://cryptocointalk.com/topic/10533-cornerstonecoin-ccx-information/;
- Cosmoscoin (CMC): https://bitcointalk.org/index.php?topic=245938.0 e https://cryptocointalk.com/topic/750-cosmoscoin-cmc-information/;
- Counterparty (XCP): https://bitcointalk.org/index.php?topic=395761.0 e http://counterparty.io/;
- Craftcoin (CRC): https://bitcointalk.org/index.php?topic=250343.0 e https://cryptocointalk.com/topic/792-craftcoin-crc-information/;
- CraigsCoin (CRAIG): https://bitcointalk.org/index.php?topic=780334.0 e https://cryptocointalk.com/topic/17289-craigscoin-craig-information/;
- CreateCoin (CREAT): https://cryptocointalk.com/topic/12366-createcoin-creat-information/;
- CreditCoin (CRD): https://bitcointalk.org/index.php?topic=414012.0 e https://cryptocointalk.com/topic/3703-credits-crd-information/;
- Credits (CR): https://cryptocointalk.com/topic/3703-credits-crd-information/;
- Creds (XXC): https://cryptocointalk.com/topic/8084-creds-xxc-information/;
- CrimeCoin: https://bitcointalk.org/index.php?topic=959024.0 e https://cryptocointalk.com/topic/936-ann-crimecoin-test-version/;
- CrownCoin (CRW): https://bitcointalk.org/index.php?topic=815487.0 e https://cryptocointalk.com/topic/18847-crowncoin-crw-information/;
- CRTCoin - CryptographicCoin (CRT): https://bitcointalk.org/index.php?topic=555578.0 e https://cryptocointalk.com/topic/10890-cryptographiccoin-crt-information/;
- CryptCoin (CRY): https://bitcointalk.org/index.php?topic=618377.0 e https://cryptocointalk.com/topic/11554-

cryptcoin-cry-information/;

- Crypti (XCR): https://bitcointalk.org/index.php?topic=654463.0 e https://cryptocointalk.com/topic/14487-crypti-xcr-?-3-pos-algorithms-ed25519-2nd-gen-source/;
- CryptoApples (CRA): https://bitcointalk.org/index.php?topic=457078.0;
- Cryptobits (CYB): https://bitcointalk.org/index.php?topic=261194.0 e https://cryptocointalk.com/topic/850-cryptobits-cyb-information/;
- Cryptobuck (BUK): https://bitcointalk.org/index.php?topic=285224.0 e https://cryptocointalk.com/topic/1122-cryptobuck-buk-information/;
- Crypto Bullion (CBX): https://bitcointalk.org/index.php?topic=951753.0, https://cryptocointalk.com/topic/44690-cbx-crypto-bullion-cbx-aditivado-com-posp-est-2013/ e http://cryptobullion.io/;
- CryptoClub (CCB): https://bitcointalk.org/index.php?topic=667866.0 e https://cryptocointalk.com/topic/17501-annccb-cryptoclub-?-round-s-5-?-swap-your-coins-?-subscription-?/;
- CryptoEagle (CREA): https://bitcointalk.org/index.php?topic=497796.0 e https://cryptocointalk.com/topic/6981-ann-crea-cryptoeagle-sha256-kgw-10000000-max-coins/;
- CryptoEscudo (CESC): https://bitcointalk.org/index.php?topic=524124.0, https://cryptocointalk.com/topic/9038-cryptoescudo-cesc-information/, https://cryptoescudo.org/ e http://cryptoescudotalk.com/;
- CryptoGenicBullion (CGB): https://bitcointalk.org/index.php?topic=285774.0 e https://cryptocointalk.com/topic/743-cryptogenic-bullion-cgb-information/;
- CryptographicAnomaly (CGA): https://bitcointalk.org/index.php?topic=443094.0 e https://bitcointalk.org/index.php?topic=771830 e https://cryptocointalk.com/topic/4141-cryptographic-anomaly-cga-information/;
- CryptographicCoin (CRT): https://bitcointalk.org/index.php?topic=555578.0 e

https://cryptocointalk.com/topic/10890-cryptographiccoin-crt-information/;

- CryptoLoot (LOOT): https://bitcointalk.org/index.php?topic=497021.0 e https://cryptocointalk.com/topic/5098-cryptoloot-loot-information/;
- CryptoMeth (METH): https://bitcointalk.org/index.php?topic=500175.0 e https://cryptocointalk.com/topic/9360-cryptometh-meth-information/;
- Cryptonite (XCN): https://bitcointalk.org/index.php?topic=713538.0 e https://cryptocointalk.com/topic/13846-cryptonite-xcn-information/;
- CryptoniumCoin (CRN): https://cryptocointalk.com/topic/3146-cryptonium-crn-information/;
- CryptoShekel (SHKL): https://bitcointalk.org/index.php?topic=394123.0 e https://cryptocointalk.com/topic/2747-cryptoshekel-shkl-information/;
- Cryptsy Points: https://bitcointalk.org/index.php?topic=349069.0;
- CrystalCoin (CRYSTAL): https://bitcointalk.org/index.php?topic=715316.0 e https://cryptocointalk.com/topic/14013-crystalcoin-crystal-information/;
- CsCoin (CSO): https://bitcointalk.org/index.php?topic=664262.0 e https://cryptocointalk.com/topic/13161-cscoin-cso-information/;
- CthulhuCoin (OFF): https://bitcointalk.org/index.php?topic=294383.0 e https://cryptocointalk.com/topic/1196-promises-of-dreamland-offerings-to-cthulhu/;
- Cubits (QBT): https://bitcointalk.org/index.php?topic=345328.0 e https://cryptocointalk.com/topic/1638-cubits-qbt-information-v3/;
- CummingTonite (CUM): https://bitcointalk.org/index.php?topic=792203.0 e https://cryptocointalk.com/topic/17108-cummingtonite-cum-information/;
- CureCoin: https://bitcointalk.org/index.php?topic=603757.0 e https://www.curecoin.net/;

- CypherFunks (FUNK): https://bitcointalk.org/index.php?topic=469407.0 e https://cryptocointalk.com/topic/5968-cypherfunk-funk-information/;
- CzechCoin: https://bitcointalk.org/index.php?topic=596649.0;
- CzechCrownCoin (CZC): https://bitcointalk.org/index.php?topic=712960.0 e https://cryptocointalk.com/topic/14708-czechcrowncoin-czc-information/;
- CzeCoin (CZE): https://bitcointalk.org/index.php?topic=679856.0 e https://cryptocointalk.com/topic/13850-czecoin-cze-information/;
- DafuqCoin (DFQ): https://bitcointalk.org/index.php?topic=575281.0;
- DaMaCoin (DMC): https://bitcointalk.org/index.php?topic=497079.0 e https://cryptocointalk.com/topic/6989-damacoin-dmc-information/;
- DarkCash (DRKC): https://bitcointalk.org/index.php?topic=709322.0 e https://cryptocointalk.com/topic/13775-darkcash-drkc-information/;
- DarkCoin: https://bitcointalk.org/index.php?topic=384582.0, https://cryptocointalk.com/topic/8971-4-10givecoin-give-darkcoins-x11-algokgw/ e https://www.darkcoinfoundation.org/;
- DarkFox (DRX): https://bitcointalk.org/index.php?topic=730801.0 e https://cryptocointalk.com/topic/14072-darkfox-drx-information/;
- DarkGold: https://bitcointalk.org/index.php?topic=868354.0 e https://cryptocointalk.com/topic/22865-ann-darkgold-x13/;
- DarkNetCoin (DNC): https://bitcointalk.org/index.php?topic=818365.0;
- DarkNote (XDN): https://bitcointalk.org/index.php?topic=788916.0 e https://cryptocointalk.com/topic/11873-darknote-xdn-information/;
- DarkPeer (DPC): https://bitcointalk.org/index.php?topic=797897.0 e https://cryptocointalk.com/topic/18643-darkpeer-

dpc-information/;

- Dash: https://bitcointalk.org/index.php?topic=421615.0, https://cryptocointalk.com/topic/3373-dash-dash-information/ e https://www.dashpay.io/;

- Dashcoin (DSH): https://bitcointalk.org/index.php?topic=678232.0, https://cryptocointalk.com/topic/13547-dashcoin-dsh-information/ e http://dashcoin.net/;
- DataCoin (DTC): https://bitcointalk.org/index.php?topic=325735.0 e https://cryptocointalk.com/topic/1569-datacoin-dtc-information/;
- Dcom (DCM): https://bitcointalk.org/index.php?topic=636470.0 e https://cryptocointalk.com/topic/12445-digital-commerce-dcm-information/;
- DeafDollars ($DEAF): https://bitcointalk.org/index.php?topic=624682.0 e https://cryptocointalk.com/topic/22335-deafdollars-deaf-network-resources/;
- DebtCoin (DBT): https://bitcointalk.org/index.php?topic=671209.0 e https://cryptocointalk.com/topic/12860-debtcoin-dbt-information/;
- DecryptRcoin (DECR): https://bitcointalk.org/index.php?topic=926536.0 e https://cryptocointalk.com/topic/27779-ann-decryptrcoin-decr-fast-transactions-no-ipo-launched/;
- DeepCoin (DCN): https://bitcointalk.org/index.php?topic=667470.0 e https://cryptocointalk.com/topic/12831-deepcoin-dcn-information/;
- DefCoin: https://bitcointalk.org/index.php?topic=1649671.0 e http://defcoin.org/;
- DeleteCoin (DEL): https://bitcointalk.org/index.php?topic=511880.0 e https://cryptocointalk.com/topic/8217-deletecoin-del-information/;
- DeltaCoin: https://bitcointalk.org/index.php?topic=510039.0 e https://cryptocointalk.com/topic/8024-deltacoin-delta-information/;
- Denarius (DRS): https://bitcointalk.org/index.php?topic=591323.0 e https://cryptocointalk.com/topic/10665-denarius-drs-information/;
- Deutsche eMark (DEM): https://bitcointalk.org/index.php?topic=310939.0 e https://cryptocointalk.com/topic/1408-deutsche-emark-dem-information/;

- Devcoin (DVC): https://bitcointalk.org/index.php?topic=34586, https://cryptocointalk.com/topic/120-devcoin-dvc-information/ e http://devcoin.org/;
- Diamond (DMD): https://bitcointalk.org/index.php?topic=255806.0, https://cryptocointalk.com/topic/2228-diamond-dmd-information/ e http://bit.diamonds/;
- DiamondBack (DBK): https://bitcointalk.org/index.php?topic=741340.0 e https://cryptocointalk.com/topic/14536-diamondback-dbk-information/;
- DiamondCoin (DMC): https://bitcointalk.org/index.php?topic=502060.0 e https://cryptocointalk.com/topic/7516-diamondcoin-dmc-information/;
- DigiByte (DGB): https://bitcointalk.org/index.php?topic=408268.0, https://cryptocointalk.com/topic/3137-digibyte-dgb-information/ e http://www.digibyte.co/;
- DigiGems (DGMS): https://bitcointalk.org/index.php?topic=913237.0 e https://cryptocointalk.com/topic/28264-ann-dgms-digigems-no-preminescryptno-ipo-information/;
- Digit (DIG): https://bitcointalk.org/index.php?topic=597634.0 e https://cryptocointalk.com/topic/11063-digit-dig-information/;
- Digitalcoin (DGC): https://bitcointalk.org/index.php?topic=209508.0, https://cryptocointalk.com/topic/271-digitalcoin-dgc-information/ e http://digitalcoin.org/;
- Digital Commerce (dCom / DCM): https://bitcointalk.org/index.php?topic=636470.0 e https://cryptocointalk.com/topic/12445-digital-commerce-dcm-information/;
- DigitalNote (XDN): https://bitcointalk.org/index.php?topic=1082745.0, http://digitalnotetalk.org/ e http://digitalnote.org/;
- DigitalPrice (DP): https://bitcointalk.org/index.php?topic=789847.0 e https://cryptocointalk.com/topic/17690-digitalprice-dgr-information/;
- DijkstraCoin (DKC): https://bitcointalk.org/index.php?topic=658988.0 e https://cryptocointalk.com/topic/13002-dijkstracoin-dkc-information/;

- Dilmacoin: https://bitcointalk.org/index.php?topic=527353.0, http://dilmacoin-criptomoeda.rhcloud.com/, https://bitcointalk.org/index.php?topic=1298394.0, http://dilmacoin.tk/ e http://tutoriais-dilmacoin.rhcloud.com/;
- Dimecoin (DIME): https://bitcointalk.org/index.php?topic=382164.0 e https://cryptocointalk.com/topic/2431-dimecoin-dime-information/;
- DinarCoin (IQD): https://bitcointalk.org/index.php?topic=494685.0 e https://cryptocointalk.com/topic/6866-dinarcoin-iqd-information/;
- DinosaurCoin (DINO): https://bitcointalk.org/index.php?topic=678073.0 e https://cryptocointalk.com/topic/13090-dinosaurcoin-dino-information/;
- Dirac (XDQ): https://bitcointalk.org/index.php?topic=616288.20 e https://cryptocointalk.com/topic/11422-dirac-xdq-information/;
- DistroBlitz (DB): https://bitcointalk.org/index.php?topic=585741.0 e https://cryptocointalk.com/topic/10934-dbann-?-?-?-?-???distroblitz???-?-?-?-?-??_?test-giveaway-?_??/;
- Distrocoin (DISTRO): https://bitcointalk.org/index.php?topic=614921.0 e https://cryptocointalk.com/topic/11119-distrocoin-distro-information/;
- DNotes (NOTE): https://bitcointalk.org/index.php?topic=470155.0, https://cryptocointalk.com/topic/5706-dnotes-note-information/ e http://dnotescoin.com/;
- DobbsCoin (BOB): https://bitcointalk.org/index.php?topic=792459.0, https://cryptocointalk.com/topic/3037-dobbscoin-bob-information/ e http://www.dobbscoin.info/;
- Dogecoin (DOGE): https://bitcointalk.org/index.php?topic=361813.0, https://cryptocointalk.com/topic/2016-dogecoin-doge-information/ e http://dogecoin.com/;
- Dogecoin Dark (DOGED): https://bitcointalk.org/index.php?topic=770742.0, https://cryptocointalk.com/topic/18797-dogecoindark-doged-information/ e http://dogecoindark.net/;
- DokdoCoin (DOKDO): https://bitcointalk.org/index.php?topic=493712.0 e https://cryptocointalk.com/topic/6872-

dokdocoin-dokdo-information/;

- DollarCoin (DOLLAR): https://bitcointalk.org/index.php?topic=702098.0 e https://cryptocointalk.com/topic/20909-dollarcoin-dollar-information/;
- DollarPounds (DPS): https://bitcointalk.org/index.php?topic=274194.0 e https://cryptocointalk.com/topic/1020-dollarpound-dpz-information/;
- DolphinCoin (DOLP): https://bitcointalk.org/index.php?topic=625466.0 e https://cryptocointalk.com/topic/13342-dolphincoin-dolp-information/;
- DomeCoin (DOME): https://bitcointalk.org/index.php?topic=514017.0 e https://cryptocointalk.com/topic/8011-domecoin-dome-information/;
- DonateCoin: https://bitcointalk.org/index.php?topic=510037.0;
- Donationcoin (DON): https://bitcointalk.org/index.php?topic=589852.0 e https://cryptocointalk.com/topic/10521-donationcoin-don-information/;
- DoomCoin (DOOM): https://bitcointalk.org/index.php?topic=713003.0 e https://cryptocointalk.com/topic/13818-doomcoin-doom-information/;
- Dopecoin (DOPE): https://bitcointalk.org/index.php?topic=467641.0 e https://cryptocointalk.com/topic/36897-ann-dopecoin-the-worlds-first-cryptocoin-weed/;
- DorianCoin: https://bitcointalk.org/index.php?topic=508366.0 e http://doriancoin.org/;
- Doscoin (DOS): https://bitcointalk.org/index.php?topic=720001.0 e https://cryptocointalk.com/topic/13924-doscoin-dos-information/;
- Dosh-Kapital: https://bitcointalk4.com/announcements-(altcoins)/dosh-kapital/ e https://cryptocointalk.com/topic/14220-dosh-information/;
- DotCoin (DOT): https://bitcointalk.org/index.php?topic=550851.0 e https://cryptocointalk.com/topic/9383-annscrypt-dotcoin/;
- DoubleEagle (XDE): https://bitcointalk.org/index.php?topic=736702.0 e https://cryptocointalk.com/topic/14258-

doubleeagle-xde-information/;

- Doubloons (DBL): https://bitcointalk.org/index.php?topic=206361.0 e https://cryptocointalk.com/topic/164-doubloons-dbl-information/;
- DougCoin (DOUG): https://bitcointalk.org/index.php?topic=464267.0 e https://cryptocointalk.com/topic/6086-dougcoin-doug-information/;
- DragonCoin (DNC): https://bitcointalk.org/index.php?topic=216653.0 e https://cryptocointalk.com/topic/364-dragoncoin-dnk-information/;
- DreamCoin (DRM): https://bitcointalk.org/index.php?topic=599854.0 e https://cryptocointalk.com/topic/10928-dreamcoin-drm-information/;
- DsCoin (DSC): https://cryptocointalk.com/topic/935-dscoin-dsc-information/;
- DubCoin (DUB): https://bitcointalk.org/index.php?topic=740223.0 e https://cryptocointalk.com/topic/14254-dubcoin-dub-information/;
- DubstepCoin (WUBS): https://bitcointalk.org/index.php?topic=387614.0 e https://cryptocointalk.com/topic/2567-dubstepcoin-wubs-information/;
- Ducats (DUC): https://bitcointalk.org/index.php?topic=419943.0 e https://cryptocointalk.com/topic/3321-ducats-duc-information/;
- DuckDuckCoin (DUCK): https://bitcointalk.org/index.php?topic=448221.0 e https://cryptocointalk.com/topic/4859-duckduckcoin-duck-information/;
- DulorCoin (DUL): https://bitcointalk.org/index.php?topic=687519.0 e https://cryptocointalk.com/topic/13389-dulorcoin-dul-information/;
- DvoraKoin (DVK): https://bitcointalk.org/index.php?topic=613854.0 e https://cryptocointalk.com/topic/11631-annmulti-algorithms-dvorakoin-dvk-25-may/;
- E-Currency (ISO): https://cryptocointalk.com/topic/12398-e-currency-iso-information/;

- E-Dinar Coin (EDC): https://bitcointalk.org/index.php?topic=1586602.0 e https://cryptocointalk.com/topic/49252-e-dinar-coin-meet-the-revolutionary-new-generation-cryptocurrency/;
- EagleCoin (EGC): https://bitcointalk.org/index.php?topic=260484.0 e https://cryptocointalk.com/topic/870-eaglecoin-egc-information/;
- EarthCoin (EAC): https://bitcointalk.org/index.php?topic=379236.0, https://cryptocointalk.com/topic/2347-earthcoin-eac-information/, http://earthcoin.org/ e http://getearthcoin.com/;
- EasterCoin (ETR): https://bitcointalk.org/index.php?topic=569220.0 e https://cryptocointalk.com/topic/10004-eastercoin/;
- EBTCoin (EBT): https://bitcointalk.org/index.php?topic=437660.0 e https://cryptocointalk.com/topic/3811-ebtcoin-ebt-information/;
- ECCoin (ECC): https://cryptocointalk.com/topic/7602-eccoin-ecc-information/;
- EcoCoin (ECO): https://bitcointalk.org/index.php?topic=269312.0 e https://cryptocointalk.com/topic/1090-ecocoin-eco-information/;
- E-Currency (ISO): https://bitcointalk.org/index.php?topic=647254.0 e https://cryptocointalk.com/topic/12398-e-currency-iso-information/;
- EdisonX3 (EDISON): https://www.reddit.com/r/CryptoCurrency/comments/1z5zxr/preann_edisonx3_the_first_historical_crypto/ e https://cryptocointalk.com/topic/8561-edisonx3-edison-information/;
- EduCoin (EDU): https://bitcointalk.org/index.php?topic=486600.0 e https://cryptocointalk.com/topic/7836-educoin-edu-information/;
- Eirecoin (EIR): https://bitcointalk.org/index.php?topic=656051 e https://cryptocointalk.com/topic/12599-eirecoin-eir-information/;
- Einsteinium (EMC2): https://bitcointalk.org/index.php?topic=494708.0, https://cryptocointalk.com/topic/6901-einsteinium-emc2-information/ e http://einsteiniumfoundation.com/;

- Ekita: https://bitcointalk.org/index.php?topic=715696.0 e https://cryptocointalk.com/topic/13845-ekita-ekita-information/;
- Ekrona (KRN): https://bitcointalk.org/index.php?topic=421376.0 e https://cryptocointalk.com/topic/3132-ekrona-krn-information/;
- Elacoin (ELC): https://bitcointalk.org/index.php?topic=203647.0 e https://cryptocointalk.com/topic/130-elacoin-elc-information/;
- ElectricCoin (VOLT): https://bitcointalk.org/index.php?topic=396293.0 e https://cryptocointalk.com/topic/2746-electric-volt-information/;
- Electron (ELT): https://bitcointalk.org/index.php?topic=624595.0 e https://cryptocointalk.com/topic/11662-electron-elt-information/;
- Electronic Benefit Transfer (EBTcoin / EBT): https://bitcointalk.org/index.php?topic=436045.0, https://cryptocointalk.com/topic/3811-ebtcoin-ebt-information/ e https://bitcointalk4.com/announcements-(altcoins)/(ann)-(ebt)-crypto-assistance-for-the-bitcoin-impaired!/;
- Electronic Gulden (EFL): https://bitcointalk.org/index.php?topic=522661.0, https://cryptocointalk.com/topic/8521-electronic-gulden-efl-information/ e http://e-gulden.org/;
- Electronic LIRA (LIRA): https://bitcointalk.org/index.php?topic=561954.0 e https://cryptocointalk.com/topic/10337-annlirex11ipoescrow-electronic-lira-2-days-until-ipo-ends/;
- ElephantCoin (ELP): https://bitcointalk.org/index.php?topic=256501.0 e https://cryptocointalk.com/topic/841-elephantcoin-elp-information/;
- eLira (ELIRA): https://bitcointalk.org/index.php?topic=602142.0 e https://cryptocointalk.com/topic/11273-elira-elira-information/;
- Elitecoin (ELC): https://bitcointalk.org/index.php?topic=702757.0 e https://cryptocointalk.com/topic/13607-elitecoin-elc-information/;

- eMark (DEM): https://bitcointalk.org/index.php?topic=310939.0 e https://cryptocointalk.com/topic/1408-deutsche-emark-dem-information/;
- EmbargoCoin (EBG): https://bitcointalk.org/index.php?topic=574155.0 e https://cryptocointalk.com/topic/11002-embargocoin-ebg-information/;
- Emerald (EMD): https://bitcointalk.org/index.php?topic=235870.0 e https://cryptocointalk.com/topic/613-emerald-emd-information/;
- Emeraldcrypto (EMD): https://bitcointalk.org/index.php?topic=1343027.0 e http://emeraldcrypto.de/;
- EmerCoin (EMC): https://bitcointalk.org/index.php?topic=362513.0, https://cryptocointalk.com/topic/2144-emercoin-emc-information/ e http://emercoin.com/;
- EmiratesCoin (UAE): https://bitcointalk.org/index.php?topic=1476203.0 e https://cryptocointalk.com/topic/10206-pre-annuae-emiratescoin-mintpal-x11-darkgravitywave-ipo/;
- EmotiCoin (EMO): https://bitcointalk.org/index.php?topic=496129.0;
- EMUCoin (EMU): https://bitcointalk.org/index.php?topic=494855.0 e https://cryptocointalk.com/topic/7392-emucoin-emu-information/;
- EnergyCoin (ENRG): https://bitcointalk.org/index.php?topic=589008.0 e https://cryptocointalk.com/topic/10588-energycoin-enrg-information/;
- Entropycoin (ENC): https://bitcointalk.org/index.php?topic=482284.0 e https://cryptocointalk.com/topic/6082-entropycoin-enc-information/;
- EonCoin (EON): https://bitcointalk.org/index.php?topic=573459.0 e https://cryptocointalk.com/topic/10489-eoncoin-eon-information/;
- Equestrianbit (EQB): https://bitcointalk.org/index.php?topic=471712.0 e https://cryptocointalk.com/topic/5314-equestrianbit-eqb-information/;
- Ermahgerdcern (EMG): https://bitcointalk.org/index.php?topic=401099 e https://cryptocointalk.com/topic/2911-ermahgerd-emg-information/;

- ErmisCoin (ERM): https://bitcointalk.org/index.php?topic=822443.0 e https://cryptocointalk.com/topic/19991-erm-ipo2-days-left-lifetime-dual-profit-sharing-dual-buy-support-program-going-registered-cooperative-to-be-govt-backed-community/;
- EscudoPtCoin (ESC): https://bitcointalk.org/index.php?topic=512385.0;
- ESportsCoin (ESC): https://bitcointalk.org/index.php?topic=689852.0 e https://cryptocointalk.com/topic/13663-esportscoin-esc-information/;
- ESportsMoney (ESM): https://bitcointalk.org/index.php?topic=401818.0 e https://cryptocointalk.com/topic/2919-esportsmoney-esm-information/;
- EternalCoin (ETC): https://bitcointalk.org/index.php?topic=423626.0 e https://cryptocointalk.com/topic/3415-eternalcoin-etc-information/;
- EthanCoin (ETHAN): https://bitcointalk.org/index.php?topic=690841.0 e https://cryptocointalk.com/topic/13938-ethancoin-ethan-information/;
- Ethereum (ETH): https://bitcointalk.org/index.php?topic=428589.0, https://cryptocointalk.com/topic/45225-ethereum-eth-information/ e https://www.ethereum.org/;
- EthereumDark (ETD): https://bitcointalk.org/index.php?topic=848304.0 e https://cryptocointalk.com/topic/21505-ethereumdark-edt-information/;
- eToken (ETOK): https://bitcointalk.org/index.php?topic=403597.0 e https://cryptocointalk.com/topic/2974-etoken-etok-information/;
- EuroCoin (EUC): https://bitcointalk.org/index.php?topic=1105215.0 e https://cryptocointalk.com/topic/6991-eurocoin-euc-information/;
- eUtopium (UPM): https://bitcointalk.org/index.php?topic=702380.0 e https://cryptocointalk.com/topic/13879-eutopium-upm-information/;
- EverGreenCoin (EGC): https://bitcointalk.org/index.php?topic=1272091.0 e https://cryptocointalk.com/topic/43888-ann-egc-

ever-green-coin-pow-pos-aimed-at-sustainable-projects-x15-algo/ e http://evergreencoin.org/;

- EvolveCoin (EVC): https://bitcointalk.org/index.php?topic=737226.0 e https://cryptocointalk.com/topic/14190-evolvecoin-evc-information/;
- ExclusiveCoin (EXCL): https://bitcointalk.org/index.php?topic=1546005.0 e https://cryptocointalk.com/topic/17360-exclusivecoin-excl-information/;
- Execoin (EXE): https://bitcointalk.org/index.php?topic=491058.0 e https://cryptocointalk.com/topic/6758-execoin-exe-information/;
- ExileCoin (EXN): https://bitcointalk.org/index.php?topic=369569.0 e https://cryptocointalk.com/topic/2184-exilecoin-exn-information/;
- eXoCoin (EXO): https://bitcointalk.org/index.php?topic=430467.0 e http://exocoin.org/;
- ExtremeCoin (EXC): https://bitcointalk.org/index.php?topic=276609.0 e https://cryptocointalk.com/topic/1025-extremecoin-exc-information/;
- Ezcoin (EZC): https://bitcointalk.org/index.php?topic=220103.0 e https://cryptocointalk.com/topic/390-ezcoin-ezc-information/;
- FaceBookCoin (FBC): https://bitcointalk.org/index.php?topic=585011.0;
- FailCoin (FAIL): https://bitcointalk.org/index.php?topic=505290.0 e https://cryptocointalk.com/topic/11030-failcoin-fail-information/;
- FairBrix: https://bitcointalk.org/index.php?topic=46528.0;
- FairByte (FBT): https://bitcointalk.org/index.php?topic=700920.0 e https://cryptocointalk.com/topic/13496-fairbyte-fbt-information/;
- FairCoin (FAC): https://bitcointalk.org/index.php?topic=702675.0, https://cryptocointalk.com/topic/14817-faircoin-fac-information/ e https://fair-coin.org/;
- FairQuark (FRQ): https://bitcointalk.org/index.php?topic=417700.0 e https://cryptocointalk.com/topic/3275-fairquark-

frq-information/;

- FantomCoin (FCN): https://bitcointalk.org/index.php?topic=598823.0, https://cryptocointalk.com/topic/11162-fantomcoin-fcn-information/ e http://fantomcoin.org/;
- FastCoin (FST): https://bitcointalk.org/index.php?topic=218852.0, https://cryptocointalk.com/topic/387-fastcoin-fst-information/ e http://www.fastcoin.ca/;
- FastCoinSHA (FSS): https://bitcointalk.org/index.php?topic=506452.0 e https://cryptocointalk.com/topic/3085-fastcoinsha-fss-information/;
- FBCoin (XFB): https://bitcointalk.org/index.php?topic=641386.0 e https://cryptocointalk.com/topic/12257-fbcoin-xfb-information/;
- FCKBanksCoin (FCK): https://bitcointalk.org/index.php?topic=407447.0 e https://cryptocointalk.com/topic/3050-fckbanks-fck-information/;
- Feathercoin (FTC): https://bitcointalk.org/index.php?topic=178286.0, https://cryptocointalk.com/topic/122-feathercoin-ftc-information/ e https://www.feathercoin.com/;
- FeatherCoinClassic: https://feathercoinclassic.wordpress.com/;
- Federal Reserve System Coin (FRSC): https://bitcointalk.org/index.php?topic=392043.0;
- FederationCredits (UFC): https://bitcointalk.org/index.php?topic=280114.0 e https://cryptocointalk.com/topic/1063-federationcredits-ufc-information/;
- FedoraCoin (TIPS): https://cryptocointalk.com/topic/2371-fedoracoin-tips-information/ e http://fedoraco.in/;
- FerengiCoin (FER): https://bitcointalk.org/index.php?topic=484841.0 e https://cryptocointalk.com/topic/6268-3-20-annfer-ferengicoin/;
- FerretCoin (FEC): https://bitcointalk.org/index.php?topic=247208.0;
- Fetish: https://bitcointalk.org/index.php?topic=789338.0 e https://cryptocointalk.com/topic/17325-?-?-?-bdsm-fetish-?-?-?/;

- Fibre (FIBRE): https://bitcointalk.org/index.php?topic=737771.0 e https://cryptocointalk.com/topic/14280-fibre-fibre-information/;
- FIFAWCCoin (FWCC): https://bitcointalk.org/index.php?topic=647666.0;
- FileBit (FBIT): https://bitcointalk.org/index.php?topic=722679.0, https://bitcointalk.org/index.php?topic=727418.0 e https://cryptocointalk.com/topic/14042-filebit-fbit-information/;
- FilmCoin (FILM): https://bitcointalk.org/index.php?topic=715458.0 e https://cryptocointalk.com/topic/13843-filmcoin-film-information/;
- FindCoin (FIND): https://bitcointalk.org/index.php?topic=905226.0;
- FinerCoin (XFC): https://bitcointalk.org/index.php?topic=661788.0 e https://cryptocointalk.com/topic/12760-finercoin-xfc-information/;
- Firecoin (FIRE): https://bitcointalk.org/index.php?topic=669757.0 e https://cryptocointalk.com/topic/12868-firecoin-fire-information/;
- FireflyCoin (FFC): https://bitcointalk.org/index.php?topic=318589.0 e https://cryptocointalk.com/topic/1450-fireflycoin-ffc-information/;
- Fitcoin (FIT): https://bitcointalk.org/index.php?topic=608252.0 e https://cryptocointalk.com/topic/11198-fitcoin-fit-information/;
- Flappycoin (FLAP): https://bitcointalk.org/index.php?topic=464743 e https://cryptocointalk.com/topic/5131-flappycoin-flap-information/;
- FlashCoin (FLC): https://bitcointalk.org/index.php?topic=222450.0 e https://cryptocointalk.com/topic/465-flashcoin-flc-information/;
- FloridaCoin (FLC): https://bitcointalk.org/index.php?topic=528967.0 e https://cryptocointalk.com/topic/9146-floridacoin-flc-information/;
- FlorinCoin (FLO): https://bitcointalk.org/index.php?topic=236742.0, https://cryptocointalk.com/topic/621-florincoin-flo-information/ e http://florincoin.org/;

- Floripacoin (FLN): https://bitcointalk.org/index.php?topic=525640.0 e https://cryptocointalk.com/topic/8742-floripacoin-fln-information/;
- FlowerCoin (FLC): https://bitcointalk.org/index.php?topic=717031.0 e https://cryptocointalk.com/topic/13841-flowercoin-flc-information/;
- Fluttercoin (FLT): https://bitcointalk.org/index.php?topic=509499.0 e https://cryptocointalk.com/topic/7068-fluttercoin-flt-information-update-now/;
- Flux (FLX): https://bitcointalk.org/index.php?topic=585314.0, https://bitcointalk.org/index.php?topic=634479 e https://cryptocointalk.com/topic/7060-ann-fluttercoin-flt-pow-pos-and-new-proof-of-block-pob-mining/;
- FlyMeCoin (FlyME): https://bitcointalk.org/index.php?topic=663221.0;
- FootballCoin (FBC): https://bitcointalk.org/index.php?topic=622366.0 e https://cryptocointalk.com/topic/11853-footballcoin-fbc-information/;
- Forexcoin (FRX): https://bitcointalk.org/index.php?topic=517319.0 e https://cryptocointalk.com/topic/8364-forexcoin-frx-information/;
- ForvikCoin (FVK): https://bitcointalk.org/index.php?topic=763462.0 e https://cryptocointalk.com/topic/14784-forvikcoin-fkg-information/;
- FourOhFourCoin (FFC): https://bitcointalk.org/index.php?topic=515642.0;
- FoxCoin (FOX): https://bitcointalk.org/index.php?topic=420727.0 e https://cryptocointalk.com/topic/3451-foxcoin-fox-information/;
- Fractalcoin (FRAC): https://bitcointalk.org/index.php?topic=650173.0 e https://cryptocointalk.com/topic/12308-fractalcoin-frac-information/;
- FrankoCoin: https://bitcointalk.org/index.php?topic=202417.0;
- FreebiesCoin (FREEB): https://bitcointalk.org/index.php?topic=579688.0 e https://cryptocointalk.com/topic/11053-freebiescoin-freeb-information/;

- FreeCoin (FEC): https://bitcointalk.org/index.php?topic=268883.0 e https://cryptocointalk.com/topic/993-freecoin-fec-information/;
- FreedomCoin (FRDC): https://bitcointalk.org/index.php?topic=1172885.0;
- Freicoin (FRC): https://bitcointalk.org/index.php?topic=89843.0 e https://cryptocointalk.com/topic/121-freicoin-frc-information/;
- FreshCoin (FRSH): https://bitcointalk.org/index.php?topic=670939.0 e https://cryptocointalk.com/topic/13141-freshcoin-frsh-information/;
- FrictionlessCoin (FLC): https://bitcointalk.org/index.php?topic=429478.0;
- Friendshipcoin (FSC): https://bitcointalk.org/index.php?topic=461358.0 e https://cryptocointalk.com/topic/5671-friendshipcoin-fsc-information/;
- FriendshipCoin 2 (FSC2): https://bitcointalk.org/index.php?topic=917364.0;
- FrogCoin (FGC): https://bitcointalk.org/index.php?topic=997099.0;
- FrozenCoin (FZ): https://bitcointalk.org/index.php?topic=366762.0 e https://cryptocointalk.com/topic/2104-frozen-fz-information/;
- FryCoin (FRY): https://bitcointalk.org/index.php?topic=449648.0 e https://cryptocointalk.com/topic/4768-frycoin-fry-information/;
- FuckCoin (FUCK): https://bitcointalk.org/index.php?topic=421182.0 e https://cryptocointalk.com/topic/3360-fuckcoin-fuck-information/;
- FuelCoin (FC2): https://bitcointalk.org/index.php?topic=589879.0, https://cryptocointalk.com/topic/10612-annfuel-fuelcoin-charity-project/ e http://fuelcrypto.com/;
- FugueCoin (FC): https://bitcointalk.org/index.php?topic=519138.0 e https://cryptocointalk.com/topic/8259-fuguecoin-fc-information/;
- FujiCoin (FJC): https://bitcointalk.org/index.php?topic=607348.0, https://cryptocointalk.com/topic/11889-fujicoin-

fjc-information/ e http://www.fujicoin.org/;

- FujiCoin 2.0 (FJC): https://bitcointalk4.com/announcements-(altcoins)/(ann)-(fjc)-fujicoin-2-0-japan-launched-june-2014-bleutrade-c-cex/;
- Full Integrity Coin (FIC): https://bitcointalk.org/index.php?topic=837752.0;
- FunCoin (FUN): https://bitcointalk.org/index.php?topic=605315.0;
- FundCoin (FUND): https://bitcointalk.org/index.php?topic=728320.0 e https://cryptocointalk.com/topic/14039-fundcoin-fund-information/;
- FurryCoin (FUR): https://bitcointalk.org/index.php?topic=400815.0 e https://cryptocointalk.com/topic/10919-furrycoin-fur-information/;
- FuseCoin (FUSE): https://bitcointalk.org/index.php?topic=708717.0 e https://cryptocointalk.com/topic/13739-fusecoin-fuse-information/;
- FusionCoin (FSC): https://bitcointalk.org/index.php?topic=512149.0 e https://cryptocointalk.com/topic/8159-fusioncoin-fsc-information/;
- FutureCoin (KFC): https://bitcointalk.org/index.php?topic=565610.0 e https://cryptocointalk.com/topic/10745-futurecoin-kfc-information/;
- FVZcoin (FVZ): https://bitcointalk4.com/announcements-(altcoins)/(ann)(fvz)-fvzcoin-fast-rare-x11-pow/ e https://cryptocointalk.com/topic/13404-fvzcoin-fvz-information/;
- Frycoin (FRY): https://bitcointalk.org/index.php?topic=449648.0 e https://cryptocointalk.com/topic/4768-frycoin-fry-information/;
- G8Coin (G8): https://bitcointalk.org/index.php?topic=667329.0 e https://cryptocointalk.com/topic/12811-launched-today-wwwg8coincom-g8-gold-backed-crypto-currency/;
- GabenCoin (GBN): https://bitcointalk.org/index.php?topic=432600.0 e https://cryptocointalk.com/topic/3674-gabencoin-gbn-information/;
- GaelCoin (GAC): https://bitcointalk.org/index.php?topic=506076.0 e https://cryptocointalk.com/topic/7597-gaelcoin-

gac-information/;

- GalaxyCoin (GLX): https://bitcointalk.org/index.php?topic=252127.0 e https://cryptocointalk.com/topic/804-galaxycoin-glx-information/;
- Galleon (GLN): https://bitcointalk.org/index.php?topic=463817.0 e https://cryptocointalk.com/topic/8374-galleon-gln-information/;
- GaltCoin (GLT): https://bitcointalk.org/index.php?topic=417537.0 e https://cryptocointalk.com/topic/3590-galtcoin-glt-information/;
- Gamecoin (GME): https://bitcointalk.org/index.php?topic=202764.0 e https://cryptocointalk.com/topic/66-gamecoin-gme-information/;
- GameCredits (GMC): http://gamecredits.net/;
- GameCrypto (GEC): https://bitcointalk.org/index.php?topic=666570.0 e https://cryptocointalk.com/topic/12850-gamecrypto-gec/;
- GameLeagueCoin (GML): https://bitcointalk.org/index.php?topic=595779.0 e https://cryptocointalk.com/topic/11064-gameleaguecoin-gml-information/;
- Gamerscoin (GMC): https://bitcointalk.org/index.php?topic=481173.0 e https://cryptocointalk.com/topic/7918-gamerscoin-gmc-information/;
- GapCoin (GAP): https://bitcointalk.org/index.php?topic=822498.0 e https://cryptocointalk.com/topic/12462-pre-ann-gapcoin-prime-gap-based-hashing/;
- GatesCoin (GTC): https://bitcointalk.org/index.php?topic=396936.0 e https://cryptocointalk.com/topic/2766-gatescoin-gtc-information/;
- GayCoin (GAY) https://bitcointalk.org/index.php?topic=465940.0 e https://cryptocointalk.com/topic/5151-gaycoin-gay-information/;
- GB Coin (GBC): https://bitcointalk.org/index.php?topic=530308.0 e https://cryptocointalk.com/topic/10435-gb-coin-gbc-information/;

- GCoin (GCN): https://bitcointalk.org/index.php?topic=665858.0, https://cryptocointalk.com/topic/13065-gcoin-gcn-information/ e http://www.gcoin.us/;
- GeistGeld (GG): https://bitcointalk.org/index.php?topic=42417.0 e https://cryptocointalk.com/topic/35-gg-geistgeld/;
- GenesisCoin (GNS): https://bitcointalk.org/index.php?topic=1096804.0 e https://cryptocointalk.com/topic/8264-genesiscoin-gns-information/;
- GeoCoin (GEO): https://bitcointalk.org/index.php?topic=923995.0 e http://geocoin.cash/;
- GermanyCoin (GER): https://bitcointalk.org/index.php?topic=523083.0 e https://cryptocointalk.com/topic/8626-germanycoin-ger-information/;
- GetGems (GEMZ): https://bitcointalk.org/index.php?topic=758004.0 e http://getgems.org/;
- GhostCoin (GHC): https://bitcointalk.org/index.php?topic=509522.0 e https://cryptocointalk.com/topic/7801-ghostcoin-ghc-information/;
- GiarCoin (GIARCOC): https://bitcointalk.org/index.php?topic=545529.0 e https://cryptocointalk.com/topic/10408-giarcoin-giarcoc-information/;
- GiftCoin (GFT): https://bitcointalk.org/index.php?topic=392465.0 e https://cryptocointalk.com/topic/2670-giftcoin-gft-information/;
- GILCoin (GIL): https://bitcointalk.org/index.php?topic=255844.0 e https://cryptocointalk.com/topic/838-gil-gil-information/;
- GirlCoin (GIRL): https://bitcointalk.org/index.php?topic=573917.0 e https://cryptocointalk.com/topic/10491-girlcoin-girl-information/;
- GiveCoin (GIVE): https://bitcointalk.org/index.php?topic=529181.0 e https://cryptocointalk.com/topic/10433-givecoin-give-information/;
- GlobalBoost (BST): https://bitcointalk.org/index.php?topic=584865.0 e https://cryptocointalk.com/topic/10517-globalboost-bst-information/;

- GlobalBoost-Y (BSTY): https://bitcointalk.org/index.php?topic=775289.0;
- GlobalCoin (GLC): https://bitcointalk.org/index.php?topic=243911.0 e https://cryptocointalk.com/topic/732-globalcoin-glc-information/;
- GlobalDenomination (GDN): https://bitcointalk.org/index.php?topic=578574.0 e https://cryptocointalk.com/topic/10503-global-denomination-gdn-information/;
- GlobeCoin (GLB): https://bitcointalk.org/index.php?topic=360255.0 e https://cryptocointalk.com/topic/2473-glb-globe-christmas-giveaway-free-globes/;
- Glyphcoin (GLYPH): https://bitcointalk.org/index.php?topic=644141.0 e https://cryptocointalk.com/topic/12621-glyphcoin-glyph-information/;
- Gnosis (GNS): https://bitcointalk.org/index.php?topic=782154.0 e https://cryptocointalk.com/topic/16080-gnosis-gns-information/;
- GoatCoin (GOAT): https://bitcointalk.org/index.php?topic=430858.0 e https://cryptocointalk.com/topic/3587-goatcoin-goat-information/;
- GodCoin (GOD): https://bitcointalk.org/index.php?topic=649099.0 e https://cryptocointalk.com/topic/12737-godcoin-god-information/;
- GoldCoin (GLD): https://bitcointalk.org/index.php?topic=317568.0, https://cryptocointalk.com/topic/43025-goldcoin-gld-giveaway/ e http://www.gldcoin.com/;
- Golden Loaf Yanukovich (GLY): https://bitcointalk.org/index.php?topic=685042.0 e https://cryptocointalk.com/topic/13229-8-20golden-loaf-yanukovich-gly/;
- GoldFlexibly (JRY): https://cryptocointalk.com/topic/1264-goldflexibly-jry-information/;
- GoldPieces (GP): https://bitcointalk.org/index.php?topic=915899.0;

- Gold Pressed Latinum (GLP): https://bitcointalk.org/index.php?topic=1392930.0 e https://cryptocointalk.com/topic/1103-goldpressedlatinum-gpl-information/;
- GoldReserveCoin (XRG): https://bitcointalk.org/index.php?topic=641064.0 e https://cryptocointalk.com/topic/12159-goldreserve-xgr-information/;
- GollumCoin (GLM): https://bitcointalk.org/index.php?topic=548093.0 e https://cryptocointalk.com/topic/9306-3-30-annglmgollumcoinscrypt/;
- GoodCoin (GOOD): https://bitcointalk.org/index.php?topic=578963.0 e https://cryptocointalk.com/topic/11123-goodcoin-good-information/;
- GoxCoin (GOX): https://bitcointalk.org/index.php?topic=481185.0 e https://cryptocointalk.com/topic/7808-mtgoxcoin-gox-information/;
- GPUCoin (GPUC): https://bitcointalk.org/index.php?topic=469887.0 e https://cryptocointalk.com/topic/7070-gpucoin-gpuc-information/;
- GrainCoin (GRA): https://bitcointalk.org/index.php?topic=361503.0 e https://cryptocointalk.com/topic/2011-grain-gra-information/;
- GrandCoin (GDC): https://bitcointalk.org/index.php?topic=255629.0, https://cryptocointalk.com/topic/835-grandcoin-gdc-information/ e http://grandcoin.org/;
- GraniteCoin (GRN): https://bitcointalk.org/index.php?topic=621544.0 e https://cryptocointalk.com/topic/11588-granitecoin-grn-information/;
- Graphene (GRP): https://bitcointalk.org/index.php?topic=527890.0 e https://cryptocointalk.com/topic/9138-graphene-grp-information/;
- GreatBritainCoin (GBR): https://bitcointalk.org/index.php?topic=413168.0;
- GreeceCoin (GRCE): https://bitcointalk.org/index.php?topic=516955.0 e https://cryptocointalk.com/topic/8737-greececoin-grce-information/;

- GreekCoin (GRK): https://bitcointalk.org/index.php?topic=637529.0 e https://cryptocointalk.com/topic/12122-greekcoin-grk-information/;
- GreenBacks (GB): https://bitcointalk.org/index.php?topic=740744.0 e https://cryptocointalk.com/topic/14515-greenbacks-gb-information/;
- GreenCoin (GRE): https://bitcointalk.org/index.php?topic=636548.0, https://cryptocointalk.com/topic/12396-greencoin-gre-information/ e http://www.grcoin.com/;
- GridBit (GRID): https://bitcointalk.org/index.php?topic=740955.0 e https://cryptocointalk.com/topic/14281-gridbit-grid-information/;
- GridCoin (GRC): https://bitcointalk.org/index.php?topic=324118.0, https://cryptocointalk.com/topic/1331-new-coin-launch-announcement-grc-gridcoin/ e http://www.gridcoin.us/;
- GrifCoin: https://bitcointalk.org/index.php?topic=635736.0;
- GroestlCoin (GRS): https://bitcointalk.org/index.php?topic=525926.0, https://cryptocointalk.com/topic/8739-groestlcoin-grs-information/ e http://www.groestlcoin.org/;
- GroinCoin: http://groincoin.com/;
- GroupCoin (GPC): https://cryptocointalk.com/topic/13968-groupcoin-gpc-information/;
- GrowthCoin (GRW): https://bitcointalk.org/index.php?topic=267019.0 e https://cryptocointalk.com/topic/947-growthcoin-grw-information-old/;
- GrumpyCoin (GRUMP): https://bitcointalk.org/index.php?topic=403936.0 e https://cryptocointalk.com/topic/2962-grumpycoin-grump-information/;
- GryfenCoin (GRYF): https://bitcointalk.org/index.php?topic=687216.0 e https://cryptocointalk.com/topic/15937-gryfencoin-gryf-information/;
- GSMCoin (GSM): https://bitcointalk.org/index.php?topic=964014.0 e https://cryptocointalk.com/topic/31391-???-ann-gsmcoin-x11-???-gsm-network-freedom-70ghs/;
- GuarantCoin (GTC): https://bitcointalk.org/index.php?topic=581679.0;

- Guarany (GUA): https://bitcointalk.org/index.php?topic=900091.0, https://cryptocointalk.com/topic/22552-ann-guarany-the-original-brazilian-cryptocurrency-gua/ e http://guarany.co/;
- GuerillaCoin (GUE): https://bitcointalk.org/index.php?topic=656167.0 e https://cryptocointalk.com/topic/12584-guerillacoin-gue-information/;
- Guinea (GUINEA): https://bitcointalk.org/index.php?topic=684159.0 e https://cryptocointalk.com/topic/13212-guinea-guinea-information/;
- GuldenCoin (NLG): https://bitcointalk.org/index.php?topic=554412.0, https://cryptocointalk.com/topic/41623-nlg-gulden-guldencom-—-important-update-155/ e https://guldenpay.com/;
- GunCoin (GUN): https://bitcointalk.org/index.php?topic=498671.0, https://cryptocointalk.com/topic/10674-guncoin-gun-information/ e http://guncoin.info/;
- GyteCoin (GEC): https://bitcointalk.org/index.php?topic=776454.0;
- H2OCoin (H2O): https://bitcointalk.org/index.php?topic=494229.0 e https://cryptocointalk.com/topic/8982-h2ocoin-h2o-information/;
- HadokenCoin (HDK): https://bitcointalk.org/index.php?topic=598223.0 e https://cryptocointalk.com/topic/11120-hadokencoin-hdk-information/;
- Halcyon (HAL): https://bitcointalk.org/index.php?topic=741728.0 e https://cryptocointalk.com/topic/14272-halcyon-hal-information/;
- HamburgerCoin (HAC): https://bitcointalk.org/index.php?topic=431512.15 e https://cryptocointalk.com/topic/2859-hamburgercoin-hac-information/;
- HamRadioCoin (HAM): https://bitcointalk4.com/announcements-(altcoins)/(ann)-ham-hamradiocoin-sha-256-crypto-on-the-radio!-official-thread/, https://cryptocointalk.com/topic/13009-hamradiocoin-ham-information/ e http://www.hamradiocoin.com/;

- HansaCoin (HANSA): https://bitcointalk.org/index.php?topic=921745.0;
- HappyCoin (HPY): https://bitcointalk.org/index.php?topic=616114.0;
- HarCoin (HAR): https://bitcointalk.org/index.php?topic=792861.0;
- Hardcider (WHC): https://bitcointalk.org/index.php?topic=670746.0 e https://cryptocointalk.com/topic/13013-hardcider-whc-information/;
- Harmonycoin (HMY): https://bitcointalk.org/index.php?topic=639835.0 e https://cryptocointalk.com/topic/12461-harmonycoin-hmy-information/;
- HashCoin (HASH): https://bitcointalk.org/index.php?topic=560955.0 e https://cryptocointalk.com/topic/10828-hashcoin-hash-information/;
- HawaiiCoin (HIC): https://bitcointalk.org/index.php?topic=508506.0 e https://cryptocointalk.com/topic/9316-hawaiicoin-hic-information/;
- HeavyCoin (HVC): https://bitcointalk.org/index.php?topic=470391.0 e https://cryptocointalk.com/topic/7661-heavycoin-hvc-information/;
- Heisenberg (HEX): https://bitcointalk.org/index.php?topic=502589.0 e https://cryptocointalk.com/topic/7526-heisenberg-hex-information/;
- HelixCoin (HXC): https://bitcointalk.org/index.php?topic=489172.0 e https://cryptocointalk.com/topic/6839-helixcoin-hxc-information/;
- HellenicCoin (HNC): https://bitcointalk.org/index.php?topic=950020.0;
- HelveticaCoin (CHC): https://bitcointalk.org/index.php?topic=631899.0 e https://cryptocointalk.com/topic/11875-helveticacoin-chc-information/;
- HempCoin (THC): https://bitcointalk.org/index.php?topic=506320.0;
- HeroCoin (HRC): https://bitcointalk.org/index.php?topic=466679.0 e https://cryptocointalk.com/topic/5691-herocoin-hrc-information/;

- HertzCoin (HZ): https://bitcointalk.org/index.php?topic=736313.0 e https://cryptocointalk.com/topic/14192-hertzcoin-hz-information/;
- HighFiveCoin (H5C): https://bitcointalk.org/index.php?topic=558286.0 e https://cryptocointalk.com/topic/9812-annh5c-highfivecoin-?x11?-launched/;
- HiroCoin (HIRO): https://bitcointalk.org/index.php?topic=516349.0 e https://cryptocointalk.com/topic/8139-hirocoin-hiro-information/;
- HispaCoin (HPC): https://bitcointalk.org/index.php?topic=1331971.0 e https://cryptocointalk.com/topic/7989-hispacoin-hpc-information/;
- HobbitCoin (HBC): https://bitcointalk.org/index.php?topic=437947.0 e https://cryptocointalk.com/topic/4018-hobbitcoin-hbc-information/;
- HoboNickels (HBN): https://bitcointalk.org/index.php?topic=261550.0, https://cryptocointalk.com/topic/881-hobonickels-hbn-information/, http://www.hobonickels.org/ e http://hobonickels.info/;
- HodorCoin (HODOR): https://bitcointalk.org/index.php?topic=665818 e https://cryptocointalk.com/topic/12764-hodorcoin-hodor-information/;
- HongKetoCoin (HKC): https://bitcointalk.org/index.php?topic=612919.0 e https://cryptocointalk.com/topic/11377-hongketocoin-hkc-information/;
- HongKongCoin (HKC): https://bitcointalk.org/index.php?topic=518669.0 e https://cryptocointalk.com/topic/8225-hongkongcoin-hkc-information/;
- Honorcoin (XHC): https://bitcointalk.org/index.php?topic=639043.0 e http://www.honorcoin.org;
- Horizon (HZ): https://bitcointalk.org/index.php?topic=823785.0;
- HorseCoin (HORS): https://bitcointalk.org/index.php?topic=489289.0 e https://cryptocointalk.com/topic/6973-horsecoin-hors-information/;
- HorusCoin (RX): https://bitcointalk.org/index.php?topic=640303.0 e https://cryptocointalk.com/topic/12085-

horuscoin-rx-information/;

- Hotcoin (HOT): https://bitcointalk.org/index.php?topic=382947.0 e https://cryptocointalk.com/topic/2453-hotcoin-hot-information/;
- HouseOfCoins (HOC): https://bitcointalk.org/index.php?topic=553599.0 e https://cryptocointalk.com/topic/10506-houseofcoins-hoc-information/;
- HtmlCoin (HTML5): https://bitcointalk.org/index.php?topic=801489.0, https://cryptocointalk.com/topic/17467-htmlcoin-html5-information/ e http://www.htmlcoin.com/;
- HuateCoin (HUC): https://bitcointalk.org/index.php?topic=417143.0 e https://cryptocointalk.com/topic/3285-huatecoin-huc-information/;
- Huitong (HTC): https://bitcointalk.org/index.php?topic=308713.0 e https://cryptocointalk.com/topic/1385-huitong-htc-information/;
- HunterCoin (HUC): https://bitcointalk.org/index.php?topic=435170.0, https://cryptocointalk.com/topic/4121-huntercoin-huc-information/ e http://huntercoin.org/;
- HuskyCoin (HC): https://bitcointalk.org/index.php?topic=615268.0 e https://cryptocointalk.com/topic/11241-huskycoin-hc-information/;
- Hyper (HYPER): https://cryptocointalk.com/topic/11669-hyper-hyper-information/;
- Hypercoin (HYC): https://bitcointalk.org/index.php?topic=218737.0;
- HyperStake (HYP): https://bitcointalk.org/index.php?topic=678849.0, https://cryptocointalk.com/topic/13145-hyperstake-hyp-information/ e http://hyperstake.com/;
- I0coin (I0C): https://bitcointalk.org/index.php?topic=624935.0, https://cryptocointalk.com/topic/1096-i0coin-i0c-information/ e http://izerocoin.org/;
- I/O Coin (IOC): https://bitcointalk.org/index.php?topic=695855.0, https://cryptocointalk.com/topic/13690-iocoin-io-information/ e http://iocoin.io/;
- Iaurab (IAURAB): https://bitcointalk.org/index.php?topic=623193.0 e https://cryptocointalk.com/topic/11705-pre-

anniaurab-iaurab-coin-x11-algo-7-days-mining-pos-pow-androidiphone-wallet/;

- Icebergcoin (ICB): https://bitcointalk.org/index.php?topic=673524.0;
- Icoin (ICN): https://bitcointalk.org/index.php?topic=407866.0 e https://cryptocointalk.com/topic/2620-icoin-icn-information/;
- IconicX (ICNX): https://bitcointalk.org/index.php?topic=840139.0 e https://cryptocointalk.com/topic/21066-iconicx-icnx-information/;
- Ilcoin: https://bitcointalk.org/index.php?topic=1269380.0 e https://bitcointalk4.com/announcements-(altcoins)/ilcoin-new-e-currency/;
- ImaCredit (IMA): https://bitcointalk.org/index.php?topic=768704.0 e https://cryptocointalk.com/topic/14859-ann-imacredit-coin-official-annoucement/;
- Imperialcoin (IPC): https://bitcointalk.org/index.php?topic=476091.0 e http://imperialcoin.org/;
- IncaKoin: https://bitcointalk.org/index.php?topic=933851.0 e https://cryptocointalk.com/topic/42513-ann-incakoin-l-crowdfunding-to-support-development-android-wallet-released/;
- IncogCoin (ICG): https://bitcointalk.org/index.php?topic=702336.0 e https://cryptocointalk.com/topic/13691-incogcoin-icg-information/;
- IndoCoin (IDC): https://bitcointalk.org/index.php?topic=612311.0 e https://cryptocointalk.com/topic/11524-indocoin-idc-information/;
- Industrycoin (IND): https://cryptocointalk.com/topic/4293-industrycoin-ind-information-on-exchnage-btc-ltc/;
- Infinitecoin (IFC): https://bitcointalk.org/index.php?topic=225891.0, https://cryptocointalk.com/topic/509-infinitecoin-ifc-information/ e http://www.infinitecoin.com/;
- Infinium-8 (INF8): https://bitcointalk.org/index.php?topic=698727.0 e https://cryptocointalk.com/topic/13511-infinium-8-inf8-information/;

- InformationCoin (ITC): https://bitcointalk.org/index.php?topic=578723.0 e https://cryptocointalk.com/topic/10751-informationcoin-itc-information/;
- INKcoin (INK): https://bitcointalk.org/index.php?topic=481516.0 e https://cryptocointalk.com/topic/6048-inkcoin-ink-information/;
- InnovationCoin (IVC): https://bitcointalk.org/index.php?topic=575636.0 e https://cryptocointalk.com/topic/6867-ivycoin-ivc-information/;
- InsanityCoin: https://bitcointalk.org/index.php?topic=471166.0 e https://cryptocointalk.com/topic/5707-annwolf-insanitycoin-coin-for-investors-and-traders/;
- InstaMineNuggets ($MINE): https://bitcointalk.org/index.php?topic=968028.0, https://bitcointalk.org/index.php?topic=988166.0 e https://cryptocointalk.com/topic/31330-instaminenuggets-exchange-ticker-symbol-mine/;
- InstaMineNuggets A ($MINEW): http://coinmarketcap.com/currencies/instaminenuggets-minew/;
- InstaMineNuggets B ($MINEZ): http://coinmarketcap.com/currencies/instaminenuggets-minez/;
- Instantcoin (BTI): https://bitcointalk.org/index.php?topic=693243.0 e https://cryptocointalk.com/topic/13699-bitcoininstant-btisha-256-based-bitcoin-with-progressive-difficulty-re-target-pow-1-coin-per-block-and-250-thousand-total-coins/;
- InstantDEX (DEX): https://bitco.in/forum/threads/instantdex-decentralized-shapeshift-proof-of-concept.1287/ e http://www.instantdex.org/;
- Intellicoin (INT): https://bitcointalk.org/index.php?topic=720292.0 e https://cryptocointalk.com/topic/14231-intellicoin-int-information/;
- InterCoin (INC): https://bitcointalk.org/index.php?topic=384113.0;
- Involution (INV): https://bitcointalk.org/index.php?topic=624109.0;

- IrCoin (IRC): https://bitcointalk.org/index.php?topic=557397.0 e https://cryptocointalk.com/topic/9613-annirc-ircoin-scrypt/;
- IrishCoin: https://bitcointalk.org/index.php?topic=612983.0 e http://irishcoin.org/;
- IsisCoin (https://bitcointalk.org/index.php?topic=675509.0 e https://forum.bits.media/index.php?/topic/8576-isis-isiscoin-x15/;
- IsraCoin (ISR): https://bitcointalk.org/index.php?topic=529409.0 e https://cryptocointalk.com/topic/9159-isracoin-isr-information/;
- Italycoin (ITC): https://cryptocointalk.com/topic/1207-italycoin-itc-information/;
- IvugeoEvolutionCoin: https://cryptocointalk.com/topic/40039-anniecivugeoevolutioncoinscryptpowmobile-wallet-faucet-relased/ e http://www.ivugeocoin.com/;
- IvyCoin (IVY): https://bitcointalk.org/index.php?topic=493495.0 e https://cryptocointalk.com/topic/6867-ivycoin-ivc-information/;
- IxCoin (IXC): https://bitcointalk.org/index.php?topic=36218.0, https://cryptocointalk.com/topic/124-ixcoin-ixc-information/ e http://www.ixcoin.co/?lang=pt;
- JackpotCoin (JPC): https://bitcointalk.org/index.php?topic=584481.0, https://cryptocointalk.com/topic/10428-annjackpotjackpotcoin-mandatory-update-block-6000/ e http://explorer.jpcpal.com/;
- JadeCoin (JADE): https://bitcointalk.org/index.php?topic=728567.0 e https://cryptocointalk.com/topic/14038-jadecoin-jade-information/;
- JCoin: https://bitcointalk.org/index.php?topic=264556.0;
- JebigaCoin (JBG): https://bitcointalk.org/index.php?topic=530408.0 e https://cryptocointalk.com/topic/9476-jebigacoin-jbg-information/;
- JennyCoin (JNY): https://bitcointalk.org/index.php?topic=527919.0 e https://cryptocointalk.com/topic/10414-jennycoin-jny-information/;

- JerkyCoin (JKY): https://cryptocointalk.com/topic/3036-jerkycoin-jky-information/;
- Jinn: https://nxtforum.org/news-and-announcements/(ann)-jinn/;
- JohnKeyoin: https://bitcointalk.org/index.php?topic=626705.10 e https://cryptocointalk.com/topic/11708-annninja-johnkeyoin-key/;
- JoinCoin (J): https://bitcointalk.org/index.php?topic=737405.0 e https://cryptocointalk.com/topic/14184-annjoincoin-j-tor-anonymous-all-algorithm-mining-15-day-pre-sale-on-c-cex/;
- JouleCoin (XJO): https://bitcointalk.org/index.php?topic=299308.0 e https://cryptocointalk.com/topic/1222-joulecoin-xjo-information/;

- JudgeCoin (JUDGE): https://bitcointalk.org/index.php?topic=666335.0 e https://cryptocointalk.com/topic/13101-judgecoin-judge-information/;
- JuggaloCoin (JUG): https://bitcointalk.org/index.php?topic=555896.0 e https://cryptocointalk.com/topic/11342-juggalocoin-jug-information/;
- JumBucks (JBS): https://bitcointalk.org/index.php?topic=765082.0 e https://cryptocointalk.com/topic/14865-jumbucks-jbs-information/;
- JunkCoin (JKC): https://bitcointalk.org/index.php?topic=194756.0 e https://cryptocointalk.com/topic/111-junkcoin-jkc-information/;
- JupiterCoin (JPC): https://bitcointalk.org/index.php?topic=1268962.0 e https://cryptocointalk.com/topic/846-jupitercoin-jpc-information/;
- KaChingCoin (KAC): https://bitcointalk.org/index.php?topic=509880.0 e https://cryptocointalk.com/topic/7797-ann-kac-kachingcoin-200-coins-per-block-etc/;
- KakaCoin (KKC): https://bitcointalk.org/index.php?topic=437085.0 e https://cryptocointalk.com/topic/3833-kakacoin-kkc-information/;
- Karmacoin (KARM): https://bitcointalk.org/index.php?topic=447657.0 e https://cryptocointalk.com/topic/4306-karma-karm-information/;
- KarpelesCoin (KAR): https://bitcointalk.org/index.php?topic=511457.0 e https://cryptocointalk.com/topic/9359-karpelescoin-kar-information/;
- KashmirCoin (KSC): https://bitcointalk.org/index.php?topic=550728.0 e https://cryptocointalk.com/topic/9382-ksc-rare-kashmircoin-1001-coins-max-worth-4x-more-than-bitcoin-launched/;
- KeyCoin (KEY): https://bitcointalk.org/index.php?topic=695457.0 e https://cryptocointalk.com/topic/13385-keycoin-key-information/;
- KibweeCoin (KIB): https://bitcointalk.org/index.php?topic=642933.0 e https://cryptocointalk.com/topic/12021-13-june-

kibweecoin-powpocpos-0-premine-new-proof-of-contribution-system-sources-release-today/;

- KillerCoin (KILR): https://bitcointalk.org/index.php?topic=530736.0 e https://cryptocointalk.com/topic/9234-killercoin-kilr-information/;
- KimoCoin (KMC): https://bitcointalk.org/index.php?topic=524216.0 e https://cryptocointalk.com/topic/10516-kimocoin-kmc-information/;
- KingCoin (KING): https://bitcointalk.org/index.php?topic=278834.0 e https://cryptocointalk.com/topic/1055-kingcoin-king-information/;
- KittehCoin (MEOW): https://bitcointalk.org/index.php?topic=383068.0 e https://cryptocointalk.com/topic/2463-kittehcoin-meow-information/;
- KiwiCoin (KIWI): https://bitcointalk.org/index.php?topic=637004.0, https://cryptocointalk.com/topic/12140-kiwicoin-kiwi-information/ e http://kiwicoin.pw/;
- Klingon Darsek (KED): https://bitcointalk.org/index.php?topic=377997.0, https://bitcointalk.org/index.php?topic=468388.0 e https://cryptocointalk.com/topic/2739-ked-klingon-darsek-giveaway/;
- KlondikeCoin (KDC): https://bitcointalk.org/index.php?topic=407705.0 e https://cryptocointalk.com/topic/3056-klondike-kdc-information/;
- Kolschcoin (CGN): https://bitcointalk.org/index.php?topic=1019421.0, https://cryptocointalk.com/topic/38293-cgn-kolschcoin-giveaway/ e http://www.coin.cologne/;
- Koolio (KOOL): https://bitcointalk.org/index.php?topic=686727.0 e https://cryptocointalk.com/topic/13302-kooliocoin-kool-information/;
- KoreCoin (KORE): https://bitcointalk.org/index.php?topic=652700.0 e https://cryptocointalk.com/topic/12397-korecoin-kore-information/;
- KrugerCoin (KGC): https://bitcointalk.org/index.php?topic=246803.0 e https://cryptocointalk.com/topic/756-krugercoin-kgc-information/;

- Kryptkoin (KTK): https://bitcointalk.org/index.php?topic=606809.0 e https://cryptocointalk.com/topic/38830-kryptkoin-ktk-faucet/;
- Kryptonite (KRYP): https://bitcointalk.org/index.php?topic=606682.0 e https://cryptocointalk.com/topic/11623-kryptonite-kryp-information/;
- KuberCoin (KBC): https://bitcointalk.org/index.php?topic=519091.0;
- KudosCoin: https://bitcointalk.org/index.php?topic=307024.140;
- Kumacoin (KUMA): https://bitcointalk.org/index.php?topic=585772.0;
- Latium (LAT): https://bitcointalk.org/index.php?topic=610614.0 e https://cryptocointalk.com/topic/11294-latium/;
- Latinumcoin (LTM): https://bitcointalk.org/index.php?topic=620246.0;
- LaurabCoin (LAURAB): https://bitcointalk.org/index.php?topic=623193.0;
- LBRY: https://bitcointalk.org/index.php?topic=1551021.0 e https://cryptocointalk.com/topic/48533-lbry-play-share-earn-next-big-thing-in-crytpo-earn-001-btc-ref/;
- LeaCoin (LEA): https://bitcointalk.org/index.php?topic=1006917.0 e http://leacoin.org/;
- LeadCoin (LDC): https://bitcointalk.org/index.php?topic=382404.0 e https://cryptocointalk.com/topic/2863-leadcoin-ldc-information/;
- LeafCoin (LEAF): https://bitcointalk.org/index.php?topic=430091.0 e https://cryptocointalk.com/topic/3597-leafcoin-leaf-information/;
- Leaguecoin (LOL): https://bitcointalk.org/index.php?topic=622801.0 e https://cryptocointalk.com/topic/12045-leaguecoin-lol-information/;
- Lebowskis (LBW): https://bitcointalk.org/index.php?topic=260311.0, https://cryptocointalk.com/topic/1009-the-big-lebowski-short-version/ e http://lebowski.criptomonedas.tel/;
- Legendarycoin (LGD): https://bitcointalk.org/index.php?topic=530175.0 e https://cryptocointalk.com/topic/9458-

legendarycoin-lgd-information/;

- LemonCoin (LMC): https://bitcointalk.org/index.php?topic=1392177.0 e https://cryptocointalk.com/topic/4907-lemoncoin-lmc-information/;
- LemurCoin (LMR): https://bitcointalk.org/index.php?topic=739681.0 e https://cryptocointalk.com/topic/14299-lemurcoin-lmr-information/;
- LEOcoin: https://bitcointalk.org/index.php?topic=1289299.0, https://cryptocointalk.com/topic/46135-ann-leocoin-official-leocoin-thread-updated/, https://bitcointalk4.com/announcements-(altcoins)/ann-leocoin-official-leocoin-thread-(moderated-by-leocoin-foundation)/, http://www.leocoin.org/ e http://leocoinfoundation.org/;
- LeproCoin (LPC): https://bitcointalk.org/index.php?topic=398722.0 e https://cryptocointalk.com/topic/2810-leprocoin-lpc-information/,
- LFTCCoin (LFTC): https://bitcointalk.org/index.php?topic=841568.0;
- LibertyCoin (XLB): https://bitcointalk.org/index.php?topic=600322.0 e https://cryptocointalk.com/topic/11007-libertycoin-xlb-information/;
- LibrexCoin (LXC): https://bitcointalk.org/index.php?topic=703042.0 e https://cryptocointalk.com/topic/13911-librexcoin-lxc-information/;
- LightCoin (LIT): https://bitcointalk.org/index.php?topic=649890.0 e https://cryptocointalk.com/topic/12343-lightcoin-lit-information/;
- LightSpeed (LSD): https://bitcointalk.org/index.php?topic=769832.0 e https://cryptocointalk.com/topic/15156-lightspeed-lsd-information/;
- LimeCoin (LIM): https://bitcointalk.org/index.php?topic=559534.0 e https://cryptocointalk.com/topic/10431-limecoin-lim-information-old/;
- LimeCoinLite (LCL): https://cryptocointalk.com/topic/11448-limecoinlite-lcl-information/;

- LimeCoinX (LIMX): https://bitcointalk.org/index.php?topic=637366.0 e http://www.limx.eu/;
- LinearCoin (LNC): https://bitcointalk.org/index.php?topic=656845.0;
- LionCoin (LION): https://bitcointalk.org/index.php?topic=871052.0 e https://cryptocointalk.com/topic/8366-lioncoin-lic-information/;
- LiquidCoin (LQD): https://bitcointalk4.com/announcements-(altcoins)/liquid-(ethereum-fork)/, http://www.liquidtech.info/ e https://www.liquid-crypto.com/;
- Lira Elettronica (LIRA): https://bitcointalk.org/index.php?topic=562800.0 e https://cryptocointalk.com/topic/10681-lira-elettronica-lira-information/;
- Litebar (LTB): https://bitcointalk.org/index.php?topic=1413832.0 e https://cryptocointalk.com/topic/46068-ann-litbar-ltb-reborn-sub-bitbar-has-a-little-brother/;
- LiteCoin (LTC): https://bitcointalk.org/index.php?topic=47417.0, https://cryptocointalk.com/topic/140-litecoin-ltc-information/ e https://litecoin.com/;
- LiteCoinDark (LTCD): https://bitcointalk.org/index.php?topic=760143.0, https://cryptocointalk.com/topic/14883-litecoindark-ltcd-information/ e http://www.litecoindark.com/;
- LiteCoinPlus (XLC): https://bitcointalk.org/index.php?topic=599095.0 e https://cryptocointalk.com/topic/12757-litecoinplus-xlc-information/;
- LiteCoinX (LTCX): https://bitcointalk.org/index.php?topic=624378.0 e https://cryptocointalk.com/topic/11763-litecoinx-ltcx-information/;
- LiteDoge (DOGE): https://bitcointalk.org/index.php?topic=1077390.0 e https://cryptocointalk.com/topic/38317-litedoge-very-currency-many-coin-lite-version-of-dogecoin/;
- LiteStarCoin (LTS): https://bitcointalk.org/index.php?topic=959292.0;
- LithiumCoin (LIT): https://bitcointalk.org/index.php?topic=810688.0 e https://cryptocointalk.com/topic/18799-lithiumcoin-lit-information/;

- LiveCoin (LVC): https://bitcointalk.org/index.php?topic=1428405.0 e https://cryptocointalk.com/topic/3012-livecoin-lvc-information/;
- Lizarde (LIZE): https://bitcointalk.org/index.php?topic=683741.0 e https://cryptocointalk.com/topic/13428-lizarde-lize-information/;
- LockCoin (LOCK): https://bitcointalk.org/index.php?topic=682408.0 e https://cryptocointalk.com/topic/13271-lockcoin-lock-information/;
- LogiCoin (LGC): https://bitcointalk.org/index.php?topic=567114.0 e https://cryptocointalk.com/topic/10639-logicoin-lgc-information/;
- LogosCoin (LGS): https://bitcointalk.org/index.php?topic=842719.0 e https://cryptocointalk.com/topic/12039-logos-lgs-information/;
- LolCoin (LOL): https://bitcointalk.org/index.php?topic=471249.0;
- LongCoin (LNG): https://bitcointalk.org/index.php?topic=711982.0 e https://cryptocointalk.com/topic/13969-longcoin-lng-information/;
- LottoCoin (LOT): https://bitcointalk.org/index.php?topic=368153.0, https://cryptocointalk.com/topic/2167-lottocoin-lot-information/ e http://lottocoin.org/;
- LottoShares (LTS): https://bitcointalk.org/index.php?topic=694341.0 e https://cryptocointalk.com/topic/45361-ann-%C4%A7-hodl-interest-on-all-balances-huge-bonuses-for-early-adopters-3500/;
- LotusCoin (LTS): https://bitcointalk.org/index.php?topic=658104.0 e https://cryptocointalk.com/topic/12899-lotuscoin-lts-information/;
- LoveCoin (LOVE): https://bitcointalk.org/index.php?topic=550452.0 e https://cryptocointalk.com/topic/2157-lovecoin-love-information/;
- Lucky7Coin (LK7); https://bitcointalk.org/index.php?topic=295157.0 e https://cryptocointalk.com/topic/1201-lucky7coin-lk7-information/;

- LuckyCoin (LKY): https://bitcointalk.org/index.php?topic=214614.0 e https://bitcointalk.org/index.php?topic=568287.0;
- LycanCoin (LYC): https://bitcointalk.org/index.php?topic=455770.0 e https://cryptocointalk.com/topic/5244-lycancoin-lyc-information/;
- M.JCoin (M.J): https://bitcointalk.org/index.php?topic=665964.0 e https://cryptocointalk.com/topic/13001-mjcoin-mj-information/;
- MACDCoin (MACD): https://bitcointalk.org/index.php?topic=683253.0 e https://cryptocointalk.com/topic/12861-macdcoin-macd-information/;
- MachineCoin (MAC): https://bitcointalk.org/index.php?topic=434190.0 e https://cryptocointalk.com/topic/3697-mac-machinecoin-the-steampunk-cryptocurrency-now-with-timetravel-pow/;
- MachineryCoin (MHYC): https://bitcointalk.org/index.php?topic=630205.0 e https://cryptocointalk.com/topic/12284-machinerycoin-mhyc-information/;
- MacroCoin (MCR): https://bitcointalk.org/index.php?topic=455269.0 e https://cryptocointalk.com/topic/4850-macrocoin-mcr-information/;
- MadCowCoin (MCC): https://bitcointalk.org/index.php?topic=511988.0;
- Magic Internet Money (MIM): https://bitcointalk.org/index.php?topic=464184.0 e https://cryptocointalk.com/topic/5081-magic-internet-money-mim-information/;
- MagiCoin (XMG): https://bitcointalk.org/index.php?topic=735170.0 e https://cryptocointalk.com/topic/38116-magi-xmg-coin-of-the-future-social-media-give-away/;
- MaiaCoin (MAIA): https://bitcointalk.org/index.php?topic=667250.0 e https://cryptocointalk.com/topic/12875-maiacoin-maia-information/;
- MaidSafeCoin: https://bitcointalk.org/index.php?topic=577149.0, https://bitcointalk.org/index.php?topic=579797.0 e http://maidsafe.net/;

- MakiCoin (MAKI): https://bitcointalk.org/index.php?topic=511252.0 e https://cryptocointalk.com/topic/8314-makicoin-maki-information/;
- MaleCoin (MLC): https://bitcointalk.org/index.php?topic=418619.0 e https://cryptocointalk.com/topic/3296-malecoin-mlc-information/;
- Malegebe (MLGB): https://bitcointalk.org/index.php?topic=611614;
- MammothCoin (MAMM): https://bitcointalk.org/index.php?topic=635751.0 e https://cryptocointalk.com/topic/12155-mammothcoin-mamm-information/;
- Mana (MANA): https://bitcointalk.org/index.php?topic=760289.0 e https://cryptocointalk.com/topic/14702-mana-mana-information/;
- MangoCoinz: https://bitcointalk.org/index.php?topic=902788.0;
- MantisCoin (MTS): https://bitcointalk.org/index.php?topic=729345.0 e https://cryptocointalk.com/topic/14058-mantiscoin-mts-information/;
- Maples (MPL): https://bitcointalk.org/index.php?topic=288690.0 e https://cryptocointalk.com/topic/1154-maples-mpl-information/;
- MarineCoin (MTC): https://bitcointalk.org/index.php?topic=879880.0 e https://cryptocointalk.com/topic/3276-marinecoin-mtc-information/;
- MarioBrosCoin (MBC): https://bitcointalk.org/index.php?topic=420849.0 e https://cryptocointalk.com/topic/3332-ann-mariobroscoin-mbc-is-out-now/;
- MarsCoin (MRS): https://bitcointalk.org/index.php?topic=434971.0, https://cryptocointalk.com/topic/3763-marscoin-mrs-information/ e http://marscoin.org/;
- MarteXCoin (MXT): https://bitcointalk.org/index.php?topic=1354130.0 e https://cryptocointalk.com/topic/11234-martexcoin-mxt-information/;
- MaruCoin (MARU): https://bitcointalk.org/index.php?topic=570744.0 e https://cryptocointalk.com/topic/11284-

marucoin-maru-information/;

- MasonCoin (MSC): https://bitcointalk.org/index.php?topic=742979.0;
- MastCoin (MAST): https://bitcointalk.org/index.php?topic=613622.0 e https://cryptocointalk.com/topic/11559-mastcoin-mast-information/;
- MasterCoin (MST): https://bitcointalk.org/index.php?topic=242406.0 e https://cryptocointalk.com/topic/711-mastercoin-mst-information/;
- MatrixCoin (MTX): https://bitcointalk.org/index.php?topic=552713.0 e https://cryptocointalk.com/topic/9459-matrixcoin-mtx-information/;
- MavroCoin: https://bitcointalk.org/index.php?topic=504193.0;
- MaxCoin (MAX): https://bitcointalk.org/index.php?topic=438150.0, https://cryptocointalk.com/topic/4464-maxcoin-max-information/ e http://www.maxcoin.co.uk/;
- MazaCoin (MZC): https://bitcointalk.org/index.php?topic=508849.0 e https://cryptocointalk.com/topic/6252-mazacoin-mzc-information/;
- MediCoin (MDC): https://cryptocointalk.com/topic/21963-medicoin-mdc-information/;
- MedicCoin (MDC): https://bitcointalk.org/index.php?topic=856624.0 e https://bitcointalk.org/index.php?topic=856624.0;
- MediterraneanCoin (MED): https://bitcointalk.org/index.php?topic=397831.0;
- MegaCoin (MEC): https://bitcointalk.org/index.php?topic=218851.0, https://cryptocointalk.com/topic/475-megacoin-m%CF%83c-information/ e http://www.megacoin.co.nz/;
- MemeCoin (MEM): https://bitcointalk.org/index.php?topic=217526.0 e https://cryptocointalk.com/topic/376-memecoin-mem-information/;
- Memorycoin (MMC): https://bitcointalk.org/index.php?topic=267522.0 e https://cryptocointalk.com/topic/2190-memorycoin-mmc-information/;
- MetalCoin (MTC): https://bitcointalk.org/index.php?topic=651653.0 e https://cryptocointalk.com/topic/12374-

metalcoin-mtc-information/;

- MentalHealthAwareness (MND / MindCoin): https://bitcointalk.org/index.php?topic=1305652.0, https://bitcointalk.org/index.php?topic=1308702.0 e https://cryptocointalk.com/topic/11124-mental-health-awareness-coin-mha-information/;
- MetalMusicCoin: https://bitcointalk.org/index.php?topic=808657.0 e https://cryptocointalk.com/topic/17368-pre-ann-metal-music-coin-scrypt/;
- MetisCoin (MTS): https://bitcointalk.org/index.php?topic=424517.0 e https://cryptocointalk.com/topic/3447-metiscoin-mts-information/;
- MHACoin (MHA): https://bitcointalk.org/index.php?topic=590957.0 e https://cryptocointalk.com/topic/11124-mental-health-awareness-coin-mha-information/;
- Microcash (MCR): https://bitcointalk.org/index.php?topic=1381328.0 e https://cryptocointalk.com/topic/2406-microcash-mcr-information/;
- MicroCoin (MRC): https://bitcointalk.org/index.php?topic=397679.0 e https://cryptocointalk.com/topic/2811-microcoin-mrc-information/;
- MiddleEarthCoin (MEA): https://bitcointalk.org/index.php?topic=590844.0 e https://cryptocointalk.com/topic/10831-middleearthcoin-mea-information/;
- MilanCoin (MLC): https://bitcointalk.org/index.php?topic=375732.10 e https://cryptocointalk.com/topic/3356-milancoin-mlc-information/;
- MileyCyrusCoin (MCC): https://bitcointalk.org/index.php?topic=732345.0 e https://cryptocointalk.com/topic/14097-mileycyruscoin-mcc-information/;
- MillionaireCoin (MIL): https://bitcointalk.org/index.php?topic=633914.0 e https://cryptocointalk.com/topic/12181-millionairecoin-mil-information/;
- MinCoin (MNC): https://bitcointalk.org/index.php?topic=165397.0 e https://cryptocointalk.com/topic/5826-mincoin-

mnc-information/;

- Minerals (MIN): https://bitcointalk.org/index.php?topic=641057.0 e https://cryptocointalk.com/topic/12300-minerals-min-information/;
- MinersCoin (MIC): https://bitcointalk.org/index.php?topic=766157 e https://cryptocointalk.com/topic/14839-minerscoin-mic-information/;
- MintCoin (MINT): https://bitcointalk.org/index.php?topic=450381.0 e https://cryptocointalk.com/topic/4563-mintcoin-mint-information/ e http://www.mintcoinofficial.com/;
- MiracleCoin (MCL): https://bitcointalk.org/index.php?topic=822317.0 e https://cryptocointalk.com/topic/18876-miraclecoin-mcl-information/;
- Mjollnircoin (NNR): https://bitcointalk.org/index.php?topic=577437.0 e https://cryptocointalk.com/topic/10912-mjollnircoin-mnr-information/;
- MLKCoin (MLK): https://bitcointalk.org/index.php?topic=596605.0 e https://cryptocointalk.com/topic/10827-mlkcoin-mlk-information/;
- MMNXT: https://bitcointalk.org/index.php?topic=930228.0, https://bitcointalk.org/index.php?topic=1098824.0 e http://www.mmnxt.com/;
- MMXIVcoin (MMXIV): https://cryptocointalk.com/topic/11629-mmxiv-mmxiv-information/;
- MobCoin (MOB): https://bitcointalk.org/index.php?topic=873867.0;
- MobiusCoin (MOBI): https://bitcointalk.org/index.php?topic=774762.0 e https://cryptocointalk.com/ topic/15478-möbiuscoin-mobi-information/;
- MoleculeCoin (MOL): https://bitcointalk.org/index.php?topic=371576.0 e https://cryptocointalk.com/topic/2189-moleculecoin-mol-information/;
- MonaCoin (MONA): https://bitcointalk.org/index.php?topic=392436.0, https://cryptocointalk.com/topic/2664-monacoin-mona-information/ e http://monacoin.org/en/;
- Monero (MRO): https://bitcointalk.org/index.php?topic=583449.0, https://cryptocointalk.com/topic/11933-monero-

mro-information/ e http://www.monero.cc/;

- MonetaryUnit (MUE): https://bitcointalk.org/index.php?topic=778322.0, https://cryptocointalk.com/topic/13770-ann-monetaryunit-mue-fair-launch-cpu-miningfaucetexplorergiveaways-more/ e http://www.monetaryunit.org/;
- MonetaVerde (MCN): https://bitcointalk.org/index.php?topic=653141.0 e https://cryptocointalk.com/topic/12455-moneta-verde-mcn-information/;
- Money ($$$): https://bitcointalk.org/index.php?topic=863954.0 e http://moneyfoundation.github.io/moneypage/index.html;
- MoneyEnom: https://bitcointalk.org/index.php?topic=559096.0;
- Monocle (MON): https://bitcointalk.org/index.php?topic=585817.0 e https://cryptocointalk.com/topic/10881-monocle-mon-information/;
- MoonCoin (MOON): https://bitcointalk.org/index.php?topic=389403.0, https://cryptocointalk.com/topic/2582-mooncoin-moon-information/ e http://www.mooncoin.com/;
- MorCoin: https://bitcointalk.org/index.php?topic=663513.0;
- MothMan (MOM): https://bitcointalk.org/index.php?topic=824389.0;
- MotoCoin (MOTO): https://bitcointalk.org/index.php?topic=591724.0 e https://cryptocointalk.com/topic/10653-motocoin-moto-information-proof-of-play-human-mineable-cryptocurrency/;
- MountCoin (MNT) https://bitcointalk.org/index.php?topic=658072.0 e https://cryptocointalk.com/topic/11779-mountcoin-mnt-information/;
- MovieCoin (MVC): https://bitcointalk.org/index.php?topic=466953.0.0 e https://cryptocointalk.com/topic/6291-moviecoin-mvc-information/;
- MRTCoin (MRT): https://bitcointalk.org/index.php?topic=411692.0;
- MtGoxCoin (GOX): https://bitcointalk.org/index.php?topic=506287.0 e https://cryptocointalk.com/topic/7808-mtgoxcoin-

gox-information/;

- MugatuCoin (MUGA): https://bitcointalk.org/index.php?topic=632419.0 e https://cryptocointalk.com/topic/11953-mugatucoin-muga-information/;
- MultiCoin (MC): https://bitcointalk.org/index.php?topic=703723.0 e https://cryptocointalk.com/topic/13728-multicoin-mc-information/;
- MultiWalletCoin (MWC): https://bitcointalk.org/index.php?topic=725620.0 e https://cryptocointalk.com/topic/14011-multiwalletcoin-mwc-information/;
- Muniti (MUN): https://bitcointalk.org/index.php?topic=545886.0 e https://cryptocointalk.com/topic/9472-muniti-mun-information/;
- Munne (MNE): https://bitcointalk.org/index.php?topic=797828.0 e https://cryptocointalk.com/topic/18674-ann-mne-munne?x13?pos-?pod?new-wallet-released?strong-marketing?ico-open?/;
- MurrayCoin (MRY): https://bitcointalk.org/index.php?topic=424179.0, https://cryptocointalk.com/topic/3431-murraycoin-mry-information/ e https://www.murraycoin.org/;
- Muva (XCH): https://bitcointalk.org/index.php?topic=944847.0;
- MybroCoin (MBC): https://cryptocointalk.com/topic/3335-mybrocoin-mbc-information/;
- MyCoin (MYC): https://bitcointalk.org/index.php?topic=548490.0 e https://cryptocointalk.com/topic/9368-mycoin-myc-information/;
- MyriadCoin (MYR): https://bitcointalk.org/index.php?topic=483515.0 e https://cryptocointalk.com/topic/6126-myriadcoin-myr-information/;
- MysteryCoin (MYST): https://bitcointalk.org/index.php?topic=939935.0 e https://cryptocointalk.com/topic/13767-mysterycoin-myst-information/;
- N5Coin (N5): https://bitcointalk.org/index.php?topic=684024.0 e https://cryptocointalk.com/topic/13203-n5coin-n5-information/;

- Naanayam (NYM): https://bitcointalk.org/index.php?topic=326784.0 e https://cryptocointalk.com/topic/1497-naanayam-nym-information/;
- NakaCoin (NKC): https://bitcointalk.org/index.php?topic=409506.0;
- Nakamotodark (NKT): https://bitcointalk.org/index.php?topic=896354.0;
- NameCoin (NMC): https://bitcointalk.org/?topic=6017.0, https://cryptocointalk.com/topic/118-namecoin-nmc-information/ e http://namecoin.info/;
- NanoLite (NL): https://bitcointalk.org/index.php?topic=626717.0 e https://cryptocointalk.com/topic/11730-nanolite-nl-information/;
- Nanotoken (NAN): https://bitcointalk.org/index.php?topic=378876.msg4061028;topicseen e https://cryptocointalk.com/topic/1247-nanotoken-nan-information/;
- NapalCoin (NA): https://bitcointalk.org/index.php?topic=623314.0;
- Nas: https://bter.com/coininfo/NAS;
- NautilusCoin: http://www.nautiluscoin.com/#store-of-value;
- NavajoCoin (NAV): http://www.navajocoin.org/;
- NBCoin (NBC): https://bitcointalk.org/index.php?topic=284007.0 e https://cryptocointalk.com/topic/1111-nbcoin-nbc-information/;
- NebulaCoin (NEB): https://bitcointalk.org/index.php?topic=660833.0 e https://cryptocointalk.com/topic/12695-nebulacoin-neb-information/;
- NectarCoin: https://bitcointalk.org/index.php?topic=812124.0;
- NEMCoim (XEM): https://bitcointalk.org/index.php?topic=422129.0 e http://nem.io/;
- Neocoin (NEC): https://bitcointalk.org/index.php?topic=262973.0 e https://cryptocointalk.com/topic/903-neocoin-nec-information/;
- NeoCortex (NEOC): https://bitcointalk.org/index.php?topic=713427.0 e https://cryptocointalk.com/topic/13771-

neocortex-neoc-information/;

- NeosCoin (NEOS): https://bitcointalk.org/index.php?topic=744291.0 e https://cryptocointalk.com/topic/14218-neoscoin-neos-information/;
- NetCoin: https://bitcointalk.org/index.php?topic=295616.0, https://cryptocointalk.com/topic/1133-netcoin-net-information/ e http://netcoinfoundation.org/;
- NetworkCoin (NWC): https://bitcointalk.org/index.php?topic=1121052.0 e https://cryptocointalk.com/topic/1609-networkcoin-nwc-information/;
- Neucoin: https://bitcointalk.org/index.php?topic=944933.0, http://www.neucoin.org/en/ e https://www.myneucoin.com/en/;
- Neutrino (NTR): https://bitcointalk.org/index.php?topic=1014398.0 e https://cryptocointalk.com/topic/12354-neutrino-coin/;
- NeverHoodCoin (NHC): https://bitcointalk.org/index.php?topic=702466.0 e https://cryptocointalk.com/topic/13582-neverhoodcoin-nhc-information/;
- New Universal Dollar (NUD): https://bitcointalk.org/index.php?topic=640933.0 e https://cryptocointalk.com/topic/12092-new-universal-dollar-nud-information/;
- New Universal Euro (NUE): https://bitcointalk.org/index.php?topic=700856.0 e https://cryptocointalk.com/topic/13528-new-universal-euro-nue-information/;
- NeWOcoin (NEWO): https://bitcointalk.org/index.php?topic=650295.0 e https://cryptocointalk.com/topic/12318-newocoin-newo-information/;
- NewWorldOrderCoin (NWO): https://bitcointalk.org/index.php?topic=764660.0 e https://cryptocointalk.com/topic/14813-newworldordercoin-nwo-information/;
- NewYorkCoin (NYC): https://bitcointalk.org/index.php?topic=499842.0 e https://cryptocointalk.com/topic/7503-

newyorkcoin-nyc-update/;

- NextColoredCoin: https://bitcointalk.org/index.php?topic=600204.0;
- Nexus: https://bitcointalk.org/index.php?topic=657601.0;
- NfdCoin (NFD): https://bitcointalk.org/index.php?topic=603932.0 e https://nxtforum.org/assets-board/(ann)-nfdcoin-gateway-nfdgate/?PHPSESSID=jcv857gef9vcg8pu9h8rdk9vv0;
- NibbleCoin (NBL): https://bitcointalk.org/index.php?topic=209035.0;
- NigeriaCoin (NGC): https://bitcointalk.org/index.php?topic=520100.0 e https://cryptocointalk.com/topic/9071-nigeriacoin-ngc-information/;
- Nightmare (NM): https://bitcointalk.org/index.php?topic=740936.0 e https://cryptocointalk.com/topic/14261-nightmare-nm-information/;
- Nimbus (NMB): https://bitcointalk.org/index.php?topic=622323 e https://cryptocointalk.com/topic/14257-nimbus-nmb-information/;
- NineElevenTruthCoin (NTC): https://bitcointalk.org/index.php?topic=947299.0 e https://www.cryptopia.co.nz/Forum/Thread/168;
- NinjaCoin (NJA): https://bitcointalk.org/index.php?topic=648093.0 e https://cryptocointalk.com/topic/12278-ninjacoin-nja-information/;
- NoahCoin (NOAH): https://bitcointalk.org/index.php?topic=676280.0 e https://cryptocointalk.com/topic/13265-noahcoin-noah-information/;
- NobleCoin (NOBL): https://bitcointalk.org/index.php?topic=402667.0 e https://cryptocointalk.com/topic/2932-noblecoin-nobl-information/;
- NodeCoin: https://bitcointalk.org/index.php?topic=590421.0 e https://bitcointalk.org/index.php?topic=595391.0;
- NoFiatCoin: https://bitcointalk.org/index.php?topic=407787.0;
- Noirbits (NRB): https://bitcointalk.org/index.php?topic=226903.0 e https://cryptocointalk.com/topic/998-noirbits-nrb-information-takeover/;

- NoirShares (NRS): https://bitcointalk.org/index.php?topic=565623.0;
- NooCoin (NOO): https://bitcointalk.org/index.php?topic=895226.0 e https://cryptocointalk.com/topic/24991-annnoonoocoin-nootropic-payment-gateway-25-discounts-cfc-live/;
- NoodlyAppendageCoin (NDL): https://bitcointalk.org/index.php?topic=396227.0 e https://cryptocointalk.com/topic/2752-noodlyappendagecoin-ndl-information/;
- NopeCoin (NOPE): https://bitcointalk.org/index.php?topic=827192.0 e https://cryptocointalk.com/topic/19345-nopecoin-nope-information/;
- NovaCoin (NVC): https://bitcointalk.org/index.php?topic=143221.0, https://cryptocointalk.com/topic/123-novacoin-nvc-information/ e http://novacoin.org/;
- NuBits (NBT): https://bitcointalk.org/index.php?topic=791518.0 e https://www.nubits.com/;
- NuCoin (NUC): https://bitcointalk.org/index.php?topic=241128.0 e https://cryptocointalk.com/topic/705-nucoin-nuc-information/;
- NuggetCoin (NGT): https://bitcointalk.org/index.php?topic=619049.0 e https://cryptocointalk.com/topic/11508-nuggetcoin-ngt-information/;
- NumberCoin (NUMC): https://bitcointalk.org/index.php?topic=631948.0 e https://cryptocointalk.com/topic/11901-numbercoin-numc-information/;
- NuShares (NSR): https://nubits.com/nushares/introduction;
- NutCoin (NUT) https://bitcointalk.org/index.php?topic=397938.0 e https://cryptocointalk.com/topic/2718-nutcoin-nut-information/;
- Nxt (NXT): https://bitcointalk.org/index.php?topic=303898.0, https://cryptocointalk.com/topic/1752-nxt-nxt-information/ e http://nxt.org/;
- NyanCoin (NYAN): https://bitcointalk.org/index.php?topic=402085.0 e https://cryptocointalk.com/topic/2844-nyancoin-nyan-information/;

- O2oCoin (O2O): https://bitcointalk.org/index.php?topic=523196.0 e https://cryptocointalk.com/topic/8520-o2ocoin-o2o-information/;
- OceanCoin (OCC): https://bitcointalk.org/index.php?topic=570463.0;
- Ocoin (OSC): https://bitcointalk.org/index.php?topic=312597.0 e https://cryptocointalk.com/topic/1180-ocoin-osc-information/;
- OCOW: https://bitcointalk.org/index.php?topic=1451789.0;
- OctoCoin (888): https://bitcointalk.org/index.php?topic=504265.20 e https://cryptocointalk.com/topic/45131-just-released-888-octocoin-core-104-with-bip65/;
- OcultCoin (OCC): https://bitcointalk.org/index.php?topic=825517.0 e https://cryptocointalk.com/topic/19653-ocultcoin-occ-information/;
- OcupyCoin: https://bitcointalk.org/index.php?topic=959155.0;
- Offerings to Cthulu: https://bitcointalk.org/index.php?topic=294383.0 e https://cryptocointalk.com/topic/1196-promises-of-dreamland-offerings-to-cthulhu/;
- OilCoin (OIC): https://bitcointalk.org/index.php?topic=399065.0 e https://cryptocointalk.com/topic/4864-oilcoin-oil-information-oil-on-exchange-btc-ltc/;
- OlympicCoin (OLY): https://bitcointalk.org/index.php?topic=453085.0 e https://cryptocointalk.com/topic/4618-olympiccoin-oly-information/;
- OmniCoin (OMC): https://bitcointalk.org/index.php?topic=962832.0;
- OneCoin (ONC): https://bitcointalk.org/index.php?topic=200177.0, https://cryptocointalk.com/topic/583-onecoin-onc-information/ e http://tenhodividas.com/onecoin-e-uma-fraude;
- OneEvilCoin (OEC): https://bitcointalk.org/index.php?topic=693540.0 e https://cryptocointalk.com/topic/13367-oneevilcoin-oec-information/;
- OneRareCoin: https://bitcointalk.org/index.php?topic=473921.0s;

- OnionCoin (ONI): https://bitcointalk.org/index.php?topic=449964.0 e https://cryptocointalk.com/topic/4797-onioncoin-oni-information/;
- OnlineGamingCoin (OGC): https://bitcointalk.org/index.php?topic=393475.0 e https://cryptocointalk.com/topic/2693-onlinegamingcoin-ogc-information/;
- OnyxCoin (ONYX): https://bitcointalk.org/index.php?topic=717337.0 e https://cryptocointalk.com/topic/13981-onyxcoin-onyx-v2-information-relaunch/;
- OPECCoin (OPC): https://bitcointalk.org/index.php?topic=1440847.0 e https://cryptocointalk.com/topic/12003-opec-coin-opc-information/;
- OpenSourceCoin (OSC): https://bitcointalk.org/index.php?topic=268705.0 e https://cryptocointalk.com/topic/1180-ocoin-osc-information/;
- OptimumCoin (OPTI): https://bitcointalk.org/index.php?topic=856814.0 e https://cryptocointalk.com/topic/21969-optimumcoin-opti-information/;
- OrangeCoin (OC): https://bitcointalk.org/index.php?topic=581894.0 e https://cryptocointalk.com/topic/10667-orangecoin-oc-information/;
- OrbitCoin (ORB): https://bitcointalk.org/index.php?topic=586674.0 e https://cryptocointalk.com/topic/927-orbitcoin-orb-official-release-thread/;
- OrcaCoin (ORCA): https://bitcointalk.org/index.php?topic=475799.0 e https://cryptocointalk.com/topic/5879-orcacoin-orca-information/;
- Orobit (ORO): https://bitcointalk.org/index.php?topic=490556.0 e https://cryptocointalk.com/topic/4343-orobit-oro-information/;
- OttomanCoin (OTC): https://bitcointalk.org/index.php?topic=644426.0 e https://cryptocointalk.com/topic/12669-ottomancoin-otc-information/;
- OverlyAttachedCoin (OAC): https://bitcointalk.org/index.php?topic=552057.40;

- Overtime (OT): https://bitcointalk.org/index.php?topic=736588.0 e https://cryptocointalk.com/topic/14215-overtime-ot-information/;
- OzzieCoin (OZC): https://bitcointalk.org/index.php?topic=578881.0, https://cryptocointalk.com/topic/13078-ozziecoin-ozc-information/ e http://ozziecoin.com/;
- PacCoin (PAC): https://bitcointalk.org/index.php?topic=331394.0 e https://cryptocointalk.com/topic/1533-paccoin-pac-information/;
- Palcoin (PAL): https://bitcointalk.org/index.php?topic=1462217.0;
- PandaCoin (PAND): https://bitcointalk.org/index.php?topic=399127.0, https://cryptocointalk.com/topic/2826-pandacoin-pand-information/ e http://www.digitalpandacoin.org/;
- PanguCoin (PGC): https://cryptocointalk.com/topic/1203-pangu-pgc-information/;
- ParallaxCoin (PLX): https://bitcointalk.org/index.php?topic=583660.0 e https://cryptocointalk.com/topic/11300-parallaxcoin-plx-information/;
- ParallelCoin (DUO): https://bitcointalk.org/index.php?topic=721170.0, https://cryptocointalk.com/topic/13917-parallelcoin-duo-information/ e http://parallelcoin.info/;
- Particle (PRT): https://bitcointalk.org/index.php?topic=392804.0 e https://cryptocointalk.com/topic/2686-particle-prt-information/;
- PawnCoin (PAWN): https://bitcointalk.org/index.php?topic=552819.0 e https://cryptocointalk.com/topic/7809-ann-ipcopawn-pawncoin-escrow-accepted-and-25-first-day-bonus/;
- PayCoin (PYC): https://bitcointalk.org/index.php?topic=268941.0, http://www.paycoin.co/ e https://bitcoinmagazine.com/20050/death-Paycoin-employee-video-reveals-internal-chaos/;
- PayCoin (XPY): https://bitcointalk.org/index.php?topic=857670.0, https://cryptocointalk.com/topic/972-paycoin-pyc-information/, https://cryptocointalk.com/topic/24969-paycoin-xpy-coin-information/, https://bitcointalk4.com/announcements-

(altcoins)/(ann)(gaw-miners)(xpy)-paycoin-(-40-phash-)/ e https://www.paycoin.com/;

- PayCon (CON): https://paycon.pw/;
- PayProCoin (PRO): https://bitcointalk.org/index.php?topic=643028.0 e https://cryptocointalk.com/topic/12369-payprocoin-pro-information/;
- PayzorCoin (PZR): https://bitcointalk.org/index.php?topic=695063.0 e https://cryptocointalk.com/topic/13734-payzorcoin-pzr-information/;
- Paxum: https://bitcointalk.org/index.php?topic=1571995.0, https://bitcointalk.org/index.php?topic=63431.0 e https://www.paxum.com/payment/index.php?view=views/index.xsl;
- Peacecoin (PEC): https://bitcointalk.org/index.php?topic=432889.0 e https://cryptocointalk.com/topic/3947-peacecoin-pec-information/;
- PeerCoin (PPC): https://bitcointalk.org/index.php?topic=793142.0, https://cryptocointalk.com/topic/113-peercoin-ppc-information/ e http://www.peercoin.net/;
- PeerPay (PP): https://bitcointalk.org/index.php?topic=661506.new;
- PenguinCoin: https://bitcointalk.org/index.php?topic=573842.0, https://cryptocointalk.com/topic/4268-penguincoin-peng-information/ e http://penguincoin.wix.com/penguincoin;
- Pennies (CENT): https://bitcointalk.org/index.php?topic=269145.0 e https://cryptocointalk.com/topic/975-pennies-cent-information/;
- PeopleCoin (PPL): https://bitcointalk.org/index.php?topic=295980.0 e https://cryptocointalk.com/topic/1204-peoplecoin-ppl-information/;
- PeoplesCurrency (PPL): https://bitcointalk.org/index.php?topic=684854.0 e https://cryptocointalk.com/topic/13225-peoples-currency-ppl-information/;
- Pesa (PES): https://bitcointalk.org/index.php?topic=701621.0 e https://cryptocointalk.com/topic/13549-pesa-pes-information/;

- PesetaCoin (PTC): https://bitcointalk.org/index.php?topic=403378.0 e https://cryptocointalk.com/topic/2961-pesetacoin-ptc-information/;
- PetroDollar (P$ / XPD): https://bitcointalk.org/index.php?topic=472238.0, https://cryptocointalk.com/topic/5764-petrodollar-xpd-information/, http://bitcoin4all.net/index.php?topic=42382 e http://petrodollar.org/;
- PHcoin (PHC): https://bitcointalk.org/index.php?topic=589992.0 e https://cryptocointalk.com/topic/11706-phcoin-phc-information/;
- PhenixCoin: https://bitcointalk.org/index.php?topic=211165.0;
- PhiCoin (PHI): https://bitcointalk.org/index.php?topic=449104.0 e https://cryptocointalk.com/topic/4470-phicoin-phi-information/;
- Philosopherstone (PQS): https://bitcointalk.org/index.php?topic=263744.0 e https://cryptocointalk.com/topic/909-philosopherstone-phs-information/;
- PhoenixCoin (PXC): https://bitcointalk.org/index.php?topic=330956.120, https://cryptocointalk.com/topic/1268-phoenixcoin-pxc-information/ e http://phoenixcoin.org/;
- Phonecoin (TEL): https://bitcointalk.org/index.php?topic=445691.0 e https://cryptocointalk.com/topic/3672-phonecoin-tel-information-on-exchange-btc-ltc/;
- PhooeyCoin: https://bitcointalk.org/index.php?topic=615326.0;
- Photon (PHO): https://bitcointalk.org/index.php?topic=478136.0 e https://cryptocointalk.com/topic/5903-photon-pho-information/;
- PiCoin (PI): https://bitcointalk.org/index.php?topic=502448.0 e https://cryptocointalk.com/topic/3419-picoin-pi-information/;
- PiggyCoin: https://bitcointalk.org/index.php?topic=633803.0, https://cryptocointalk.com/topic/6613-piggycoin-

pig-information-old/ e https://cryptocointalk.com/topic/12253-piggycoin-piggy-information/;

- PikaCoin (PIKA): https://bitcointalk.org/index.php?topic=440337.0 e https://cryptocointalk.com/topic/3984-pikacoin-pika-information/;
- PimpCash (PIMP): https://bitcointalk.org/index.php?topic=871506.0 e https://cryptocointalk.com/topic/24638-ann-pimp-pimpcash-fun-fast-and-secure-digital-currency-community-coin-pos-69/;
- PiniumCoin (PNC): https://bitcointalk.org/index.php?topic=413492.0;
- PinkCoin (PC): https://bitcointalk.org/index.php?topic=591666.0 e https://cryptocointalk.com/topic/10747-pinkcoin-pc-information/;
- PioneerCoin (PER): https://bitcointalk.org/index.php?topic=648489.0 e https://cryptocointalk.com/topic/12341-pioneercoin-per-information/;
- PirateCoin (PIR): https://bitcointalk.org/index.php?topic=407723.0 e https://cryptocointalk.com/topic/3054-piratecoin-pir-information/;
- PixCoin (PIX): https://bitcointalk.org/index.php?topic=599443.0 e https://cryptocointalk.com/topic/11646-pixcoin-pix-information/;
- Pixelcoin (PXL): https://bitcointalk.org/index.php?topic=419201.0 e https://cryptocointalk.com/topic/3284-pxlcoin-pxl-information/;
- PizzaCoin (PIC): https://bitcointalk.org/index.php?topic=431508.0 e https://cryptocointalk.com/topic/2857-pizzacoin-pic-information-mandatory-update-new-ver-1001/;
- PlanetDollar (PDR): https://bitcointalk.org/index.php?topic=524080.0 e https://cryptocointalk.com/topic/9061-planetdollar-pdr-information/;
- PlanktonCoin (FOOD): https://bitcointalk.org/index.php?topic=673734.0 e https://cryptocointalk.com/topic/13316-plankton-food-information/;
- PlatinumCoin (PT): https://bitcointalk.org/index.php?topic=1049589.0 e https://cryptocointalk.com/topic/3212-platinum-

pt-information/;

- PLNCoin (PLNC): https://bitcointalk.org/index.php?topic=509433.0 e https://cryptocointalk.com/topic/8268-plncoin-plnc-information/;
- PlayToken (PLT): https://bitcointalk.org/index.php?topic=266521.0 e https://cryptocointalk.com/topic/939-playtoken-plt-information/;
- Plutonium (RODS): https://bitcointalk.org/index.php?topic=680286.0 e https://cryptocointalk.com/topic/13128-plutonium-rods-information/;
- Podcoin (POD): https://bitcointalk.org/index.php?topic=465846.0 e https://cryptocointalk.com/topic/5156-podcoin-pod-information/;
- PokerCoin (POK): https://bitcointalk.org/index.php?topic=278417.0 e https://cryptocointalk.com/topic/1069-pokercoin-pok-information-reboot/;
- PolCoin (PLC2): https://bitcointalk.org/index.php?topic=421964.0, https://cryptocointalk.com/topic/3402-polcoin-plc-information/ e http://www.polcoin.pl/index.php/pl/;
- PolishCoin (PCC): https://bitcointalk.org/index.php?topic=461130.0 e https://cryptocointalk.com/topic/5234-polishcoin-pcc-information/;
- PopulaceCoin (POC): https://bitcointalk.org/index.php?topic=502135.0 e https://cryptocointalk.com/topic/8746-populacecoin-poc-information/;
- PopularCoin (POPCoin): https://bitcointalk.org/index.php?topic=437929.0, https://cryptocointalk.com/topic/3832-popularcoin-pop-information/ e http://popularcoin.com/;
- Porncoin (PNC): https://bitcointalk.org/index.php?topic=219452.0 e https://cryptocointalk.com/topic/393-porncoin-pnc-information/;
- PortCoin: https://bitcointalk.org/index.php?topic=763856.0 e https://cryptocointalk.com/topic/14785-portcoin-port-information/;
- PosCoin (POS): https://bitcointalk.org/index.php?topic=680769.0 e https://cryptocointalk.com/topic/13162-poscoin-

pos-information/;

- PotatoCoin (SPUDS): https://bitcointalk.org/index.php?topic=722255.0 e https://cryptocointalk.com/topic/14699-potatocoin-spuds-information/;
- PotCoin (POT): https://bitcointalk.org/index.php?topic=426324.0 e http://www.potcoin.com/;
- PowCoin (POW): https://bitcointalk.org/index.php?topic=762335.0 e https://cryptocointalk.com/topic/14762-powcoin-pow-information/;
- PowerBTC: https://bitcointalk.org/index.php?topic=660365.0 e http://www.powerbtc.com/;
- PowerCoin (PWR): https://bitcointalk.org/index.php?topic=1475699.0 e https://cryptocointalk.com/topic/3244-powercoin-pow-information/;
- PreisCoin: https://bitcointalk.org/index.php?topic=863886.0 e http://www.preiscoin.com/pt/;
- PremineCoin (PMC): https://bitcointalk.org/index.php?topic=427519.0 e https://cryptocointalk.com/topic/3558-premine-pmc-information/;
- PreminePlus (PMP): https://bitcointalk.org/index.php?topic=673760.0 e https://cryptocointalk.com/topic/13391-premineplus-pmp-information/;
- PrimeCoin (XPM): https://bitcointalk.org/index.php?topic=251850.0, https://cryptocointalk.com/topic/798-primecoin-xpm-information/ e http://primecoin.io/;
- PrimioCoin (PRIMIO): https://cryptocointalk.com/topic/11104-primio-primio-information/;
- ProCoin (PCN): https://bitcointalk.org/index.php?topic=511678.0 e https://cryptocointalk.com/topic/8076-procoin-pcn-information/;
- Prometheus (PMC): https://bitcointalk.org/index.php?topic=718100.0 e https://cryptocointalk.com/topic/12792-prometheus-pmc-information/;
- ProsperCoin (PRC): https://bitcointalk.org/index.php?topic=438433.0 e https://cryptocointalk.com/topic/3899-prospercoin-prc-information/;

- Prototanium (Pr): https://bitcointalk.org/index.php?topic=1352148.0, https://cryptocointalk.com/topic/40178-prototanium-pure-pow-sha256-rare-250k/ e http://proto.uno/;
- Pseudocash / PseudoCoin (PSEUD): https://bitcointalk.org/index.php?topic=676343.0 e https://cryptocointalk.com/topic/13073-pseudocash-pseud-information/;
- PugCoin (PUG): https://cryptocointalk.com/topic/13297-pugcoin-pug-information/;
- PureCoin (PURE): https://bitcointalk.org/index.php?topic=627749.0 e https://cryptocointalk.com/topic/11832-purecoin-pure-information/;
- PWNYCoin (PWNY): https://cryptocointalk.com/topic/5088-pwnycoin-pwny-information/;
- PxlCoin (PXL): https://bitcointalk.org/index.php?topic=418088.0 e https://cryptocointalk.com/topic/3284-pxlcoin-pxl-information/;
- PyramidsCoin (PYRA): https://bitcointalk.org/index.php?topic=795047.0 e https://cryptocointalk.com/topic/12209-pyramidscoin-pyra-information/;
- Qora: https://bitcointalk.org/index.php?topic=522102.0, https://bitcointalk.org/index.php?topic=1015379.0 e http://www.qora.org/;
- Quark (QRK): https://bitcointalk.org/index.php?topic=260031.0, https://cryptocointalk.com/topic/865-quark-qrk-information/ e http://www.quarkcoins.com/;
- Quarkbar (QB): https://bitcointalk.org/index.php?topic=488455.0 e https://cryptocointalk.com/topic/6961-quarkbar-qb-information/;
- Quatloo (QTL): https://bitcointalk.org/index.php?topic=655793.0, https://cryptocointalk.com/topic/12847-quatloo-qtl-information/ e http://quatloos.org/;
- QuazarCoin (QCN): https://bitcointalk.org/index.php?topic=600658.0 e https://cryptocointalk.com/topic/11156-quazarcoin-qcn-information/;

- Qubitcoin (Q2C): https://bitcointalk.org/index.php?topic=411065.0, https://cryptocointalk.com/topic/3143-qubitcoin-q2c-information/ e http://www.qubitcoin.com/;
- Quebecoin (QBC): https://bitcointalk.org/index.php?topic=552561.0 e https://cryptocointalk.com/topic/10493-qu%C3%A9becoin-qbc-information/;
- QuickCoin (QWC): https://cryptocointalk.com/topic/508-quickcoin-qwc-information/'<a;
- QuickQuickCoin (QQC): https://cryptocointalk.com/topic/2574-qqcoin-qqc-information/;
- QuidCoin (QUID): https://bitcointalk.org/index.php?topic=714582.0 e https://cryptocointalk.com/topic/13881-quidcoin-quid-information/;
- QuitDough (QUIT): https://bitcointalk.org/index.php?topic=919267.0;
- Quotient (XQN): https://bitcointalk.org/index.php?topic=854299.0 e https://cryptocointalk.com/topic/21576-quotient-xqn-information/;
- RabbitCoin (RBBT): https://bitcointalk.org/index.php?topic=466621.0 e https://cryptocointalk.com/topic/5786-rabbitcoin-rbbt-information/;
- RaceCoin (RACE): https://bitcointalk.org/index.php?topic=734819.0 e https://cryptocointalk.com/topic/14153-racecoin-race-information/;
- RadioactiveCoin (RAD): https://bitcointalk.org/index.php?topic=405481.0 e https://cryptocointalk.com/topic/2989-radioactivecoin-rad-information/;
- RadioShares (RDSH): https://bitcointalk.org/index.php?topic=404533.0 e https://cryptocointalk.com/topic/3165-radioshares-rdsh-information/;
- RainbowCoin (LGBT): https://bitcointalk.org/index.php?topic=467851.0 e https://cryptocointalk.com/topic/5525-rainbowcoin-lgbt-information/;
- RainbowGoldCoin (RAIN): https://bitcointalk.org/index.php?topic=509203.0 e

https://cryptocointalk.com/topic/8237-rainbowgoldcoin-rain-information/;

- RandomQuark (RQC): https://bitcointalk.org/index.php?topic=500123.0 e https://cryptocointalk.com/topic/7838-randomquark-rqc-information/;
- RapeCoin: https://bitcointalk.org/index.php?topic=395747.0 e https://cryptocointalk.com/topic/9905-ninja-?-?-?-?-join-the-free-rapecoin-revolution-today-rape-?-?-?-?/;
- RapidCoin (RPD): https://bitcointalk.org/index.php?topic=448291 e https://cryptocointalk.com/topic/4728-rapidcoin-rpd-information/;
- RastaCoin (RTC): https://bitcointalk.org/index.php?topic=441606.0;

- RatCoin (RATC): https://bitcointalk.org/index.php?topic=619051.0 e https://cryptocointalk.com/topic/11407-ratcoin-ratc-information/;
- RawCoin (RAW): https://bitcointalk.org/index.php?topic=708461.0 e https://cryptocointalk.com/topic/13735-rawcoin-raw-information/;
- Razor (RZR): https://bitcointalk.org/index.php?topic=644498.0 e https://cryptocointalk.com/topic/12395-razor-rzr-information/;
- RealCoin (REC): https://bitcointalk.org/index.php?topic=227149.0 e https://cryptocointalk.com/topic/516-realcoin-rec-information/;
- RealStackCoin (RSC): https://bitcointalk.org/index.php?topic=491255.0 e https://cryptocointalk.com/topic/6776-realstackcoin-rsc-information/;
- ReckoningCoin (RKN): https://bitcointalk.org/index.php?topic=683943.0;
- RedCoin (RED): https://bitcointalk.org/index.php?topic=246693.0, https://cryptocointalk.com/topic/757-redcoin-red-information/ e http://redcoin.pw/;
- ReddCoin (RDD): https://bitcointalk.org/index.php?topic=423597.0, https://cryptocointalk.com/topic/4252-reddcoin-rdd-information/ e https://www.reddcoin.com/;
- RedOakCoin (ROC): https://bitcointalk.org/index.php?topic=781905.0 e https://cryptocointalk.com/topic/16067-redoakcoin-roc-information/;
- RedWire: https://github.com/CyberCRI/RedWire;
- ReikiCoin (RKC): https://bitcointalk.org/index.php?topic=343615.0 e https://cryptocointalk.com/topic/1603-reikicoin-rkc-information/;
- RepublicCoin (RC): https://bitcointalk.org/index.php?topic=670788.0 e https://cryptocointalk.com/topic/12931-republiccoin-rc-information/;
- RescueCoin (RSCC): https://bitcointalk.org/index.php?topic=679760.0 e https://cryptocointalk.com/topic/13424-rescuecoin-rscc-information/;

- RevolutionCoin (CHE): https://bitcointalk.org/index.php?topic=469910.0 e https://cryptocointalk.com/topic/6721-revolutioncoin-che-information/;
- RhinoCoin (XRC): https://bitcointalk.org/index.php?topic=668572.0 e https://cryptocointalk.com/topic/13083-pre-annrhinocoin-a-decentralized-record-label-xrc/;
- RibbitRewards (RBR): https://bitcointalk.org/index.php?topic=857452.0 e https://www.reddit.com/r/RibbitRewards/;
- RiceCoin (RCC): https://bitcointalk.org/index.php?topic=398709.0;
- RichCoin (RCH): https://bitcointalk.org/index.php?topic=239251.0 e https://cryptocointalk.com/topic/648-richcoin-rch-information/;
- RieCoin (RIC): https://bitcointalk.org/index.php?topic=446703.0, https://cryptocointalk.com/topic/4914-riecoin-ric-information/ e http://riecoin.org/;
- Rightcoin (RTC): https://bitcointalk.org/index.php?topic=607076.0 e https://cryptocointalk.com/topic/11323-rightcoin-rtc-information/;
- Rimbit (RBT): https://cryptocointalk.com/topic/14635-rimbitcoin-buying-out-dying-altcoin/ e http://rimbit.com/;
- Ringo (RIN): https://bitcointalk.org/index.php?topic=622288.0;
- RiotCoin (RIOT): https://bitcointalk.org/index.php?topic=675631.0 e https://cryptocointalk.com/topic/13019-riotcoin-riot-information/;
- RipOffCoin (RIPO): https://bitcointalk.org/index.php?topic=721006.0 e https://cryptocointalk.com/topic/14040-ripoffcoin-ripo-information/;
- Ripple (XRP): https://bitcointalk.org/index.php?topic=1381669.0, https://guiadobitcoin.com.br/10-coisas-que-voce-precisa-saber-sobre-a-ripple-xrp/ e https://ripple.com/;
- RippleLite (XPL): https://bitcointalk.org/index.php?topic=918132.0, https://cryptocointalk.com/topic/28633-xpl-ripplelite/ e https://ripplelite.wordpress.com/;
- RivrCoin (RIVR): https://cryptocointalk.com/topic/13878-rivrcoin-rivr-information/;

- RobotSexNickels (RSN): https://bitcointalk.org/index.php?topic=700491.0 e https://cryptocointalk.com/topic/13519-robotsexnickels-rsn-information/;
- RockCoin (ROCK): https://bitcointalk.org/index.php?topic=690002.0 e https://cryptocointalk.com/topic/13337-rockcoin-rock-information/;
- RomanCoin: (ROM): https://cryptocointalk.com/topic/11764-romancoin-rom-information/'<a;
- RonPaulCoin (RPC): https://bitcointalk.org/index.php?topic=389070.0 e https://cryptocointalk.com/topic/2648-ronpaulcoin-rpc-information/;
- RootCoin (ROOT): https://bitcointalk.org/index.php?topic=714793.0 e https://cryptocointalk.com/topic/14519-rootcoin-root-information/;
- RotoCoin (Rt2): https://bitcointalk.org/index.php?topic=516138.0 e https://cryptocointalk.com/topic/8653-rotocoin-rt2-information/;
- RoxCoin (ROX): https://bitcointalk.org/index.php?topic=668876.0 e https://cryptocointalk.com/topic/12867-roxcoin-rox-information/;
- RoyalCoin (RYC): https://bitcointalk.org/index.php?topic=199839.0 e https://cryptocointalk.com/topic/109-royalcoin-ryc-information/;
- RubberDuckie (RBC): https://bitcointalk.org/index.php?topic=403940.0 e https://cryptocointalk.com/topic/2954-rubberduckie-rbc-information/;
- Ruble (RU): https://bitcointalk.org/index.php?topic=765513.0 e https://cryptocointalk.com/topic/14821-ruble-ru-information/;
- RubyCoin (RBY): https://bitcointalk.org/index.php?topic=459622.0, https://cryptocointalk.com/topic/6260-rubycoin-ruby-information/ e http://www.rubycoin.org/;
- RuCoin: https://bitcointalk.org/index.php?topic=48582.0;
- RupayaCoin (RUP): https://bitcointalk.org/index.php?topic=521251.0 e https://cryptocointalk.com/topic/9478-

rupayacoin-rup-information/;

- RussiaCoin (RC): https://bitcointalk.org/index.php?topic=630009.0 e https://cryptocointalk.com/topic/12208-russiacoin-rc-information/;
- RVDCoin (RVD): https://bitcointalk.org/index.php?topic=357196.0 e https://cryptocointalk.com/topic/1881-rvdcoin-rvd-information/;
- SaffronCoin (SFR): https://bitcointalk.org/index.php?topic=586320.0 e https://cryptocointalk.com/topic/10601-saffroncoin-sfr-information/;
- SailboatCoin (SBC): https://bitcointalk.org/index.php?topic=698655.0 e https://cryptocointalk.com/topic/13498-sailboatcoin-sbc-information/;
- SalonCoin (SALON): https://bitcointalk.org/index.php?topic=597644.0 e https://github.com/Saloncoin/saloncoin;
- SambaCoin (SMB): https://bitcointalk.org/index.php?topic=497195.0 e https://cryptocointalk.com/topic/5982-sambacoin-smb-information/;
- SapientaCoin (SAP): https://bitcointalk.org/index.php?topic=663102.0 e https://cryptocointalk.com/topic/12772-sapientacoin-sap-information/;
- SapphireCoin (SPH): https://bitcointalk.org/index.php?topic=526655.0 e https://cryptocointalk.com/topic/9153-sapphire-sph-information/;
- SativaCoin (STV): https://bitcointalk.org/index.php?topic=791266.0 e https://cryptocointalk.com/topic/16732-sativacoin-stv-information/;
- SaturnCoin (SAT): https://bitcointalk.org/index.php?topic=441760.0 e https://cryptocointalk.com/topic/4127-saturncoin-sat-information/;
- SauronRings (SAU): https://bitcointalk.org/index.php?topic=273198.0 e https://cryptocointalk.com/topic/1014-sauron-rings-sau-information/;
- SaveCoin (SPC): https://bitcointalk.org/index.php?topic=570526.0 e https://cryptocointalk.com/topic/10457-savecoin-spc-information/;

- SaveAndGain(SANDG): https://bitcointalk.org/index.php?topic=1091306.0;
- SavingCoin (SAV): https://bitcointalk.org/index.php?topic=285621.0 e https://cryptocointalk.com/topic/1125-savingcoin-sav-information/;
- sCoin (SCO): https://bitcointalk.org/index.php?topic=400825.0 e https://cryptocointalk.com/topic/2884-scoin-sco-information/;
- ScotCoin (SCOT): https://bitcointalk.org/index.php?topic=1392196.0, https://cryptocointalk.com/topic/9033-scotcoin-scot-information/, http://scotcoinproject.com/ e http://scotcoin.org/;
- Scrolls (SCQ): https://cryptocointalk.com/topic/11983-scrolls-scq-information/;
- SecondsCoin (SEC): https://bitcointalk.org/index.php?topic=381587.0 e https://cryptocointalk.com/topic/2384-secondscoin-sec-information/;
- SecureCoin (SRC): https://bitcointalk.org/index.php?topic=270852.0, https://cryptocointalk.com/topic/1102-securecoin-src-information/ e http://securecoin.org/;
- SeedCoin (SEED): https://bitcointalk.org/index.php?topic=795954.0;
- SeedCoin (SDC): https://cryptocointalk.com/topic/1224-seedcoin-sdc-information/;
- Sembro Token (SMBR): https://bitcointalk.org/index.php?topic=819427.0;
- SerraCoin (SRR): https://bitcointalk.org/index.php?topic=527204.0 e https://cryptocointalk.com/topic/8754-serracoin-srr-information/;
- Servx (XSX): https://bitcointalk.org/index.php?topic=750752.0 e https://cryptocointalk.com/topic/14550-servx-xsx-information/;
- SexCoin (SXC): https://bitcointalk.org/index.php?topic=218158.0 e https://cryptocointalk.com/topic/382-sexcoin-sxc-information/;
- SHAcoin (SHA): https://bitcointalk.org/index.php?topic=512808.0 e https://cryptocointalk.com/topic/8190-shacoin-sha-information/;

- ShadeCoin (SHADE): https://bitcointalk.org/index.php?topic=768941.0 e https://cryptocointalk.com/topic/15290-shadecoin-shade-information/;
- ShadowCash (SDC): https://bitcointalk.org/index.php?topic=745352.0, https://cryptocointalk.com/topic/13533-shadowcoin-sdc-information/ e http://aboutshadow.com/;
- SharkCoin (SAK): https://bitcointalk.org/index.php?topic=617410.0 e http://www.sharkcoin.org/;
- ShareCoin (SHARE): https://bitcointalk.org/index.php?topic=587051.0;
- SherlockCoin (SHC): https://bitcointalk.org/index.php?topic=641410.0 e https://cryptocointalk.com/topic/4691-sherlockcoin-shc-information/;
- ShibeCoin (SHIBE): https://bitcointalk.org/index.php?topic=724624.0 e https://cryptocointalk.com/topic/10826-shibecoin-shibe-information/;
- ShieldCoin (SHLD): https://bitcointalk.org/index.php?topic=681570.0 e https://cryptocointalk.com/topic/13159-shieldcoin-shld-information/;
- ShinyCoin (SHC): https://bitcointalk.org/index.php?topic=655789.0 e https://cryptocointalk.com/topic/12732-shinycoin-shc-information/;
- ShireCoin (SCN): https://bitcointalk.org/index.php?topic=659306.0 e https://cryptocointalk.com/topic/12666-shirecoin-scn-information/;
- ShitCoin (SHT): https://bitcointalk.org/index.php?topic=307419.0 e https://cryptocointalk.com/topic/1366-shitcoin-sht-information/;
- ShiteCoin: http://www.shitecoin.com/;
- ShopCoinX (SHOPX): https://bitcointalk.org/index.php?topic=723395.0;
- SiaCoin (SC): https://bitcointalk.org/index.php?topic=1060294.0, https://cryptocointalk.com/topic/42433-ann-sia-decentralized-storage-working-beta-currency-has-been-released/ e http://www.siacoin.com/;
- SiameseCoin (SIS): https://bitcointalk.org/index.php?topic=620293.0 e https://cryptocointalk.com/topic/12355-

siamesecoin-sis-information/;

- SifCoin (SIC): https://bitcointalk.org/index.php?topic=240894.0 e https://cryptocointalk.com/topic/676-sifcoin-sic-information/;
- SiliconValleyCoin (XSV): https://bitcointalk.org/index.php?topic=520249.0 e https://cryptocointalk.com/topic/8517-siliconvalleycoin-xsv-information/;
- SilkCoin (SILK): https://bitcointalk.org/index.php?topic=599438.0 e https://cryptocointalk.com/topic/11005-silkcoin-silk-information/;
- SineCoin (SINE): https://bitcointalk.org/index.php?topic=640498.0 e https://cryptocointalk.com/topic/13063-sinecoin-sine-information/;
- Singularity (SING): https://bitcointalk.org/index.php?topic=670533.0 e https://cryptocointalk.com/topic/12903-singularity-sing-information/;
- SJWCoin (SJW): https://bitcointalk.org/index.php?topic=1094489.0, https://cryptocointalk.com/topic/39065-ann-sjwcoin-scrypt-5k-60sec-blocks-for-social-justice/ e http://sjwcoin.com/;
- SkeinCoin (SKC): https://bitcointalk.org/index.php?topic=322828.0 e https://cryptocointalk.com/topic/1478-skeincoin-skc-information/;
- SkyCoin (SKY): https://bitcointalk.org/index.php?topic=380441.0 e https://cryptocointalk.com/topic/429-skycoin-syc-information/;
- SkyNet (SNET): https://bitcointalk.org/index.php?topic=761880.0 e https://cryptocointalk.com/topic/14815-skynet-snet-information/;
- SleakCoin (SLK): https://bitcointalk.org/index.php?topic=790781.0 e https://cryptocointalk.com/topic/16724-sleakcoin-slk-information/;
- SlimCoin (SLM): https://bitcointalk.org/index.php?topic=613213.0 e https://cryptocointalk.com/topic/11782-slimcoin-slm-information/;

- SlothCoin (SLOTH): https://bitcointalk.org/index.php?topic=512903.0 e https://cryptocointalk.com/topic/8274-slothcoin-sloth-information/;
- SmartCoin (SMC): https://bitcointalk.org/index.php?topic=400893.0, https://cryptocointalk.com/topic/3721-smartcoin-smc-information/ e http://smartcoin.cc/;
- Smoke: https://bitcointalk.org/index.php?topic=658564.0;
- SnakeXCoin (SNCX): https://bitcointalk.org/index.php?topic=643352.0 e https://cryptocointalk.com/topic/12179-snakexcoin-sncx-information/;
- Snowballs: https://bitcointalk.org/index.php?topic=843495.0;
- SnowCoin (SNC): https://bitcointalk.org/index.php?topic=359948.0 e https://cryptocointalk.com/topic/1999-snowcoin-snc-information/;
- SochiCoin (SOCHI): https://bitcointalk.org/index.php?topic=454536.0 e https://cryptocointalk.com/topic/4651-sochicoin-sochi-information/;
- SocialCoin (SOC): https://bitcointalk.org/index.php?topic=412331.0 e https://cryptocointalk.com/topic/3176-socialcoin-soc-information/;
- SocialXBot (XBOT): https://bitcointalk.org/index.php?topic=760803.0 e https://cryptocointalk.com/topic/15389-socialxbot-xbot-information/;
- SolarCoin (SLR): https://bitcointalk.org/index.php?topic=785257.0, https://cryptocointalk.com/topic/3079-solarcoin-slr-information/ e http://solarcoin.org/en/front-page/;
- SolCoin (SOL): https://bitcointalk.org/index.php?topic=402170.0 e https://cryptocointalk.com/topic/3005-solcoin-sol-information/;
- SoleCoin (SOLE): https://bitcointalk.org/index.php?topic=730077.0 e https://cryptocointalk.com/topic/14093-solecoin-sole-information/;
- SongCoin (SONG): https://bitcointalk.org/index.php?topic=804527.0, https://cryptocointalk.com/topic/17888-songcoin-song-information/ e http://www.songcoin.org/;

- SonicScrewdriver (SSD): https://bitcointalk.org/index.php?topic=730844.0 e https://cryptocointalk.com/topic/14089-sonic-ssd-information/;
- SoonCoin (SOON): https://cryptocointalk.com/topic/27073-sooncoin-soon-sha256-pow-4minblocks-21-mil-total/ e http://www.sooncoin.com/;
- SoundBit (SND): https://bitcointalk.org/index.php?topic=673487.0 e https://cryptocointalk.com/topic/13370-soundbit-snd-information/;
- SoundCoin (SND): https://bitcointalk.org/index.php?topic=598874.0 e https://cryptocointalk.com/topic/11025-soundcoin-snd-information/;
- SouthwestCoin: http://southwestcoinokc.com/;
- SovereignCoin (SVC): https://bitcointalk.org/index.php?topic=489850.0, https://cryptocointalk.com/topic/6868-sovereigncoin-svc-information/ e http://coinwik.org/SovereignCoin;
- SpaceBucks (SBX): https://bitcointalk.org/index.php?topic=650146.0 e https://cryptocointalk.com/topic/12313-spacebucks-sbx-information/;
- SpainCoin (SPA): https://bitcointalk.org/index.php?topic=500511.0 e https://cryptocointalk.com/topic/7993-spaincoin-spa-information/;
- SparkCoin (SPARK): https://bitcointalk.org/index.php?topic=705629.0 e https://cryptocointalk.com/topic/19390-sparkcoin-spark-information/;
- Spartacus (SPATA): https://bitcointalk.org/index.php?topic=691134.0 e https://cryptocointalk.com/topic/13368-spartacus-spata-information/;
- SpartanCoin (SPN): https://bitcointalk.org/index.php?topic=491637.0, https://cryptocointalk.com/topic/8631-spartancoin-spn-information/ e http://www.spartancoin.org/;
- SpecialCoin (SPE): https://bitcointalk.org/index.php?topic=632404.0 e https://cryptocointalk.com/topic/11919-specialcoin-spe-information/;
- SpectrumCoin (SPEC): https://bitcointalk.org/index.php?topic=669165.0 e https://cryptocointalk.com/topic/12872-

spectrumcoin-spec-information/;

- SpeedCoin (SPD): https://cryptocointalk.com/topic/10519-speedcoin-spd-information/ e https://speedcoin.org/;
- SportCoin (SPCC): https://bitcointalk.org/index.php?topic=659470.0 e https://cryptocointalk.com/topic/12851-sportcoin-spcc-information/;
- Spots (SPT): https://bitcointalk.org/index.php?topic=579141.0, http://coinwik.org/Spots e https://bitcointalk.org/index.php?topic=615513.0;
- SpreadCoin (SPR): https://bitcointalk.org/index.php?topic=715435.0 e https://cryptocointalk.com/topic/13842-spreadcoin-spr-information/;
- Sprouts: https://bitcointalk.org/index.php?topic=1103868.0 e http://sproutcoin.github.io/;
- SquallCoin: https://bitcointalk.org/index.php?topic=763406.0 e http://www.squallcoin.com/;
- SquareCoin (XSC): https://bitcointalk.org/index.php?topic=909998.0;
- StabilityShares (XSI): https://bitcointalk.org/index.php?topic=572508.0 e https://cryptocointalk.com/topic/11136-stabilityshares-xsi-information/;
- StableCoin (SBC): https://bitcointalk.org/index.php?topic=227766.0, https://cryptocointalk.com/topic/526-stablecoin-sbc-information/ e http://coinwik.org/StableCoin;
- StackedCoin (STC): https://bitcointalk.org/index.php?topic=401968.0 e https://cryptocointalk.com/topic/2922-stackedcoin-stc-information/;
- StalwartBucks (SBX): https://bitcointalk.org/index.php?topic=429856.0 e https://cryptocointalk.com/topic/2944-stalwartbucks-sbx-information/;
- StandardCoin (STD): https://bitcointalk.org/index.php?topic=522874.0 e https://cryptocointalk.com/topic/9041-standardcoin-std-information/;
- StarbucksCoin (SUC): https://bitcointalk.org/index.php?topic=625364.0;

- StarCoin (STR): https://bitcointalk.org/index.php?topic=259012.0 e https://cryptocointalk.com/topic/858-starcoin-str-information/;
- StartCoin (START): https://bitcointalk.org/index.php?topic=651307.0, https://cryptocointalk.com/topic/12344-startcoin-start-information/ e https://startcoin.org/;
- StashCoin (STA): https://bitcointalk.org/index.php?topic=493942.0 e https://cryptocointalk.com/topic/7665-stashcoin-sta-information/;
- StealthCoin (XST): https://bitcointalk.org/index.php?topic=681725.0 e https://cryptocointalk.com/topic/13160-stealthcoin-xst-information/;
- Stellar (STR): https://bitcointalk.org/index.php?topic=719019.0 e https://www.stellar.org/;
- SterlingCoin (SLG): https://bitcointalk.org/index.php?topic=721936.0, https://www.cryptopia.co.nz/Forum/Thread/738 e http://sterlingcoin.guru/;
- STLCoin (STL): https://bitcointalk.org/index.php?topic=450858.0 e https://cryptocointalk.com/topic/3939-stlcoin-stl-information/;
- StockCoin (STC): https://bitcointalk.org/index.php?topic=431450.0 e https://cryptocointalk.com/topic/3014-stockcoin-stc-information/;
- StoopidCoin (STP): https://bitcointalk.org/index.php?topic=557795.0 e https://cryptocointalk.com/topic/10432-stoopidcoin-stp-information/;
- Stories (STY): https://cryptocointalk.com/topic/4815-stories-sty-information/;
- StorjCoinX (SJCX): https://bitcointalk.org/index.php?topic=702602.0 e http://storj.io/;
- StormCoin (STC): https://bitcointalk.org/index.php?topic=491743.0 e https://cryptocointalk.com/topic/6853-stormcoin-stc-information/;
- SuarezCoin (SRZ): https://bitcointalk.org/index.php?topic=672109.0 e https://cryptocointalk.com/topic/12999-suarezcoin-srz-information/;

- SummerCoin (SUM): https://bitcointalk.org/index.php?topic=581065.0 e https://cryptocointalk.com/topic/10583-summercoin-sum-information/;
- SummerCoinV2 (SUM2): https://bitcointalk.org/index.php?topic=625693.0 e https://cryptocointalk.com/topic/11996-summercoinv2-sum2-information/;
- SunCoin (SUN): https://bitcointalk.org/index.php?topic=452873.0 e https://cryptocointalk.com/topic/4619-suncoin-sun-information/;
- SupCoin (SUP): https://bitcointalk.org/index.php?topic=950084.0;
- SuperCoin (SUPER): https://bitcointalk.org/index.php?topic=618552.0 e https://cryptocointalk.com/topic/11628-supercoin-super-information/;
- SuperNET (UNITY): https://bitcointalk.org/index.php?topic=762346.0, https://cryptocointalk.com/topic/40429-ann-opal-supernet-mobile-messaging-opal-drive-colored-coins/ e http://www.supernet.org/index.php;
- SurgeCoin (SRG): https://bitcointalk.org/index.php?topic=529227.0 e https://cryptocointalk.com/topic/10419-surgecoin-srg-information/;
- SurvivorCoin (SVR): https://bitcointalk.org/index.php?topic=658562.0 e https://cryptocointalk.com/topic/12729-survivorcoin-svr-information/;
- SwagCoin (SWAG): https://bitcointalk.org/index.php?topic=382068.0 e https://cryptocointalk.com/topic/3834-swagcoin-swag-information/;
- SwansonCoin (RON): https://bitcointalk.org/index.php?topic=478244.0 e https://cryptocointalk.com/topic/6022-swansoncoin-ron-information/;
- SwapCoin (SWAP): https://bitcointalk.org/index.php?topic=1604241.0;
- Swarm: https://swarm.fund/;
- Swiss Credit (CHC): https://bitcointalk.org/index.php?topic=730166.0 e https://cryptocointalk.com/topic/14056-swiss-credit-chc-information/;

- SwitzerlandCoin (SWC): https://bitcointalk.org/index.php?topic=638747.0 e https://cryptocointalk.com/topic/11998-switzerlandcoin-swc-information/;
- Sync (SYNC): https://bitcointalk.org/index.php?topic=607919.0 e https://cryptocointalk.com/topic/11374-sync-sync-information/;
- Synereo: https://bitcointalk.org/index.php?topic=827782.0 e http://www.synereo.com/;
- SysCoin (SYS): https://bitcointalk.org/index.php?topic=587080.0, https://cryptocointalk.com/topic/14286-syscoin-sys-information/ e http://syscoin.org/;
- TacoCoin (TCO): https://bitcointalk.org/index.php?topic=601960 e https://cryptocointalk.com/topic/12215-tacocoin-tco-information/;
- TagCoin (TAG): https://bitcointalk.org/index.php?topic=317408.0 e https://cryptocointalk.com/topic/1458-tagcoin-tag-information/;
- TakCoin (TAK): https://bitcointalk.org/index.php?topic=452902.0 e https://cryptocointalk.com/topic/4725-takcoin-tak-information/;
- TakeOutCoin (TOC): https://bitcointalk.org/index.php?topic=569419.0;
- TalkCoin (TAC): https://bitcointalk.org/index.php?topic=573998.0 e https://cryptocointalk.com/topic/11343-talkcoin-tac-information/;
- Tanzanite (TNZ): https://cryptocointalk.com/topic/14787-tanzanite-tnz-information/;
- TeaCoin (TEA): https://bitcointalk.org/index.php?topic=434432.0 e https://cryptocointalk.com/topic/3770-teacoin-tea-information/;
- TechCoin (TECH): https://bitcointalk.org/index.php?topic=663990.0 e https://cryptocointalk.com/topic/12753-techcoin-tech-information/;
- TeddyCoin (TDY / TED): https://bitcointalk.org/index.php?topic=678229.0 e https://cryptocointalk.com/topic/13215-teddycoin-tdy-information/;

- TekCcoin (TEK): https://bitcointalk.org/index.php?topic=320404.0, https://cryptocointalk.com/topic/1162-tekcoin-tek-information/ e http://tekcoin.org/;
- TempleCoin (TPC): https://bitcointalk.org/index.php?topic=529440.0;
- Tenebrix https://bitcointalk.org/index.php?topic=45667.0;
- TenfiveCoin (10-5): https://bitcointalk.org/index.php?topic=500971.0 e https://cryptocointalk.com/topic/8148-tenfivecoin-10-5-information/;
- TerraCoin (TRC): https://bitcointalk.org/index.php?topic=1364146.0, https://cryptocointalk.com/topic/119-terracoin-trc-information/ e http://terracoin.sourceforge.net/;
- TeslaCoin (TES): https://bitcointalk.org/index.php?topic=419494.0, https://cryptocointalk.com/topic/3339-teslacoin-tes-information/ e http://teslacoins.com/;
- Tether (USDT): https://tether.to/;
- TexasCoin (TEX): https://bitcointalk.org/index.php?topic=708747.0 e https://cryptocointalk.com/topic/13694-texascoin-tex-information/;
- ThankCoin (THANK): https://cryptocointalk.com/topic/13276-thankcoin-thank-information/;
- THCoin (TH): https://bitcointalk.org/index.php?topic=639831.0 e https://cryptocointalk.com/topic/12075-thcoin-th-information/;
- TheBotCoin (TBN): https://bitcointalk.org/index.php?topic=530303.0 e https://cryptocointalk.com/topic/9395-thebotcoin-tbn-information/;
- TheLastCoin (TLC): https://bitcointalk.org/index.php?topic=758265.0 e https://cryptocointalk.com/topic/14612-thelastcoin-tlc-information/;
- TheorumCoin (THEO): https://bitcointalk.org/index.php?topic=731983.0 e https://cryptocointalk.com/topic/14167-theoremcoin-theo-information/;
- TheSmurfsCoin (SMURFS): https://bitcointalk.org/index.php?topic=603519.0;

- Third Generation Coin (TGC): https://bitcointalk.org/index.php?topic=643300.0, https://cryptocointalk.com/topic/12314-third-generation-coin-tgc-information/ e https://bitcointalk4.com/announcements-(altcoins)/(ann)-lttgcgt-third-generation-coin-proof-of-burn-dcrypt-algo/;
- ThorCoin (THOR): https://bitcointalk.org/index.php?topic=484815.0 e https://cryptocointalk.com/topic/6242-thorcoin-thor-information/;
- Tickets (TIX): https://bitcointalk.org/index.php?topic=297666.0, https://cryptocointalk.com/topic/1210-tickets-tix-information/ e https://github.com/LotteryTickets/LotteryTickets;
- TigerCoin (TGC): https://bitcointalk.org/index.php?topic=289312.0 e https://cryptocointalk.com/topic/1158-tigercoin-tgc-information/;
- TileCoin (XTC): https://bitcointalk.org/index.php?topic=761852.0 e https://www.tilepay.org/;
- TimeCoin (TMC): https://bitcointalk.org/index.php?topic=256479.0 e https://cryptocointalk.com/topic/843-timecoin-tmc-information/;
- Timekoin (TK): https://bitcointalk.org/index.php?topic=88467.0 e https://cryptocointalk.com/topic/1553-timekoin-tk-information/;
- Titanium (TTN): https://bitcointalk.org/index.php?topic=465727.0 e https://cryptocointalk.com/topic/7987-titanium-ttn-information/;
- TitCoin (TIT): https://bitcointalk.org/index.php?topic=423523.0, https://cryptocointalk.com/topic/3407-official-titcoin™-tit-discussion-forum-2016-xbiz-awards-nominee/ e http://www.titcoins.biz/;
- TittieCoin (TTC): https://bitcointalk.org/index.php?topic=437695.0, https://cryptocointalk.com/topic/3835-tittiecoin-naughty-buy-classy/ e http://tittiecoin.com/;
- TJCoin (TJC): https://bitcointalk.org/index.php?topic=610807.0 e https://cryptocointalk.com/topic/11589-tjcoin-tjc-information/;

- TlasCoin (TLS): https://bitcointalk.org/index.php?topic=595357.0 e https://cryptocointalk.com/topic/10772-tlascoin-tls-information/;
- TopCoin (TOP): https://bitcointalk.org/index.php?topic=445007.0, https://cryptocointalk.com/topic/4175-topcoin-top-information/ e http://topcoin.pw/;
- TorCoin (TOR): https://bitcointalk.org/index.php?topic=646691.0 e https://cryptocointalk.com/topic/13084-torcoin-tor-information/;
- TornadoCoin (TORN): https://bitcointalk.org/index.php?topic=654432.0 e https://cryptocointalk.com/topic/12575-tornadocoin-torn-information/;
- TorrentCoin (TC): https://bitcointalk.org/index.php?topic=633546.0 e https://cryptocointalk.com/topic/12147-torrentcoin-tc-information/;
- TrainCoin (XTN): https://bitcointalk.org/index.php?topic=553436.0;
- TransCoin (TRN): https://bitcointalk.org/index.php?topic=617604.0 e https://cryptocointalk.com/topic/11671-transcoin-trn-information/;
- TransferCoin (TX / TFC): https://bitcointalk.org/index.php?topic=391980, https://bitcointalk.org/index.php?topic=1150229.0 e https://cryptocointalk.com/topic/44671-txtransfer-bittrex-multipool-android-postormn-stealth/;
- TreasureHuntCoin (BOOTY): https://bitcointalk.org/index.php?topic=629372.0 e https://cryptocointalk.com/topic/12293-treasurehuntcoin-booty-information/;
- Trestor: https://bitcointalk.org/index.php?topic=1106047.0;
- Triangles (TRI): https://bitcointalk.org/index.php?topic=697634.0 e https://cryptocointalk.com/topic/13532-triangles-tri-information/;
- Trinity (TTY): https://bitcointalk.org/index.php?topic=695149.0 e https://cryptocointalk.com/topic/13388-trinity-tty-information/;

- TriskeleCoin (TRS): https://bitcointalk.org/index.php?topic=640056.0;
- TRMB: http://www.taiyilabs.com/;
- TrollCoin (TRL): https://bitcointalk.org/index.php?topic=452810.0, https://cryptocointalk.com/topic/43368-ann-trollcoin-trl-?troll-chain-swap-dont-miss-out/ e http://trollcoinbase.com/;
- Troptions (TRP): https://bitcointalk.org/index.php?topic=326652.0 e https://cryptocointalk.com/topic/1508-troptions-trp-information/;
- TruckCoin (TRK): https://bitcointalk.org/index.php?topic=637785.0 e https://cryptocointalk.com/topic/12055-truckcoin-trk-information/;
- TrustCoin (TRS): https://bitcointalk.org/index.php?topic=721590.0 e https://cryptocointalk.com/topic/13910-trustcoin-trs-information/;
- TrustPlus (TRUST): https://bitcointalk.org/index.php?topic=659848.0 e https://cryptocointalk.com/topic/13077-trustplus-trust-information/;
- TuhaoCoin: https://bitcointalk.org/index.php?topic=471074.0;
- TurboCoin (XTB): https://bitcointalk.org/index.php?topic=400257.0 e https://cryptocointalk.com/topic/2976-turbocoin-xtb-information/;
- TweCoin (TWE): https://bitcointalk.org/index.php?topic=553593.0 e https://cryptocointalk.com/topic/9499-twecoin-twe-information/;
- TwilightCoin (TWC): https://bitcointalk.org/index.php?topic=576107.0 e https://cryptocointalk.com/topic/10604-twilightcoin-twc-information/;
- TwipitCoin (TWIP): https://bitcointalk.org/index.php?topic=582783.0 e https://cryptocointalk.com/topic/10157-anntwip-twipit-coin-scrypt-cryptocoin-for-everyone-launched-bounties/;
- UCoin (U): https://bitcointalk.org/index.php?topic=845110.0;
- UFOCoin (UFO): https://bitcointalk.org/index.php?topic=844754.0 e https://cryptocointalk.com/topic/2845-ufocoin-

ufo-information/;

- UltimateCoin (ULT): https://bitcointalk.org/index.php?topic=538337.0 e https://cryptocointalk.com/topic/9396-ultimatecoin-ult-information/;
- UltraCoin (UTC): https://bitcointalk.org/index.php?topic=413978.0 e https://cryptocointalk.com/topic/4125-ultracoin-utc-information/;
- Umbrella-LTC (ULTC): https://bitcointalk.org/index.php?topic=687265.0 e https://cryptocointalk.com/topic/4125-ultracoin-utc-information/;
- Unattainium (UNAT): https://bitcointalk.org/index.php?topic=685126.0 e https://cryptocointalk.com/topic/13268-unattainium-unat-information/;
- UnbreakableCoin (UNB): https://bitcointalk.org/index.php?topic=539945.0 e https://cryptocointalk.com/topic/8551-unbreakable-unb-information/;
- UniCoin: (UNIC) https://bitcointalk.org/index.php?topic=392204.0, https://cryptocointalk.com/topic/2687-unicoin-unic-information/, http://unicoins.org/ e https://www.unocoin.com/;
- UnionCoin (UNC): https://bitcointalk.org/index.php?topic=365399.0 e https://cryptocointalk.com/topic/2087-unioncoin-unc-information/;
- Unitary Status Dollar eCoin (USDe): https://bitcointalk.org/index.php?topic=410254.0, https://cryptocointalk.com/topic/3145-unitary-status-dollar-ecoin-usde/ e http://www.usd-e.com/;
- UniteCoin (UNI): https://bitcointalk.org/index.php?topic=372707.0 e https://cryptocointalk.com/topic/1768-unitecoin-uni-information/;
- UnitedScryptCoin (USC): https://bitcointalk.org/index.php?topic=353688.0 e https://cryptocointalk.com/topic/1843-unitedscryptcoin-usc-information/;
- Unitus (UIS): https://bitcointalk.org/index.php?topic=901069;

- UnityCoin (UNT): https://bitcointalk.org/index.php?topic=489255;
- UniversalCoin (UNV): https://bitcointalk.org/index.php?topic=618089.0;
- UniversalMolecule (UMO): https://bitcointalk.org/index.php?topic=702519.0 e https://cryptocointalk.com/topic/13555-universalmolecule-umo-information-checkpoint-added/;
- UniverseCoin (UNVC): https://bitcointalk.org/index.php?topic=639549.0 e https://cryptocointalk.com/topic/12176-universecoin-unvc-information/;
- UniversityCoin (UVC): https://bitcointalk.org/index.php?topic=590681.0 e https://cryptocointalk.com/topic/10605-universitycoin-uvc-information/;
- Unobtanium: https://bitcointalk.org/index.php?topic=313126.0, https://bitcointalk.org/index.php?topic=527500.0, https://cryptocointalk.com/topic/1418-unobtanium-uno-information/ e http://unobtanium.uno/;
- UpCoin (XUP): https://bitcointalk.org/index.php?topic=1182202.0 e https://cryptocointalk.com/topic/19388-upcoin-up-information/;
- UroCoin (URO): https://bitcointalk.org/index.php?topic=600639.0 e https://cryptocointalk.com/topic/11060-uro-uro-information/;
- UsbCoin (USB): https://bitcointalk.org/index.php?topic=707450.0 e https://cryptocointalk.com/topic/13773-usbcoin-usb-information/;
- USDeCoin (USDE): https://bitcointalk.org/index.php?topic=410254.0 e https://cryptocointalk.com/topic/3145-unitary-status-dollar-ecoin-usde/;
- UseCoin (USE): https://bitcointalk.org/index.php?topic=735355.0 e https://cryptocointalk.com/topic/14382-usecoin-use-information/;
- UtilityCoin (UTIL): https://bitcointalk.org/index.php?topic=797900.0 e https://cryptocointalk.com/topic/17188-utilitycoin-util-information/;

- ValueCoin (VLC): https://bitcointalk.org/index.php?topic=239666.0 e https://cryptocointalk.com/topic/660-valuecoin-vlc-information/;
- VampireCoin (VMP): https://bitcointalk.org/index.php?topic=455690.0 e https://cryptocointalk.com/topic/5228-vampirecoin-vmp-information/;
- VanillaCoin (VNL): https://bitcointalk.org/index.php?topic=977245.0, https://cryptocointalk.com/topic/3142-vanillacoin-vld-information/ e http://www.vanillacoin.net/;
- Vape (VPC): https://bitcointalk.org/index.php?topic=911357.0, https://bitcointalk.org/index.php?topic=901246.0 e https://cryptocointalk.com/topic/25289-ann-vape-x13-powpos-launched-pow-stage-now/;
- VastCoin (VAST): https://bitcointalk.org/index.php?topic=704077.0 e https://cryptocointalk.com/topic/13590-vastcoin-vast-information/;
- VaultCoin (VLT / VAULT): https://bitcointalk.org/index.php?topic=502160.0 e https://cryptocointalk.com/topic/14023-vaultcoin-vault-information/;
- VegasCoin (VGC): https://bitcointalk.org/index.php?topic=466312.0 e https://cryptocointalk.com/topic/5175-vegascoin-vgc-information/;
- VeilCoin (VEIL): https://bitcointalk.org/index.php?topic=660863.0 e https://cryptocointalk.com/topic/12702-veilcoin-veil-information/;
- VelocityCoin (VEL): https://bitcointalk.org/index.php?topic=390767.0 e https://cryptocointalk.com/topic/2630-velocitycoin-vel-information/;
- VendettaCoin (VAC): https://bitcointalk.org/index.php?topic=766087.0 e https://cryptocointalk.com/topic/4067-vendettacoin-vac-information/;
- VeniVidiViciCoin (VVV): https://bitcointalk.org/index.php?topic=662680.0 e https://cryptocointalk.com/topic/12790-venividivici-coin-vvv-information/;

- VeriCoin (VRC): https://bitcointalk.org/index.php?topic=602041.0, https://cryptocointalk.com/topic/11121-vericoin-vrc-information/ e http://www.vericoin.info/;
- VeroCoin: https://nanohub.org/wiki/VeroCoinInternationalbestexperiencedcryptocurrencysofar;
- Version (V): https://bitcointalk.org/index.php?topic=478176.0 e https://cryptocointalk.com/topic/6920-version-v-information/;
- VertCoin (VTC): https://bitcointalk.org/index.php?topic=404364.0, https://cryptocointalk.com/topic/3093-vertcoin-vtc-information/ e https://vertcoin.org/;
- VexCoin (VEX): https://bitcointalk.org/index.php?topic=775546.0 e https://cryptocointalk.com/topic/17105-vexcoin-vex-information/;
- ViaCoin (VIA): https://bitcointalk.org/index.php?topic=699278.0, https://cryptocointalk.com/topic/13521-viacoin-via-information/ e http://viacoin.org/;
- ViolinCoin (VIO): https://bitcointalk.org/index.php?topic=599353.0 e https://cryptocointalk.com/topic/11483-violincoin-vio-information/;
- ViorCoin (VIOR): https://bitcointalk.org/index.php?topic=834910.0 e https://bitcointalk.org/index.php?topic=838899.0;
- VirtaCoin (VTA): https://bitcointalk.org/index.php?topic=734859.0 e https://cryptocointalk.com/topic/13003-virtacoin-vta-information/;
- VirtualMiningCoin (VMC): https://bitcointalk.org/index.php?topic=582873.0 e https://cryptocointalk.com/topic/10748-virtual-mining-coin-vmc-information/;
- VodkaCoin (VDC): https://cryptocointalk.com/topic/3940-vodkacoin-vdc-information-new-checkpoints-version/ e https://bitcointalk.org/index.php?topic=445581.0;
- VolatilityCoin (VLTY): https://bitcointalk.org/index.php?topic=776463.0 e https://cryptocointalk.com/topic/16378-volatilitycoin-vlty-information/;

- VootCoin (VOOT): https://bitcointalk.org/index.php?topic=630628.0 e https://cryptocointalk.com/topic/12015-vootcoin-voot-information/;
- VoxPopuli (VOXP): https://bitcointalk.org/index.php?topic=815379.0;
- VPNCoin (VPN): https://bitcointalk.org/index.php?topic=705446.0 e http://w.bitnet.wang/en_US/;
- vTorrent (VTR): https://bitcointalk.org/index.php?topic=889481.0 e https://cryptocointalk.com/topic/24630-annvtr-vtorrent-share-with-freedom-bittrex-c-cex-empoex/;
- VvXx (VVXX): https://bitcointalk.org/index.php?topic=726117.0 e https://cryptocointalk.com/topic/14006-vvxx-vvxx-information/;
- W2Coin (W2C): https://bitcointalk.org/index.php?topic=635177.0 e https://cryptocointalk.com/topic/12018-w2coin-w2c-information/;
- WacCoin (WACG): https://bitcointalk.org/index.php?topic=659758.0 e https://cryptocointalk.com/topic/13374-waccoin-wacg-information/;
- WampumCoin (WAM): https://bitcointalk.org/index.php?topic=612597.0 e https://cryptocointalk.com/topic/8741-wampumcoin-wam-information/;
- WankCoin (WKC): https://bitcointalk.org/index.php?topic=625934.0 e https://cryptocointalk.com/topic/11700-wankcoin-wkc-information/;
- WaspCoin (WASP): https://bitcointalk.org/index.php?topic=678939.0;
- WatCoin (WAT): https://bitcointalk.org/index.php?topic=625238.0 e https://cryptocointalk.com/topic/12339-watcoin-wat-information/;
- WaterCoin: https://bitcointalk.org/index.php?topic=1533464.0 e https://cryptocointalk.com/topic/9375-cleanwatercoin-water-information/;
- WaveCoin (WVS): https://bitcointalk.org/index.php?topic=653969.0 e https://cryptocointalk.com/topic/12463-wavecoin-wvs-information/;

- WeAreSatoshi (WSX / WAS): https://bitcointalk.org/index.php?topic=506912.0 e https://cryptocointalk.com/topic/7723-wearesatoshi-v2-was-information/;
- WebCoin (WEB): https://bitcointalk.org/index.php?topic=406337.0 e https://cryptocointalk.com/topic/3726-webcoin-web-information/;
- WhirlCoin (WHRL): https://bitcointalk.org/index.php?topic=679134.0 e https://cryptocointalk.com/topic/13568-whirlcoin-whrl-information/;
- WhistleCoin (WSTL): https://bitcointalk.org/index.php?topic=813878.0 e https://cryptocointalk.com/topic/18641-whistlecoin-wstl-information/;
- WhiteCoin (WC): https://bitcointalk.org/index.php?topic=568517.0 e https://cryptocointalk.com/topic/10582-whitecoin-wc-information/;
- WikiCoin (WIKI): https://bitcointalk.org/index.php?topic=444014.0 e https://cryptocointalk.com/topic/4152-wikicoin-wiki-information/;
- WildWestCoin (WEST): https://bitcointalk.org/index.php?topic=607493.0 e https://cryptocointalk.com/topic/11181-wildwestcoin-west-information/;
- WinCoin (WIN): https://bitcointalk.org/index.php?topic=612352.0 e https://cryptocointalk.com/topic/11386-wincoin-win-information/;
- WinterCoin (WINTER): https://bitcointalk.org/index.php?topic=642917.0 e https://cryptocointalk.com/topic/12177-wintercoin-winter-information/;
- Wolf3dCoin (W3D): https://bitcointalk.org/index.php?topic=500921.0;
- WolfCoin (WLF): https://bitcointalk.org/index.php?topic=733588.0 e https://cryptocointalk.com/topic/14135-wolfcoin-wlf-no-longer-in-operation-dead-coin/;
- Wonderful8Coin (W8): https://bitcointalk.org/index.php?topic=705938.0 e https://cryptocointalk.com/topic/13688-wonderful8coin-w8-information/;

- WoodCoin (LOG): https://bitcointalk.org/index.php?topic=831003.0 e http://woodcoin.org/;
- WorldAidCoin (WAC): https://bitcointalk.org/index.php?topic=660090.0;
- WorldCoin (WDC): https://bitcointalk.org/index.php?topic=204894.0, https://cryptocointalk.com/topic/182-worldcoin-wdc-information/ e http://worldcoin.global/;
- WorldCupCoin (WCC): https://bitcointalk.org/index.php?topic=618850.0 e https://cryptocointalk.com/topic/12175-worldcupcoin-wcc-information/;
- WorldFootBallCoin (WFC): https://bitcointalk.org/index.php?topic=616606.0;
- WPCoin (WPC): https://bitcointalk.org/index.php?topic=522407.0 e https://cryptocointalk.com/topic/8789-wpcoin-wpc-information/;
- X11Coin (XC): https://bitcointalk.org/index.php?topic=629985.0 e http://m.20coin.com/coininfo.html?id=XC;
- X13Coin (X13C): https://bitcointalk.org/index.php?topic=635382.0 e https://cryptocointalk.com/topic/11918-x13coin-x13c-information/;
- X14Coin (X14): https://bitcointalk.org/index.php?topic=670119.0 e https://cryptocointalk.com/topic/12897-x14coin-x14-information/;
- X15Coin (X15C): https://bitcointalk.org/index.php?topic=668928.0 e https://cryptocointalk.com/topic/12956-x15coin-x15c-information/;
- XanonCoin (XAN): https://bitcointalk.org/index.php?topic=689866.0 e https://cryptocointalk.com/topic/13312-xanoncoin-xan-information/;
- Xaurum (XAUR): https://bitcointalk.org/index.php?topic=1546279.0;
- XCash (XCASH): https://bitcointalk.org/index.php?topic=765360.0 e https://cryptocointalk.com/topic/15967-xcash-xcash-information/;
- XCloudCoin (CLD): https://bitcointalk.org/index.php?topic=702981.0 e https://cryptocointalk.com/topic/14090-xcloudcoin-cld-information/;

- Xcoin (XCO): https://bitcointalk.org/index.php?topic=969896.0;
- XCurrency (XC): https://bitcointalk.org/index.php?topic=630547.0 e https://cryptocointalk.com/topic/11165-xcurrency-xc-information/;
- XedosCoin (XDC): https://bitcointalk.org/index.php?topic=445651.0 e https://cryptocointalk.com/topic/4209-xedoscoin-xdc-information/;
- XenCoin (XNC): https://bitcointalk.org/index.php?topic=237998.0 e https://cryptocointalk.com/topic/638-xencoin-xnc-information/;
- XICoin (XI): https://bitcointalk.org/index.php?topic=632755.0;
- Xivra (XIV): https://bitcointalk.org/index.php?topic=376160.0 e https://cryptocointalk.com/topic/2297-xivra-xiv-information/;
- XmasCoin (XMAS): https://bitcointalk.org/index.php?topic=390020.0;
- XryptBit (XBIT): https://bitcointalk.org/index.php?topic=722102.0 e https://cryptocointalk.com/topic/14041-xryptbit-xbit-information/;
- XtraCoin (CX): https://bitcointalk.org/index.php?topic=596545.0 e https://cryptocointalk.com/topic/11339-xtracoin-cx-information/;
- Xuro (XURO): https://bitcointalk.org/index.php?topic=745861.0 e https://cryptocointalk.com/topic/14398-xuro-xuro-information/;
- XXLCoin (XXL): https://bitcointalk.org/index.php?topic=442107.0 e https://cryptocointalk.com/topic/4107-xxlcoin-xxl-information/;
- XXXCoin (XXX): https://bitcointalk.org/index.php?topic=980945.0 e https://cryptocointalk.com/topic/12829-xxxcoin-xxx-information/;
- YacCoin (YACC): https://bitcointalk.org/index.php?topic=514739.0 e https://cryptocointalk.com/topic/5008-yaccoin-yacc-information/;

- YaCoin (YAC): https://bitcointalk.org/index.php?topic=206577.0 e https://cryptocointalk.com/topic/110-yacoin-yac-information/;
- YamashitaCoin (YMC): https://bitcointalk.org/index.php?topic=630310.0 e https://cryptocointalk.com/topic/11887-yamashitacoin-ymc-information/;
- YbCoin (YBC): https://bitcointalk.org/index.php?topic=945161.0 e https://cryptocointalk.com/topic/30130-ybcoin-ybc-top-chinese-coin-100-pos-3m-coins-top-market-cap/;
- YellowCoin (YC): https://bitcointalk.org/index.php?topic=578727.0 e https://cryptocointalk.com/topic/10504-yellowcoin-yc-information/;
- YesCoin (YES): https://bitcointalk.org/index.php?topic=600316.0 e https://cryptocointalk.com/topic/11874-yescoin-yes-information/;
- YinCoin: https://bitcointalk.org/index.php?topic=582433.0;
- YinYuanCoin (YYC): https://bitcointalk.org/index.php?topic=582433.0, https://bitcointalk.org/index.php?topic=497132.0 e https://cryptocointalk.com/topic/2566-yinyuancoin-yyc-information/;
- YoloCoin (YOLO): https://bitcointalk.org/index.php?topic=602042 e https://cryptocointalk.com/topic/11028-yolocoin-yolo-information/;
- YuanBaoCoin (YBC): https://bitcointalk.org/index.php?topic=945161.0 e https://cryptocointalk.com/topic/30130-ybcoin-ybc-top-chinese-coin-100-pos-3m-coins-top-market-cap/;
- YupCoin (YUP): https://bitcointalk.org/index.php?topic=653666.0 e https://cryptocointalk.com/topic/12610-yupcoin-yup-information/;
- ZcCoin (ZCC): https://bitcointalk.org/index.php?topic=268575.0 e https://cryptocointalk.com/topic/992-zccoin-zcc-information/;
- Zcoin (XZC): https://bitcointalk.org/index.php?topic=1638450.0;
- ZebraCoin (ZEB): https://bitcointalk.org/index.php?topic=705384.0 e https://cryptocointalk.com/topic/13840-

zebracoin-zeb-information/;

- ZedCoin (ZED): https://bitcointalk.org/index.php?topic=432261.0 e https://cryptocointalk.com/topic/3277-zedcoin-zed-information/;
- ZeitCoin (ZEIT): https://bitcointalk.org/index.php?topic=487814.0, https://cryptocointalk.com/topic/6858-zeitcoin-zeit-information/ e http://www.zeit-coin.net/;
- ZenithCoin (ZTC): https://bitcointalk.org/index.php?topic=227237.0 e https://cryptocointalk.com/topic/461-zenithcoin-ztc-information/;
- ZeroCoin (XZC): https://bitcointalk.org/index.php?topic=1638450.0 e http://zerocoin.org/;
- ZetaCoin (ZET): https://bitcointalk.org/index.php?topic=267545.0 e https://cryptocointalk.com/topic/953-zetacoin-zet-information/;
- ZeusCoin (ZEU): https://bitcointalk.org/index.php?topic=308741.0, https://cryptocointalk.com/topic/1378-zeuscoin-zeu-information/ e http://zeuscoin.webs.com/;
- ZiftrCOIN (ZRC): https://bitcointalk.org/index.php?topic=970363, https://bitcointalk.org/index.php?topic=894605.0, https://www.ziftrcoin.com/ e https://www.reddit.com/r/ziftrCOIN/;
- Zimstake (ZS): https://bitcointalk.org/index.php?topic=583591.0 e https://cryptocointalk.com/topic/10555-zimstake-zs-information/;
- ZipCoin (ZIPC): https://bitcointalk.org/index.php?topic=721306.0 e https://cryptocointalk.com/topic/13908-zipcoin-zipc-information/;
- ZipperCoin (ZIP): https://bitcointalk.org/index.php?topic=634292.0 e https://cryptocointalk.com/topic/12037-zippercoin-zip-information/;
- ZombieCoin (ZMB): https://bitcointalk.org/index.php?topic=455703.0 e https://cryptocointalk.com/topic/5235-zombiecoin-zmb-information/;
- ZoneCoin: https://bitcointalk.org/index.php?topic=1576405.0;
- ZurCoin (ZUR): https://bitcointalk.org/index.php?topic=391806.0 e https://cryptocointalk.com/topic/2647-zurcoin-

zur-information/.

ESPLANAÇÕES SOBRE ALGUMAS ALTCOINS

Litecoin (símbolo: L; abreviatura: LTC), foi criado por Charles Lee, um engenheiro de software, formado pelo MIT - *Massachusetts Institute of Technology* (Instituto de Tecnologia de Massachusetts: http://web.mit.edu/), que já trabalhou para o Google e ajudou a escrever o respectivo código do famoso site de buscas e do Chrome OS. O Litecoin foi lançado através da publicação do código fonte aberto no GitHub (https://github.com/litecoin-project), em 07/10/2011, sob os termos da licença MIT/X11 (https://opensource.org/licenses/MIT): https://github.com/litecoin-project/litecoin/blob/master-0.10/COPYING.

Conhecido como irmão pequeno do Bitcoin, o Litecoin tem as mesmas características do Bitcoin, mas possui tempo de transação mais rápido em razão de menor taxa de bloqueio e mais acessibilidade já que requer especificações menos intensivas; por isso seu nome significa "moeda leve". Cada Litecoin é subdivisível em 100.000.000 unidades menores, definidas por oito casas decimais. Litecoin é a principal competidora da Bitcoin. Alguns dizem que enquanto o Bitcoin é o ouro, a Litecoin é a prata das moedas digitais. Também é tecnicamente superior ao Bitcoin e já tem uma comunidade bem desenvolvida de mineradores, empreendedores aceitando a moeda, usuários e especuladores.

- https://litecoin.org/pt/;
- https://litecoin.com/pt/;
- https://litecoin.info/;
- https://litecoincore.org/;
- https://litecoinassociation.org/;
- http://www.litecoinblockhalf.com/;
- https://bitinfocharts.com/litecoin/;

A produção de Litecoins é conhecida como *Litecoin mining* ou mineração de Litecoin. O Litecoin é uma alteração do projeto original do Bitcoin (confluência do cliente Bitcoin-Qt) e foi desenhado para liberar quatro vezes

mais moedas (84 milhões) do que a criptomoeda que o antecedeu, em um esforço para evitar que a moeda se torne excessivamente escassa e cara com o passar do tempo. Enquanto a rede Litecoin processa um bloco a cada 2,5 minutos, a do Bitcoin faz o mesmo a cada 10 minutos; recordando-se que taxas de blocos menores significam transações mais rápidas. As transações também são processadas com mais facilidade e a mineração é mais inclusiva, permitindo que máquinas regulares possam competir em mais equanimidade com as chamadas perfuradoras digitais. Através do algoritmo de hash (*hashing algorithm*), de *PoW* - *Proof of Work* (prova de obra ou de trabalho), Scrypt (diferentemente do Bitcoin que usa sha-256), o Litecoin busca nivelar os mineradores e diminuir a vantagem daqueles que usam máquinas superpotentes e projetadas especificadamente para competir na mineração das moedas. O Litecoin utiliza o Scrypt com o objetivo de prevenir que a mineração em GPU, FPGA e ASIC tenha uma vantagem significativa sobre a mineração com CPU. Por outras palavras, o Scrypt foi escolhido porque, teoricamente, impede o uso de ASICs (chips especializados para mineração de criptomoedas), embora haja debate (divergência) sobre tal afirmativa. Entretanto, atualmente a mineração em GPU é, pelo menos, 10 vezes mais eficiente do que a mineração em CPU; já no Bitcoin a GPU era cerca de 22 vezes mais rápida do que a CPU. Mesmo assim, a distância entre os garimpeiros de CPU e GPU é bem menor do que no Bitcoin.

- http://litecoinminingcalculator.com/;
- https://www.litecoinpool.org/;
- https://www.wemineltc.com/;
- http://bravenewcoin.com/Litecoin#Trading-Pairs;
- https://www.cryptocompare.com/coins/ltc/overview.

Enquanto que a mineração do Bitcoin não exige nada da memória RAM, a mineração do Litecoin exige muita memória RAM (ou VRAM), o que dificulta o desenvolvimento de hardware ASIC para garimpá-lo. Ainda mais, no Litecoin, apenas com a alteração de uma variável (N) ao invés do algoritmo, é possível fazer com que o garimpo consuma mais, ou menos, memória RAM, inviabilizando ainda mais o desenvolvimento do hardware

ASIC. Para que a rede Bitcoin, hipoteticamente, troque o algoritmo SHA256 por outro que inviabilize os ASICs, seria necessário que mais de 51% da rede aprovasse a mudança; mas isso é praticamente impossível porque os ASICs podem atingir facilmente os 51% da rede.

Em resumo, o Litecoin vale menos do que o Bitcoin, mas é mais fácil de minerar. Se apenas alguns fornecedores aceitar Bitcoin, muito poucos aceitam Litecoin.

A cadeia de blocos do Litecoin pode ser consultada em diversos sites, tais como, por exemplos: http://block-explorer.com/ e https://bchain.info/LTC/. Já através do site http://explorer.litecoin.net/ é possível procurar Litecoin por endereço, número de bloco ou de hash, transação ou hash de chave pública ou nome de cadeia.

O site https://liteaddress.org/ é um gerador de endereço Litecoin em papel.

FTC - Feathercoin (https://github.com/FeatherCoin) é uma criptomoeda derivada direta (bifurcação) da Litecoin. No geral é muito semelhante à Litecoin. Seu algoritmo de hash é o NeoScrypt e seu mecanismo de consenso é a prova de trabalho (*Proof-of-Work*). A Feathercoin ajusta a sua dificuldade de mineração mais frequentemente do que a Litecoin. Possui um recurso avançado de *checkpointing* (ponto de verificação ou de restauração); que é uma medida de segurança contra os ataques de 51% (que objetivam reverter transações). A ORB - Orbitcoin (http://www.orbitcoin.org/) também usa o NeoScrypt.

- http://explorer.feathercoin.com/;
- https://www.feathercoin.com/;
- http://www.feathercoin.it/;
- http://coinwik.org/FeatherCoin;
- https://forum.feathercoin.com/;
- http://feathercoin.com/pools/;

- http://ftc.dnb.io/;
- https://feathercoin.miningpoolhub.com/;
- https://www.coingecko.com/en/coins/feathercoin;
- https://bitinfocharts.com/feathercoin/;
- http://www.coinwarz.com/cryptocurrency/coins/feathercoin;
- http://bravenewcoin.com/Feathercoin#Trading-Pairs.

DGC - Digitalcoin (http://digitalcoin.org/) é outra moeda criptográfica derivada da Litecoin que se destina a manter o seu valor e ser mais estável do que a maioria das criptomoeda (*cryptocurrencies*) através da otimização do desempenho e por reorientar rapidamente para o ambiente de mineração. Além disso, as recompensas por bloco são reduzidas a um ritmo muito mais lento do que outras moedas digitais. Há também um número razoável de fornecedores que aceitam Digitalcoin, que é mais do que pode ser dito sobre outras altcoins. Seu algoritmo de hash é o Scrypt e seu mecanismo de consenso é a prova de trabalho (*Proof-of-Work*).

- https://bitcointalk.org/index.php?topic=1127380.0;
- https://bitcointalk.org/index.php?topic=785601.0;
- https://github.com/DGCDev/digitalcoin;
- http://en.bitcoinwiki.org/Digitalcoin;
- https://forum.digitalcoin.co/forum.php;
- https://coinmarketcap.com/currencies/digitalcoin/;
- https://chainz.cryptoid.info/dgc/;
- http://www.digitalcoin.biz/;
- https://chainz.cryptoid.info/dgc/;
- http://digitalcoinfaucet.com/;
- http://bravenewcoin.com/Digitalcoin#Trading-Pairs.

NMC - Namecoin (https://namecoin.org/) é o primeiro *fork* (bifurcação) do Bitcoin. Igual ao Bitcoin, seu algoritmo de hash é o SHA256 e seu mecanismo de consenso é a prova de trabalho (*Proof-of-Work*). Mas, ao contrário do Bitcoin, o Namecoin pode armazenar dados dentro de seu próprio banco de dados de transações. Namecoin, ainda, é a base para um sistema descentralizado de nome de domínio (DNS), ou seja, URLs da web, o que poderia acabar com a censura na Internet (https://bit.namecoin.info/). Enquanto Namecoin também pode ser usado como moeda, o seu objetivo é gerir o acesso à informação, em vez de dinheiro. Na sua iteração atual, ele utiliza todos os mesmos princípios do Bitcoin para servir como um DNS (*Domain Name System*) distribuído para o domínio de nível superior com a terminação ".bit". Em outras palavras, é uma versão *peer-to-peer* da ICANN - *Internet Corporation for Assigned Names and Numbers* (Corporação da Internet para Atribuição de Nomes e Números). Os nomes de domínio são registrados para uma taxa em Namecoins e registrados e mantidos na cadeia de blocos. Novas transações ocorrem quando os usuários transferem os seus direitos de nome de domínio. Todo o resto funciona como no Bitcoin. Os benefícios deste sistema DNS descentralizado (em oposição ao ICANN), impediria a censura na Internet e, teoricamente, reduziria *downtimes*. O tempo de inatividade ou duração da interrupção refere-se a um período de tempo que um sistema falhar a fornecer ou desempenhar a sua função primária. Mas em razão dos domínios serem baratos e não poderem ser apreendidos, *cybersquatting* (registro de domínios relativos a grandes empresas ou pessoas famosas com objetivo de posterior venda) são cometidos. Além do DNS, um sistema semelhante pode ser empregado para gerenciar logins, *torrent trackers*, (rastreador de torrentes) ou e-mails descentralizados. Enfim, Namecoin é um sistema de transferência de informações e de proteção que usa Namecoins como sua moeda.

- https://namecoin.info/;
- https://bitcointalk.org/?topic=6017.0;
- https://github.com/namecoin;
- https://wiki.namecoin.org/;
- https://forum.namecoin.org/;
- https://explorer.namecoin.info/;

- https://coinmarketcap.com/currencies/namecoin/;
- https://bitinfocharts.com/namecoin/;
- http://bravenewcoin.com/Namecoin#Trading-Pairs.

PPCoin ou PPC – Peercoin (https://peercoin.net/), é outro clone do Bitcoin. O código fonte do Peercoin é distribuído sob a licença MIT/X11. Ao contrário do Bitcoin, Namecoin e Litecoin, o Peercoin não possui um limite rígido sobre o número de possíveis moedas, mas é projetado para eventualmente atingir uma inflação anual na taxa de 1%. Peercoin utiliza um método alternativo de geração de moedas ao lado de mineração. Trata-se da cunhagem (*minting*), método pelo qual novos blocos podem ser gerados por usuários selecionados aleatoriamente. O critério de elegibilidade do usuário para uma recompensa bloco é determinada pela idade de moeda (*coin age*); que é a quantidade de moedas em carteira, multiplicada pelo número de dias de inatividade. O usuário deve ter moedas na carteira por, pelo menos, 30 dias para poder ser elegível.

- https://bitcointalk.org/index.php?topic=793142.0;
- https://github.com/ppcoin/ppcoin;
- https://www.peercointalk.org/;
- https://peercoin.ecoining.com/;
- https://peercoin.mintr.org/;
- https://www.reddit.com/r/peercoin/;
- https://coinmarketcap.com/currencies/peercoin/;
- https://www.coingecko.com/en/price_charts/peercoin/usd;
- https://chainz.cryptoid.info/ppc/;
- https://faucetbox.com/en/list/PPC;
- https://peercoinfaucet.com/;
- http://peercoin.cryptorials.io/;
- https://bitinfocharts.com/ppcoin/;

- https://peercoin.d7.lt/;
- http://bravenewcoin.com/Peercoin#Trading-Pairs.

O Peercoin foi projetado para fornecer segurança máxima transação, mantendo o tempo das transações rápidas e um cliente de baixos recursos. *Forks* de Peercoin, como NeuCoin (http://www.neucoin.org/), continuaram esta tendência, ao abordar certos problemas de segurança que foram deixados em uma área cinzenta na versão original Peercoin. Além do processo de prova de trabalho (*Proof-of-Work*) através do SHA-256, o Peercoin também utiliza a PoS - *Proof of Stake* (prova de jogo ou de participação). Desse modo, apesar de inicialmente empregar o mesmo modelo de mineração como o Bitcoin, o Peercoin calcula o tamanho dos acervos dos usuários para estipular a quantidade de blocos que cada um poderá gerar. Além disso, introduziu o conceito de idade da moeda, que consiste na quantidade de tempo que as moedas permanecem estáticas (paradas) na carteira. Uma das vantagens desse procedimento é inviabilizar o ataque de 51% ao exigir do manipulador um pré investimento muito caro. O plano é, com o tempo, abandonar totalmente à prova de trabalho (*Proof-of-Work*); mas enquanto isso não ocorre, o Peercoin é dominado pelos ASICs.

NVC - Novacoin (https://novaco.in/) se diferencia das demais moedas digitais pelos seus fatores de segurança e porque sua mineração é de modo diverso das outras altcoins. Utiliza uma combinação de *Proof-of-Work* (prova de trabalho) e *Proof-of-Stake* (prova de jogo ou de participação). Utiliza o algoritmo Scrypt.

- https://bitcointalk.org/index.php?topic=143221.0;
- https://github.com/novacoin-project/novacoin;
- https://sourceforge.net/projects/novacoin/files/;
- http://novacoin.criptomonedas.tel/;
- http://coinwiki.info/en/Novacoin;
- http://coinwik.org/NovaCoin;
- https://wiki.novaco.in/;

- https://explorer.novaco.in/;
- http://www.coinwarz.com/cryptocurrency/coins/novacoin;
- https://bitinfocharts.com/novacoin/;
- http://bravenewcoin.com/Novacoin#Trading-Pairs.

A **BTCD - BitcoinDark** (http://bitcoindark.com/) é uma bifurcação da NovaCoin que foca em privacidade e anonimato. O Teleport permite a transferência anônima de fundos através da clonagem e troca de denominações padrão da moeda; já a telepatia (*telepathy*) criptografa a comunicação enviada pela rede e mascara o endereço IP do outro usuário. BitcoinDark incentiva a mineração ASIC (hardware especializado). Utiliza o algoritmo de hash SHA-256 e o mecanismo de consenso *Proof-of-Stake*.

SWIFT - BitSwift (http://bitswift.io/) é outra bifurcação da Novacoin de PoS (*proof-of-stake*) pura e sua cadeia de blocos é executada na plataforma BlockNet (http://blocknet.co/). A Blocknet pode ser considerada uma bifurcação da BitSwift.

BLK - BlackCoin (http://blackcoin.co/), anteriormente denominada BC - BlackCoin, é mais uma bifurcação da Novacoin, que após um período breve de prova de obra (Scrypt), passou para prova de jogo pagando um juro anual de até 1% para as partes interessadas. BlackCoin foi criada com o fim de provar a confiabilidade de um sistema de verificação de prova de participação pura. Os desenvolvedores da BlackCoin costumam manter uma presença ativa no Twitter, Facebook, Reddit e IRC, onde respondem às perguntas de usuários e emitem atualizações frequentes. Também apoiam uma Loteria BlackCoin periódica e outros eventos da comunidade. Os desenvolvedores da BlackCoin também oferecem um cliente chamado BlackHalo (http://blackhalo.info/), que funciona como uma troca de moeda descentralizada, permitindo a conversão entre praticamente quaisquer duas moedas, bem como outros recursos.

Ψ ou XPM - Primecoin (http://primecoin.io/), em vez de resolver um hash de forma arbitrária, os mineiros procuram cadeias de números primos. As sequências de números primos são denominadas cadeias de Cunningham.

A *Electronic Frontier Foundation* (https://www.eff.org/awards/coop) oferece prêmios para quem descobrir determinados números primos (http://www.mersenne.org/). O número de Primecoins liberados por bloco é determinado através de uma fórmula de auto-ajuste: 999 dividido pelo quadrado da dificuldade. Entretanto, quando o interesse em Primecoin aumenta, o preço sobe, atraindo mais mineiros e, assim, o nível de dificuldade será mais elevado, implicando na redução da quantidade de Primecoins criados. Portanto, a oferta de Primecoins cresce a um ritmo mais lento à medida que aumenta a demanda, exatamente o oposto do ideal desejado resultado. O código fonte do Primecoin é protegido para Primecoin Developers e distribuído sob a licença MIT/X11.

- https://bitcointalk.org/index.php?topic=251850.0;
- https://github.com/primecoin/primecoin;
- https://bchain.info/XPM/;
- https://www.reddit.com/r/primecoin/;
- https://coinmarketcap.com/currencies/primecoin/;
- https://www.worldcoinindex.com/coin/primecoin;
- https://faucetbox.com/en/list/XPM;
- http://xpmforall.org/;
- http://wallet.primecointalk.org/;
- http://bravenewcoin.com/Primecoin#Trading-Pairs.

ANC - Anoncoin (https://anoncoin.net/) criada por um grupo de ativistas virtuais denominados "Anonnymous" (anônimos) através de um *fork* (bifurcação) do Bitcoin. A principal característica é suporte para duas redes descentralizadas, a I2P Darknet (Internet invisível) e o *browser* Tor, com o que é impossível determinar o endereço IP do utilizador de uma transação. Utiliza *Proof-of-Work* e Scrypt.

- https://bitcointalk.org/index.php?topic=227287.0;
- https://github.com/Anoncoin/anoncoin;

- http://coinwik.org/AnonCoin;
- https://forum.anoncoin.net/;
- https://www.reddit.com/r/Anoncoin/;
- http://www.coinwarz.com/cryptocurrency/coins/anoncoin;
- http://bravenewcoin.com/Anoncoin#Trading-Pairs.

A **BTA - Bata** (https://bata.io/), uma bifurcação do Litecoin, também foca na privacidade e anonimato através das redes Tor e I2P; utiliza o algoritmo de hash Scrypt e o mecanismo de consenso prova de trabalho (*proof of work*).

WDC - Worldcoin (https://worldcoin.global/). A WorldCoin é desenhada para ser a moeda digital do futuro, entre todas as cryptocurrencies ela é a mais rápida. Sua transação pode ser confirmada em 20 segundos. Utiliza *Proof-of-Work* e Scrypt.

- https://bitcointalk.org/index.php?topic=204894.0;
- https://github.com/WorldcoinGlobal/WorldcoinLegacy;
- https://www.wdcexplorer.com/;
- http://forum.worldcoin.global/;
- http://bravenewcoin.com/WorldCoin#Trading-Pairs.

XRP - Ripple (https://ripple.com/) configurado como uma rede de pagamentos (inclusive para outras moedas) e como um sistema automatizado para negócios cambiais. Ripple permitir transações com moeda fiduciárias (dólares, euros, ienes, etc.), criptomoedas (Bitcoin, Litecoin, etc.) e, ainda, de matérias-primas ou outras unidades de valor, como, por exemplo, milhas de viagem. O banco de dados descentralizado, público e compartilhado, contém informações sobre as ofertas para comprar ou vender moedas e ativos, criando a primeira troca distribuída. Ripple é tecnicamente um protocolo de Internet, como HTTP e TCP/IP. Ripple foi criado por uma empresa chamada Ripple Labs (anteriormente denominada OpenCoin Inc.), que foi duramente criticada pela comunidade digital pelo fato de que, ao invés de permitir a mineração por qualquer pessoa, 55% das moedas foram

vendidas, 20% foram mantidas pelos fundadores e 25% foram mantidas pela Ripple Labs.

- https://bitcointalk.org/index.php?topic=1381669.0;
- https://github.com/ripple;
- https://forum.ripple.com/;
- https://www.reddit.com/r/Ripple/;
- https://charts.ripple.com/#/;
- https://charts.ripple.com/#/graph/;
- https://bithomp.com/explorer/;
- http://bravenewcoin.com/Ripples#Trading-Pairs;
- https://www.cryptocompare.com/coins/xrp/overview.

Ripple é composto de três partes principais: uma rede de pagamentos, um câmbio distribuído e sua própria moeda criptográfica. O processo de consenso ou de validação é distribuído, mas não descentralizado. Em teoria, os usuários podem escolher a sua própria rede de validadores para assegurar a integridade da transação. Mas a empresa alega que a maioria das pessoas usará o UNL - *Unique Node List* (lista de nó exclusivo) padrão, deste modo a lista de validadores será mantida pelo Ripple Labs, que promete manter uma variada seleção de validadores. Em última análise, equivale a um sistema centralizado com poder nas mãos de poucos. As transações são muito rápidas e muito acessíveis, pois os usuários podem usar qualquer moeda. Deste modo, Ripple pode acabar sendo a maneira mais fácil de comprar bitcoins ou qualquer altcoin.

XLM – Stellar Lumens (https://www.stellar.org/) é basicamente um clone do Ripple; inclusive seu principal criador é o mesmo. Tal como o Ripple, enviar moedas de um lado para outro com câmbio automático, de forma rápida, segura e confidencial. Diferentemente da maioria dos outros projetos criptomoeda, Stellar não fornece um cliente de desktop e todas as transações são realizadas por meio de sua carteira web. Além disso, uma nova conta só pode ser criada por um usuário Stellar existente que tem que enviar um mínimo de 20 STR para a nova conta (utiliza a prova de jogo);

uma conta no Facebook é obrigatória para confirmar a recepção de fundos. O protocolo Stellar é suportado por uma entidade sem fins lucrativos, a *Stellar Development Foundation* (Fundação Stellar de Desenvolvimento).

- https://bitcointalk.org/index.php?topic=719019.0;
- https://bitcointalk.org/index.php?topic=1428573.0;
- https://github.com/stellar;
- http://bravenewcoin.com/Stellar#Trading-Pairs.

Nxt – Nextcoin (https://nxt.org/), tal como o não foi construído sobre o código do Bitcoin; ele usa seu próprio código de escrita baseado no Java. Nxt é concebido como um novo sistema de pagamento e não apenas a uma única moeda. O Nextcoin inaugurou a *Proof of Stake*. Isso significa que o direito de gravar o próximo bloco de transações vai para quem tem atualmente a maior participação no sistema; isto é, a maioria das moedas em sua conta, mas só depois de terem sido mantidas estáticas por um determinado período de tempo. Tornou-se uma plataforma com muitos recursos como sistemas de mensagens criptografadas, troca de ativos, armazenamento de bens digitais e mercado livre com muitos recursos. Os principais recursos do Next são: 1) Permuta de arquivos; 2) Sistema monetário; 3) Nuvem de dados; 4) Sistema de votação; e, 5) Controle de conta. Nextcoin permite a criação de criptomoedas personalizadas. Nxt não tem aceitação varejista significativa e a maioria das bolsas de Nxt são transacionadas por indivíduos e mediada através do próprio software.

- https://bitcointalk.org/index.php?topic=587007.0;
- https://bitcointalk.org/index.php?topic=357461.0;
- https://github.com/Blackcomb/nxt;
- https://nxtportal.org/monitor/;
- https://www.mynxt.info/blockexplorer/;
- http://www.peerexplorer.com/;
- http://coinwiki.info/en/Nxt;
- http://wiki.nxtcrypto.org/wiki/Main_Page;

- http://www.nxtinfo.org/;
- https://nxtforum.org/;
- https://www.reddit.com/r/NXT/;
- https://www.cryptocompare.com/coins/nxt/overview.

ZET - Zetacoin (http://www.zetac.org/) é outra altcoin derivada do Bitcoin derivado. Sua taxa de transação é 20 vezes maior do que Bitcoin; a qual é acompanhada por um rápido reajuste de dificuldade. Zetacoin é um criptomoeda inflacionária que utiliza o algoritmo de hash SHA-256 e o mecanismo de consenso *Proof-of-Work* (prova de trabalho). Zetacoin não foi pré-extraído no lançamento e, portanto, é considerado como um criptomoeda "fair-mined" (mineirada justamente).

- https://bitcointalk.org/index.php?topic=267545.0;
- https://github.com/zetacoin/zetacoin;
- https://chainz.cryptoid.info/zet/;
- http://coinwik.org/ZetaCoin;
- http://bravenewcoin.com/Zetacoin#Trading-Pairs.

QRK - Quarkcoin (http://www.quarkcoins.com/) é essencialmente uma versão atualizada do Bitcoin, com maior segurança e confirmação quase imediata da transação. A característica mais distinta do Quark é seu foco na segurança da transação, pois utiliza nove rodadas de hash seguro (três dos quais usam algoritmos de hash aleatórios) de seis algoritmos de hash diferentes para codificar as transações (garantir a segurança e o anonimato em suas operações). Detalhe, a maioria das criptomoedas usam apenas um hash. Semelhante ao Peercoin, o Quark não tem limites rígidos sobre a quantidade de QRKs produzidos, o que levará a uma inflação esperada. O Quark é extraído (minerado ou garimpado) usando o poder de processamento do computador regular (mineração CPU); oferece, assim, um modelo de distribuição mais justa disponível.

- https://bitcointalk.org/index.php?topic=260031.0;

- https://github.com/Neisklar/quarkcoin-cpuminer;
- https://quarktalk.cc/;
- http://quark.criptomonedas.tel/;
- http://coinwik.org/Quark;
- https://www.reddit.com/r/QuarkCoin/;
- https://coinplorer.com/QRK/;
- https://chainz.cryptoid.info/zet/;
- http://www.coinwarz.com/cryptocurrency/coins/zetacoin;
- https://bitinfocharts.com/quarkcoin/;
- http://bravenewcoin.com/Quark#Trading-Pairs.

XCP - Counterparty (https://counterparty.io/) é uma plataforma financeira inovadora peer-to-peer. Ao contrário de Wall Street e de outras instituições financeiras centralizadas, proporciona o acesso, de forma aberta e segura, a instrumentos e mercados financeiros, sem necessidade de um terceiro ou intermediário de confiança. Também proporciona contratos inteligentes, Turing completos (aplicações de auto execução), tokens digitais, transações multi-assinaturas, processo de votação, permuta de Ativos (*Exchange* Descentralizada), etc.

- https://bitcointalk.org/index.php?topic=395761.0;
- https://github.com/CounterpartyXCP;
- https://counterpartytalk.org/;
- https://counterpartychain.io/;
- https://blockscan.com/;
- https://coindaddy.io/learn/what-is-counterparty;
- http://bravenewcoin.com/Counterparty#Trading-Pairs.

BCY - BitCrystals (http://bitcrystals.com/), executado através do Counterparty, são ativos digitais que atuam tanto como combustível e prêmio

no jogo *Spells of Genesis* (http://spellsofgenesis.com/) da EverdreamSoft (http://www.everdreamsoft.com/). Foram emitidas 100 milhões de unidades, das quais 70% foram disponibilizadas para compra. As BitCrystals podem ser negociadas na *Blockchain* ou serem usadas para comprar cartões jogáveis dentro de Moonga (http://www.moonga.com/) e Spells of Genesis. 30% da oferta inicial foram mantidas por EverdreamSoft para fins de promoção e desenvolvimento. No final de cada mês, 50% do lucro dos cartões são destruídos e a EverdreamSoft publica um relatório pormenorizado sobre os seus rendimentos; bem como a quantidade a queimar que será enviada ao endereço de queimadura: 1BURNSogXXXXXXXXXXXXXXXXXXXXW3ny2Y.

Dash (https://www.dash.org/), anteriormente denominada Darkcoin, foi originalmente lançado sob o nome "xcoin" e foi projetada para ser uma forma anônima de criptomoeda. Dessa forma, Dash é a primeira moeda anônima. A mudança de nome de Darkcoin para Dash se traduz na tentativa de ser livre da vinculação com negócios ilícitos e obscuros dos que se aproveitavam do seu anonimato. Em comparação com Litecoin, Dash oferece maiores privacidade e anonimato na transação; ainda seu software é mais resistente à mineração com hardware especializado. Melhor privacidade é conseguida através do Darksend, que combina entradas idênticas de vários usuários em uma única transação com várias saídas que ofusca o fluxo de fundos; desta forma, ao misturar os registos das transações de moedas, as torna indetectáveis. Dash também desenvolveu e implementou um algoritmo de hash chamado X11 que usa uma sequência de 11 rodadas de hash para o seu mecanismo de consenso de prova de obra (PoW). Para ajustar a dificuldade de mineração ao longo do tempo, Dash também desenvolveu e utiliza um algoritmo denominado *Dark Gravity Wave* (gravidade da onda escura).

- https://bitcointalk.org/index.php?topic=421615.0;
- https://github.com/dashpay/dash;
- https://www.dash.org/forum/;
- https://chainz.cryptoid.info/dash/;
- https://bitinfocharts.com/darkcoin/;

- http://www.coinwarz.com/cryptocurrency/coins/dash;
- https://coinmarketcap.com/currencies/dash/;
- http://bravenewcoin.com/dash/#Trading-Pairs;
- https://www.cryptocompare.com/coins/dash/overview.

BCN - Bytecoin (https://bytecoin.org/) é criptomoeda indetectável ante sua transação anônima através da tecnologia Cryptonote. Bytecoin utiliza SHA-256 e o algoritmo CryptoNight. O protocolo de prova de trabalho do CryptoNight (desenvolvido pelo projeto CryptoNote) tem o nome de "Prova de Trabalho igualitário" porque objetiva garantir que usuários com CPUs padrão possuam a mesma relevância quanto os usuários com hardwares especializados. Bytecoin rejeita a tecnologia ASIC de produção em massa. Cryptonote, no seu início, foi marcado por associação a iniciativas fraudulentas e ilegais. Há vários clones do Bytecoin, mas a maior parte está associada às origens pouco claras.

- https://bitcointalk.org/index.php?topic=512747.0;
- https://bitcointalk.org/index.php?topic=612206.0;
- https://github.com/amjuarez/bytecoin;
- http://bytecoin.miner.center/;
- http://bravenewcoin.com/Bytecoin#Trading-Pairs.

BBR - Boolberry (http://boolberry.org/) é uma bifurcação de Bytecoin, tendo como base do projeto a tecnologia CryptoNote (privacidade e anonimato das transações). Utiliza o algoritmo de hash *Keccak* e, como mecanismo de consenso, a *Proof-of-Work*.

XMR - Monero (http://monero.org/ ou https://getmonero.org/), cujo nome origina do Bitmonero (http://bitmonero.org/), é um *fork* (bifurcação) do Bytecoin, que utiliza o CryptoNight (64 bits e somente CPU), algoritmo de consenso PoW e com base no protocolo CryptoNote (https://cryptonote.org/). É o mais bem-sucedido clone do Bytecoin. Apesar de utilizar a *Blockchain*, as transações realizadas com Monero só podem ser vistas por quem pagou e quem recebeu a criptomoeda. O usuário cria um

endereço único para cada negócio, diferentemente da Bitcoin, em que cada pessoa possui um endereço fixo da chamada “carteira”. Com Monero, esse endereço único possui uma senha de proteção dos dados que impede que as informações sejam expostas na rede. Também possui um sistema que mescla as transações de valores semelhantes, criando-se uma nova camada de camuflagem que ajuda a mascarar as origens e os destinos das transações. Monero emprega um protocolo específico que gera vários endereços de uma só vez que só podem ser ligados pelo receptor de pagamento e impossibilita a identificação através da análise da *Blockchain*. Monero usa uma tecnologia especial do CryptoNote chamada “ring signatures” (assinaturas anel), que embaralha as chaves públicas dos usuários, a fim de eliminar a possibilidade de identificar um usuário específico; permitindo, assim, transações não rastreáveis; com o que rapidamente ganhou fama na *deep web*. Inclusive é o método de pagamento aceito no AlphaBay (um mercado on-line operado na *Darknet*).

- https://bitcointalk.org/index.php?topic=583449.0;
- https://github.com/monero-project/monero;
- http://monerostats.com/blockchain/;
- http://www.coinwarz.com/cryptocurrency/coins/monero;
- https://monerohash.com/;
- https://mymonero.com/#/;
- http://moneroblocks.info/;
- http://moneroinfo.org/;
- https://monerobase.com/Main_Page;
- https://forum.getmonero.org/;
- https://www.reddit.com/r/Monero/;
- http://pool.monero.org/;
- http://monero.miner.center/;
- https://monerodice.net/;
- https://moneroaddress.org/;

- https://www.cryptocompare.com/coins/xmr/overview.

FRC - Freicoin (http://www.freicoin.org/ e http://freico.in/) impõe uma taxa de demurrage ou deflação (inspirada na ideia de Silvio Gesell) de cerca de 5% (cinco por cento) anual sobre o montante mantido pelos usuários, o que significa quem acumula a moeda em vez de gastar, terá parte das mesmas destruída. O objetivo da demurrage é estimular a moeda como um meio de troca e não como uma reserva de valor. 80% dos Freicoins gerados devem ser distribuídos pela Fundação Freicoin via doações e apenas 20% são atribuídos aos mineiros. Freicoin utiliza a prova de obra (PoW) e usa o algoritmo de hash SHA-256.

- http://foundation.freicoin.org/#/;
- https://wiki.p2pfoundation.net/Freicoin;
- http://coinwik.org/FreiCoin;
- http://freicoin.freeforums.org/;
- https://bitcointalk.org/index.php?topic=89843.0;
- https://github.com/freicoin/freicoin;
- http://theopeneffect.com/freicoin/;
- http://www.coinchoose.com/coins/freicoin/;
- http://www.coinwarz.com/cryptocurrency/coins/freicoin;
- https://www.coingecko.com/en/coins/freicoin.

AUR - Auroracoin (http://auroracoin.is/) um *fork* (bifurcação) do Litecoin, foi concebida como um criptomoeda nacional da Islândia e distribuída para os cidadãos do país para usar como uma opção de pagamento alternativa que poderia contornar as restrições de câmbio da Islândia introduzidas após a crise financeira de 2008. Desse modo, metade das Auroracoins foram pré-extraídas e distribuídas para 330.000 islandeses residentes no país, através de um processo chamado de "lançamento aéreo". A Fundação Auroracoin (http://aurarad.is/) foi criada para liderar um maior desenvolvimento técnico e promover o uso de Auroracoin na Islândia e lhe foi disponibilizado 1.000.000 AUR pelo desenvolvedor para ajudar a

financiar este trabalho. A Auroracoin inicialmente utilizou PoW e Scrypt. Mas, em março de 2016, foi reconfigurada com base na DigiByte (https://digibyte.co/), substituindo o algoritmo Scrypt original por uma combinação de Grøstl, Qubit, Scrypt, SHA-256 e Skein.

- http://auroracoin.is/;
- https://bitcointalk.org/index.php?topic=1467050.0;
- https://bitcointalk.org/index.php?topic=446062.0;
- https://github.com/aurarad/Auroracoin;
- https://www.reddit.com/r/auroracoin/;
- http://insight.auroracoin.is/.

Doge - Dogecoin (http://dogecoin.com/), uma bifurcação do Luckycoin (https://luckycoin.cc/ e http://luckycoinfoundation.org/), que por sua vez é uma bifurcação do Litecoin), iniciou como uma brincadeira. Utiliza Proof of Work e Scrypt.

- https://bitcointalk.org/index.php?topic=361813.0;
- https://github.com/dogecoin/dogecoin;
- http://dogechain.info/;
- http://foundation.dogecoin.com/;
- https://www.reddit.com/r/dogecoin/;
- https://freedoge.co.in/;
- https://bitinfocharts.com/dogecoin/;
- https://coinmarketcap.com/currencies/dogecoin/.

O Doge nasceu de uma brincadeira de Jackson Palmer, um gerente de produtos da Adobe, que para tirar sarro da abundância de altcoins, tuitou, em novembro de 2013, que estava investido em uma nova moeda fictícia (não existia) chamada Dogecoin. Então, só pela zoeira foi feita uma moeda de verdade, com o rosto de um gentil cachorro shiba inu. Através da Reddit, a moeda-piada decolou. Ela atraía mais pessoas despreocupadas, de bem com

a vida e muito mais interessadas em fazer uma piada do que ficar ricos do dia para a noite; tanto que preferiam doar suas moedas para causas bobocas e sérias, ao invés de coletar imensidões de tesouro digital. E a comunidade Dogecoin conseguiu dinheiro para a equipe de trenó (*bobsleigh*) da Jamaica para as Olímpiadas de Inverno; o sucesso talvez tenha se dado por lembrança do filme "Jamaica abaixo de Zero" ("Cool Runnings" no original). Também doaram 25 mil dólares para uma instituição de caridade britânica que trabalha com cães-guia. A mesma também coletou 30 mil dólares para ajudar pessoas no Quênia a terem acesso à agua potável. Em 2014, usando o pseudônimo de Alex Green (outros nomes foram Ryan Francis e Ryan Gentle), Ryan Francis Kennedy apareceu na comunidade Reddit, no fórum sobre o Dogecoin. Green ganhando popularidade ao distribuir Dogecoins deliberadamente e fazendo doações generosas às campanhas de caridade da comunidade. Então quando Green pediu para que seus colegas shibes (entusiastas do Dogecoin) investissem em sua plataforma Moolah, todos atenderam e rapidamente se tornou a empresa de câmbio Dogecoin dominante. Quando Doernberg e outros chamaram atenção para a credibilidade e motivação de Green, foram banidos do site. O esquema de vendas do Moolah envolvia dividendos Doge projetados ao longo de anos. Após contar com supostas centenas de milhares de dólares de investimentos no Moolah, Green entrou em contato com terceiros (Michael Chu e Ferdous) para que se juntassem a e ele e sua funcionária Chelsea Hopkins na compra do MintPal, um site de câmbio para moedas digitais. Moolah (Green) seria responsável por criar um *backend* mais seguro para o MintPal, mas ele furava prazos, adiava a data de lançamento e, ao final, o site MintPal prosseguiu com problemas piores do que antes. No prazo de uma semana, Green tirou o MintPal do ar, citando uma “falha crítica”. No mesmo dia, ele subitamente anunciou que o Moolah estava entrando em processo de falência, afirmando que a empresa havia gasto seus investimentos e não era rentável. Logo depois, os usuários passaram a ter problemas em sacar suas altcoins tanto do MintPal quanto do Moolah. Então ele desapareceu, cessando qualquer contato com investidores, clientes e sócios. Ferdous estima que entre 2 e 4 milhões de dólares em coins tenham sumido junto com ele. Nos últimos meses, a comunidade Dogecoin tem tentado se reerguer. Muitos abandonaram a moeda de vez, outros agora tem mais cuidado e são menos generosos com suas coins.

NEU - NeuCoin (http://www.neucoin.org/en/), um *fork* (bifurcação) do Peercoin, é uma nova plataforma criada com o objetivo primário de ajudar os criadores de conteúdos através de micropagamentos online. O NeuCoin utiliza SHA2-256 e o algoritmo *Proof-of-Stake* (PoS). As pessoas que optarem por usar NeuCoins em sites de conteúdo receberão algumas moedas gratuitamente, quando criarem as suas carteiras online. As empresas que decidam trabalhar nesta nova moeda e os investidores também receberão moedas.

- https://www.myneucoin.com/en/;
- http://getneucoin.com/;
- http://blog.neucoin.org/;
- http://forum.neucoin.org/;
- https://neucoin.desk.com/;
- http://support.myneucoin.com/;
- http://neucoin.org/en/wiki;
- http://explorer.neucoin.org/;
- https://bitcointalk.org/index.php?topic=944933.0;
- https://github.com/NeuCoin;
- https://www.reddit.com/r/neucoin/;
- https://cyber.fund/system/Neucoin;
- https://coinmarketcap.com/currencies/neucoin/?markets=main;
- https://coinmarketcap.com/currencies/neucoin/.

ETH - Ethereum (https://www.ethereum.org/) é uma rede com sua própria *blockchain* (livro-razão público ou cadeia de blocos) e sua própria moeda, o Ether. Diferente do Bitcoin, o Ethereum é desenhado para interagir com outros computadores. Isto permite todo tipo de contratos automatizados possível. Dados internos de uma companhia, especificações de contratos, entrada de dados externos, hora e data e assim por diante, tudo isso pode ser coordenado e dinheiro (Ethers) pode ser distribuído automaticamente. O

Ethereum, portanto, é uma plataforma descentralizada que executa contratos inteligentes (autoexecutáveis): aplicativos que são executados exatamente como programa de computador sem qualquer possibilidade censura, fraude, interferência de terceiros ou de tempo de inatividade. A moeda por trás da rede Ethereum é chamada de Éter. Os desenvolvedores destinam os Éteres como um sinal (ao invés de moeda corrente) para pagar a computação e manutenção de rede.

- https://www.reddit.com/r/ethereum/;
- https://blog.ethereum.org/;
- https://forum.ethereum.org/;
- https://live.ether.camp/;
- https://etherscan.io/;
- https://etherchain.org/;
- https://github.com/ethereum;
- https://ethereumclassic.github.io/;
- https://ethereumpool.co/;
- https://bitinfocharts.com/ethereum/;
- http://www.coinwarz.com/cryptocurrency/coins/ethereum;
- https://www.cryptocompare.com/coins/eth/overview.

A Fundação Ethereum é uma organização sem fins lucrativos registrada na Suíça, e tem a finalidade de gerir os fundos que foram levantados a partir da venda de éter a fim de melhor servir o Ethereum e o ecossistema de tecnologia descentralizada.

Existem alguns projetos muito avançados que usam a Ethereum, como, por exemplo, o projeto conjunto da IBM e Samsung para a Internet das Coisas.

- http://www1.folha.uol.com.br/mercado/2016/06/1780369-problemas-internos-do-bitcoin-dao-oportunidade-a-nova-moeda-virtual.shtml.

POP - Popularcoin (http://popularcoin.com/), uma bifurcação da Litecoin, começou utilizando Scrypt e a prova de obra (PoW); mas a moeda passará a utilizar uma prova híbrida de obra com de jogo ou de participação. Os usuários são incentivados a executarem o programa PopularCoin que gera moedas livremente, permitindo o participante votar em enquetes da mídia popular do setor de entretenimento.

- https://bitcointalk.org/index.php?topic=444745.0;
- https://github.com/Pop-Currency-Foundation/PopularCoin;
- https://cryptocointalk.com/topic/3832- ☆ popularcoin- ☆ pop-information/;
- http://popularcoin.info/chain/PopCoin.

BTS - BitShares (https://bitshares.org/) é uma plataforma usada para trocar uma mercadoria por outra na plataforma Bitshares. Todas as mercadorias não são apoiadas pela mercadoria que eles representam, mas por uma parte diferente da plataforma do Bitshares. Também pode ser usada para lançar empresas autônomas descentralizada (DACs - *Decentralized Autonomous Companies*) que emitem ações e produzem e distribuem lucros aos acionistas. O primeiro DAC lançada por este processo foi chamado BitSharesX, uma troca de ativos descentralizado com sede em Hong Kong. BitShares foi originalmente lançado sob o nome de PhotoShares (PTS); que mais tarde foi renomeado para BitShares (PTS) e "recarregado" em novembro de 2014 através da fusão de vários produtos em BitShares (BTS).

- https://bitcointalk.org/index.php?topic=1084460.0;
- https://github.com/bitshares;
- http://cryptofresh.com/;
- http://bitsharesblog.com/;
- http://www.bitsharesinfo.com/;
- https://bitsharestalk.org/;
- https://bter.com/coininfo/BTS;
- http://bitsharesmarket.com/;

- https://www.reddit.com/r/BitShares/.

XEM - NEM (https://www.nem.io/) significa Movimento Nova Economia (*New Economy Movement*). Inspirada pelo projeto Nxt, foi escrita a partir do zero em Java. É uma plataforma de "proof-of-x"; ou seja, possui vários métodos de utilização da tecnologia *blockchain* para provar algo de uma forma que é criptograficamente verificável. Possui como objetivo fornecer serviços como pagamentos, mensagens, comércio ativo e contratos inteligentes. As características mais interessantes são: POI - *proof-of-importance* (prova de importância) com o nível de importância determinada pela quantidade de moedas de uma carteira e o número de transações feitas de e para a respectiva carteira; sistema integrado P2P-seguro; conta multi-assinatura; sistema de mensagens criptografadas; e, o sistema de reputação Eigentrust++, que avalia a qualidade da contribuição de cada cliente para manter a rede. NEM também usa um modelo cliente-servidor onde o NIS (*NEM Infrastructure Server*) é executado independente do NCC (*NEM Community Client*); e, o cliente é projetado para ser executado localmente, em um navegador web.

- https://bitcointalk.org/index.php?topic=654845.0;
- https://github.com/NemProject;
- https://www.reddit.com/r/nem/;
- http://chain.nem.ninja/#/blocks/0.

AMP - Synereo (https://www.synereo.com/) inicialmente construída para suportar uma rede social descentralizada e distribuída, chamada "cryptocurrency 2.0", baseada em uma economia da atenção humana. O registro na rede Synereo ocorre através da migração dos dados do usuário a partir de uma conta de outra rede social existente, da qual serão convidados os contatos para a Synereo. Cada utilizador recebe uma pontuação que define a sua posição relativa em termos de interação e da atenção aos conteúdos que produziu; valor este que poderá usar para amplificar a sua voz ou vender no mercado. As pessoas que contribuam para o desenvolvimento, implantação e expansão da rede receberão recompensas pelos seus esforços. Quanto mais cada um fizer pela rede, mais a sua atenção vale. Em cada Synereo (grupos, círculos básicos ou comunidades dentro da rede social),

cada utilizador recebe uma pontuação que define a sua posição relativa em termos de interação e da atenção aos conteúdos que produziu. Ao participar na chamada economia da atenção, o utilizador recebe tokens que poderá usar para amplificar a sua voz. AMP é a moeda de criptografia nativa do Synereo. REO não é uma moeda negociável, mas uma pontuação que se destina a refletir a reputação dos usuários na comunidade. Entretanto, a Synereo converteu-se em uma plataforma de computação e armazenamento descentralizado genérica.

- https://bitcointalk.org/index.php?topic=995987.0;
- https://blog.synereo.com/.

OpenBazaar (https://openbazaar.org/) é definido como o serviço do eBay sem a empresa eBay. Um mercado livre para todos, sem taxas e sem restrições. É um mercado *peer to peer*; é uma comunidade de pessoas que querem realizarem comércio diretamente uns com os outros. Qualquer um pode participar e comprar ou vender bens e serviços. Como o Bitcoin, o OpenBazaar não é propriedade de ninguém, nem é controlado centralmente; é uma rede de pares que operam sem qualquer intermediário. O que torna esta tecnologia especialmente interessante é o uso de tecnologias de resolução de conflito. Com garantia e acordo legal embutidos, estas tecnologias encorajam transações que de outra forma nunca ocorreriam devido a preocupações quanto a fraude ou as dificuldades envolvidas nas múltiplas jurisdições legais. Além de garantia e arbitragem, OpenBazaar usa as transações multi-assinadas (*multisig*) do Bitcoin para prevenir a fraude. Ao usar o OpenBazaar, as três partes envolvidas seriam o comprador, o vendedor e o garantidor. Os fundos serão enviados pelo comprador para um endereço multisig único e armazenados até que o comprador e o vendedor completem a transação com sucesso e assinem a transferência de fundos para o vendedor. Se houver uma disputa e o comprador e o vendedor não puderem concordar sobre para onde enviar os fundos, o garantidor (talvez influenciado pela decisão de um árbitro) tem o voto decisivo. Este sistema de resolução de conflitos juntamente com um sistema de reputação tem o potencial de dar às pessoas confiança suficiente para comercializar sem precisar confiar nos sistemas judiciais existentes. OpenBazaar usa a criptomoeda bitcoin e é baseado em parte no código inicial de um projeto *hacker* denominado DarkMarket. Logo após DarkMarket ter sido revelado

no *hackathon* (evento consistente numa maratona *hacker*), o desenvolvedor Brian Hoffman bifurcou o projeto e rebatizou-o como OpenBazaar.

- https://blog.openbazaar.org/what-is-openbazaar/;
- https://www.reddit.com/r/OpenBazaar/.

SBC - SilentVault (https://silentvault.com/) é uma moeda vale 100% digital apoiada por bitcoins. Isto significa que 1,0 SBC é igual a 1,0 BTC. SilentVault oferece uma solução para a questão da privacidade; permite passar e receber bitcoin (e litecoin) inteiramente fora da *Blockchain* (silenciosamente, fora da cadeia ou sem registro na *Blockchain*) e mover as moedas para e de endereços públicos regulares sempre que quiser. O se tem ou troca no SilentVault são *vauchers* que apenas representam ativos; mas não os ativos em si. *Vouchers* que são certificados ao portador criptograficamente assinados, análogos a moedas.

Open-Transactions (http://opentransactions.org/) e sua versão comercial, **Monetas** (https://monetas.net/), fornecem ferramentas para transações financeiras convencionais, cheques, faturas, etc., em um modo criptografado e distribuído. Entretanto também incluem transações financeiras como dinheiro eletrônico, emissão de moedas, comércio de mercadorias e *smart contracts*. Diferente do Bitcoin e do Ethereum, o Open-transactions é um software baseado em um servidor. Isto tem algumas vantagens - é mais rápido e barato - mas não é tão resiliente quanto o Bitcoin. Os desenvolvedores do open-transactions imaginam um sistema independente de confiança de servidores federados onde uma ampla variedade de servidores disponíveis e eles são praticamente incapazes de comportamento fraudulento. Os desenhos de sistemas muito diferentes do Bitcoin e do Open-Transactions os tornam complementares entre si. O Bitcoin funciona bem, mas não tem atualmente a escalabilidade, ampla variedade de funcionalidades ou velocidade que o Open-transactions pode fornecer. Open-Transactions e Monetas estão integrando um número de funcionalidades ao Bitcoin, tais como funções de segurança para transações em Bitcoin. O Open-transactions pode ser visto como um fornecedor de serviços financeiros ao redor do Bitcoin, como por exemplo, facilitando a troca entre ouro e bitcoin ou realizando transações externas à cadeia de blocos.

HCOIN – Hayek (https://bitcointalk.org/index.php?topic=1076305.0), criada pela empresa Anthem Vault, de Las Vegas nos Estados Unidos, é uma moeda virtual com lastro em ouro. O nome é uma homenagem ao economista austríaco Friedrich Hayek, vencedor do Nobel de Economia em 1974 e um dos papas do liberalismo. Cada HayekCoin vale o equivalente a uma grama de ouro.

MZC - MazaCoin (http://mazacoin.org/), um desdobramento do Zetacoin (http://www.zetac.org/), foi criada pela tribo indígena Oglala, que vive na reserva Pine Ridge, em Dakota do Sul, nos Estados Unidos, com o objetivo de ajudar a tribo a se tornar uma nação mais soberana, reduzindo sua dependência do dólar americano. A palavra Mazacoin é derivada das palavras Lakota Sioux "Maza" e "ska", que significam ferro e branco. MazaCoin usa SHA-256 e prova de obra (PoW).

- https://bitcointalk.org/index.php?topic=508849.0;
- https://github.com/MazaCoin/MazaCoin;
- https://www.reddit.com/r/mazacoin/;
- https://coinmarketcap.com/currencies/mazacoin/;
- https://walletgenerator.net/?currency=Mazacoin;
- http://bravenewcoin.com/mazacoin#Trading-Pairs.

Omni (http://www.omnilayer.org/), anteriormente denominada MSC – Mastercoin, foi criada como um *fork* (bifurcação) do Bitcoin para resolver alguns dos problemas do Bitcoin sobre segurança e estabilidade de preços. O protocolo Mastercoin pretende permitir a reversão de transações dentro de um determinado prazo, ao contrário do Bitcoin, em que todas as transações são irreversíveis. Em março de 2015 a Mastercoin foi rebatizada como Omni e foi declarada como sendo uma plataforma para protocolos descentralizadas como Factom (https://www.factom.com/) e MaidSafe (https://maidsafe.net/). A camada Omni objetiva tirar proveito da *Blockchain* do Bitcoin para construir o apoio para serviços distribuídos adicionais, tais como, por exemplos, uma casa de câmbio descentralizada, os ativos digitais de negociação e contratos inteligentes. Embora Mastercoin

(MSC) ainda é negociado em algumas trocas, a série atual de clientes da carteira de desktop fornecem suporte para Bitcoin (BTC) e Omni (OMNI) somente, enquanto cliente baseado na web do projeto (chamado Omniwallet) pode ser personalizado para incluir outras ativos. Omni utiliza como mecanismo de consenso o *Proof-of-Stake* e como algoritmo de hash, o Scrypt.

- https://bitcointalk.org/index.php?topic=265488.0;
- https://github.com/mastercoin-MSC;
- https://bter.com/coininfo/MSC;
- https://cyber.fund/system/Mastercoin_(Omni);
- http://bravenewcoin.com/mastercoin#Trading-Pairs.

MaidSafe (https://maidsafe.net/) e **Storj** (https://storj.io/) não são moedas, mas plataformas que objetivam serem espaços de armazenamento de dados e de aplicações com funcionamento descentralizado. Ambas confiam nos discos rígidos dos utilizadores para armazenamento em nuvem, em vez de servidores centralizados.

MoodCoin (http://moodcoin.org/) é a moeda de criptografia oficial da plataforma MoodCrawler; a primeira plataforma que facilita e premia interações humanas positivas (recompensa os usuários que ajudam os outros). Desse modo, cria um ambiente em que os usuários apresentam problemas e recebem soluções (http://moodcrawler.org/mc/the-moodcrawler-ecosystem/).

Steem (https://steem.io/ e https://github.com/steemit/steem) é um criptomoeda que premia os usuários para a construção da comunidade postando e *upvoting* (registrar aprovação ou concordância com um post) conteúdo valioso para os outros. Steem (estima) foi inspirado do sucesso do Reddit (https://www.reddit.com/), onde a comunidade ajudou a enriquecer os acionistas.

BRK - Breakout Coin (http://www.breakoutcoin.com/), é a moeda da Breakout Gaming (http://breakoutenterprise.com/); uma empresa de

entretenimento e jogos on-line (poker, apostas desportivas, casino, etc.). A moeda original, Breakout Coin, foi posteriormente integrada a um sistema de carteira multimoeda única chamada Breakout Chain (cadeia Breakout). O sistema de pagamento Breakout Coin suporta várias moedas (*multicurrency*), cada uma com propriedades diferentes. A cadeia Breakout (*Breakout Chain*) é um híbrido de PoW e PoS, mas que emitem moedas diferentes. Enquanto Breakout Coin (BRK) continua a ser a moeda principal de Breakout Gaming, há também as moedas Breakout Stake (BRX) e Sister Coin (SIS), que servem para fixar a contabilidade através de um sistema combinado de prova de participação (PoS) e prova de trabalho (PoW); enquanto que através da PoS se emite Breakout Coin, pelo PoW emite-se Sister Coin como um incentivo para os mineiros. Os proprietários de Breakout Stake (BRX) têm participação na rede de cadeia de Breakout. Ao apoiar a rede desta forma, os interessados Breakout ganham juros (de 5% por ano) sobre sua participação; que são pagos com Breakout Coin.

- https://bitcointalk.org/index.php?topic=808648.0;
- https://bitcointalk.org/index.php?topic=1509819.0;
- https://github.com/BreakoutCoin;
- https://www.reddit.com/r/BreakoutCoin/;
- http://breakoutjournal.com/;
- https://chain.breakoutcoin.com/BlockCrawler/block_crawler.php;
- http://www.breakoutcoin.com/coinsale-brx/;
- https://coinmarketcap.com/currencies/breakout/;
- https://coinmarketcap.com/currencies/breakout-stake/.

SXC - Sexcoin (https://www.sexcoin.info/), possui como meta uma maneira para fornecedores e consumidores de "conteúdo adulto" terem um método rápido, estável e seguro de transações que protege a privacidade.

- http://blockexplorer.lavajumper.com/chain/Sexcoin;
- https://bitcointalk.org/index.php?topic=218158.0;
- https://github.com/sexcoin-project/sexcoin;

- https://sexcoinforum.com/;
- http://coinwik.org/SexCoin;
- https://sexcoin.miningpoolhub.com/;
- https://coinmarketcap.com/currencies/sexcoin/;
- http://www.coinwarz.com/cryptocurrency/coins/sexcoin.

SBC - Stablecoin é um serviço de mistura de moeda objetivando garantir que as transações sejam criptografadas e não rastreáveis.

- https://bitcointalk.org/index.php?topic=227766.0;
- https://github.com/stablecoin/stablecoin;
- http://coinwik.org/StableCoin;
- https://www.reddit.com/r/StableCoin/.

BLC - Blakecoin (https://blakecoin.org/) foi a primeira criptomoeda a empregar BLAKE-256 (um candidato no Instituto Nacional de Padrões e Tecnologia na competição para se tornar o novo SHA-3 padrão) como o seu algoritmo de hashing; que é mais rápido do que o SHA-256 usado pelo Bitcoin. Blakecoin também utiliza um algoritmo de dificuldade com personalização assimétrica. A recompensa para a mineração do Blakecoin está definida em 25 *blakecoins* mais a inflação; que é calculada como sendo a raiz quadrada de: (dificuldade x altura do bloco).

Bitcoin XT (https://bitcoinxt.software/ e https://github.com/bitcoinxt/bitcoinxt), é um *fork* do Bitcoin Core. Por outras palavras, é uma implementação de um nó completo ("full node") do Bitcoin (https://bitcoin.org/pt_BR/download). O **Omni Core** (http://www.omnilayer.org/) também é uma Bitcoin Core melhorada, que fornece todas as funcionalidades do Bitcoin, bem como recursos avançados de camada Omni.

QUAIS SÃO AS ALTCOINS PROMISSORAS?

Através das orientações dadas nos outros capítulos, o leitor conseguirá realizar uma análise sobre quais altcoins possuem probabilidade de valorização, aceitação, popularização e êxito.

Recapitulando de forma superficial, há de se averiguar se é uma moeda séria; se não passa de uma mera réplica ou clonagem idêntica de outra criptomoeda já existente; qual é a atual cotação; se existem patrocinadores, investidores, colaboradores, parceiros, desenvolvedores e todo um ecossistema (*wallets*, *miners*, *exchanges*, *altcoiners*, etc.); quais são as críticas e expectativas nos fóruns; quais são os diferenciais, aperfeiçoamentos e inovações; quais são os planos, projetos, objetivos e/ou filosofia por trás da moeda; quais são os currículos e antecedentes das pessoas envolvidas no projeto; a quanto tempo a criptomoeda existe; se ocorreram escândalos, fraudes ou golpes na comunidade da moeda e quais foram as consequências, providências e repercussões disso; se algum dos componentes do código da moeda digital já demonstrou erros, defeitos, falhas, panes e/ou danos através de outra criptomoeda; se houve *premine* e qual a justificativa dessa pré-mineração; se a mineração é algo popular ou restrita ao ricos ou um grupo seleto; se a moeda possui procedimento ou manuseio simplificado ou facilitado para os leigos; etc.

Além disso, é recomendável acompanhar os fóruns (por exemplo, https://bitcointalk.org/index.php?board=67.0) e os vários sites que fornecem notícias recentes sobre bitcoin e altcoins, como forma de auxílio na avaliação das criptomoedas.

- http://www.altcointoday.com/;
- https://cointelegraph.com/;
- http://www.coindesk.com/;
- https://www.cryptocoinsnews.com/;
- http://www.cryptocoinupdates.com/;
- http://bitcoinsaltcoins.com/;

- https://www.crypto-news.net/;
- https://coins.newbium.com/;
- http://www.coinstreetnews.com/;
- http://cryptopools.com/;
- http://thedashtimes.com/;
- https://www.ethnews.com/;
- https://coinidol.com/;
- http://coingreed.com/;
- http://www.coinporch.com/;
- http://cryptohustle.com/;
- http://www.livebitcoinnews.com/;
- http://www.cryptocoinhome.com/;
- http://www.blockchainster.com/;
- http://www.newsbtc.com/;
- http://www.bitcoinbragger.com/;
- https://news.bitcoin.com/;
- http://bitcoinist.com/;
- http://woobull.com/;
- http://themerkle.com/.

A maioria das altcoins são *shitcoins* (moedas de merda) e muitas delas só podem ser compradas utilizando (como forma de pagamento, seja trocando, seja destruindo) bitcoins; o que, além de ser complicado para os leigos ou iniciantes, é algo contraditório. Explica-se. Uma altcoin séria irá querer se desprender, desvincular, separar, ser independente e superior ao Bitcoin. É, no mínimo, muito estranho uma altcoin somente poder ser comprada através de bitcoins. Isso levanta a grande possibilidade da altcoin ser apenas uma forma do seu responsável conseguir receber bitcoins facilmente através da

troca ou de forçar a valorização do bitcoin através da redução de sua quantidade através da destruição (queima) de suas unidades.

Algumas pessoas acreditam que Bitcoin, Lightcoin e outras moedas dependentes de ASIC não prosperarão. Se isso acontecer, as moedas como Vertcoin, Ultracoin ou Darkcoin poderão ser as favoritas.

O **Litecoin (LTC)** desponta como a principal competidora do Bitcoin. Alguns acreditam que enquanto o Bitcoin é o ouro, a Litecoin é a prata das moedas digitais. Criado em 2011, o Litecoin continua forte após esses anos todos. O Litecoin é tecnicamente superior ao Bitcoin e possui uma comunidade bem desenvolvida de usuários, mineradores, empreendedores e especuladores.

A **Feathercoin (FTC)** é derivada direta da litecoin, que permite ajustar sua dificuldade de mineração mais frequentemente do que o Litecoin.

A **Peercoin (PPC)** foi fundada em 2012 e tem-se mantido firme. A Peercoin também afirma exigir menos energia elétrica para sua produção em comparação com Bitcoin e outras moedas virtuais.

A **Novacoin (NVC)**, um *fork* do Peercoin, tem chamado a atenção principalmente pela segurança e pela mineração ser feita de forma diferente das outras altcoins. No futuro a rede quase não vai precisar de energia elétrica para continuar realizando as operações. Isso agrada a várias pessoas; tanto por questões ambientais como econômicas.

A **Namecoin (NMC)** começou as atividades em 2011 e já esteve no terceiro lugar das criptomoedas. A principal novidade dela é o fato o anonimato ser maior do que no Bitcoin. Característica esta que valoriza muito um altcoin.

As transações **Stablecoin (SBC)** são criptografadas e não rastreáveis.

A **Ethereum (ETH)** possui uma comunidade considerável e forte. Também pesa a seu favor os seus contratos inteligentes. Uma incógnita é qual será o resultado da solução aplicada para reparar uma falha. Essa “novela”

já rendeu uma bifurcação dividindo sua comunidade; trata-se do Ethereum clássico (ETC).

A **Dash (DASH)** utiliza o algoritmo Darksend para ajudar a tornar anônimo o processo de transação através da mistura de moedas. Dash também procura se tornar uma moeda digital mais prática do que a Bitcoin, possuindo um recurso de transação de confirmação semelhante ao que está previsto para a Gulden. Dash também planeja substituir os longos endereços de criptografia com nomes de usuários em uma grande atualização. A Dash ultrapassou em popularidade a Ethereum no Purse.io.

A **Anoncoin (ANC)** possui um toque de anarquia; vez que elas não poderiam ser rastreadas. Ela foi criada por um grupo de ativistas virtuais denominados "anonymous" (anônimos) baseada na I2P; a internet invisível.

A **Navajo (NAV)** está para retomar a possibilidade de transações anônimas criando uma segunda *blockchain*.

A **Ripple (XRP)**, ao contrário da bitcoin e de outras altcoins, não é produzida através da mineração. Em vez disso, a criptomoeda é concebida como uma rede de pagamentos. A rede Ripple acomoda outras moedas virtuais e também suporta moeda de comércios automatizados.

A **Factom (FCT)** é uma empresa de tecnologia que desenvolve ferramentas baseadas em blocos de chaves para gerenciamento de dados e segurança. A Factom pretende proporcionar acesso seguro dos dados de saúde (registros médicos seguros, prontamente disponíveis e confiáveis) via smartphones em países em desenvolvimento. Usando a tecnologia *blockchain*, a Factom constrói registros distribuídos globais que podem ser acessados, independentemente da localização, por qualquer pessoa autorizada com verificação biométrica. Detalhe, ela recebeu uma considerável doação do Bill Gates.

A **Gulden (NLG)** é uma criptomoeda focada na usabilidade como um meio digital de pagamentos diários. Está caminhando para levar sua tecnologia ao mundo de uma forma muito menos intimidante. Em vez de tentar melhorar as funcionalidades de privacidade do Bitcoin como fizeram

moedas como Monero (XMR) e Zcash (ZEC), a Gulden mantém um único foco na facilidade de uso como um meio de trocas no negócio ou comércio regular. A Gulden lançou uma atualização permitindo que os fundos sejam enviados de forma transparente para carteiras Gulden, carteiras Bitcoin e até mesmo para contas bancárias europeias. É de grande importância essa capacidade de as carteiras transferirem fundos para destinos não-Gulden. Isso significa que um usuário pode comprar Gulden e gastá-lo em qualquer lugar onde Gulden ou Bitcoin são aceitos; bem como enviar fundos para contas bancárias convencionais, tudo dentro de um único aplicativo simplificado.

Recorda-se que a acessibilidade ou a simplicidade de manuseio aumenta o valor da altcoin; vez que isso facilita a sua popularização. Outro detalhe, uma criptomoeda que só é compreendida e/ou manuseada por *nerds*, *geeks* ou expertos em informática está predestinada ao fracasso.

A **Stellar Lumens (XLM)** está a lançar uma das primeiras aplicações *blockchain* que pode conter o potencial de afetar um grande número de pessoas fora do espaço da moeda digital, através da sua transferência global de dinheiro destinada a alguns dos maiores mercados de remessas do mundo.

A **NEM (XEM)** foi lançada em 31/03/2015 e foi escrita em Java. Introduziu novos recursos na *Blockchain*, tais como, por exemplos, seguros, contas *multi-signature* (multi-assinatura) e sistema de mensagens criptografadas. É utilizada na *blockchain* privada Mijin e está sendo testada por instituições financeiras e empresas privadas no Japão.

A **Decente (DCT)** é uma plataforma de distribuição de conteúdo descentralizado, que é *open-source* e utiliza *Blockchain* para garantir a segurança. É destinada a pessoas criativas, autores, blogueiros, publicitários e seus fãs e seguidores que permite a publicação sem bordas de qualquer texto, imagem, vídeo ou música de conteúdo.

Steem (STEEM) é basicamente um site que recompensa os usuários pelas postagens que recebem múltiplos *likes* (curtidas, positivos, aprovações ou gostei) dos participantes.

A **Monero (XMR)** é outra forte concorrente dentre as criptomoedas anônimas. Ela usa um método chamado CryptoNote. Monero não é um clone do Bitcoin e deriva da Bytecoin (BCN), uma altcoin precoce.

A **Zcash (ZEC)** é uma criptomoeda descentralizada e aberta que visa estabelecer um novo padrão de privacidade e anonimato através do uso inovador de criptografia zk-SNARK. Enquanto que Zcoin (XZC) esconde todas as partes de uma transação, exceto o montante enviado, a Zcash esconde tudo. A Zcash torna possível para as empresas esconderem detalhes da transação dos concorrentes, de ladrões e de inimigos estrangeiros; ainda que revelando, simultaneamente, as informações à autoridade fiscal do país. Um artigo do jornal "The New York Times" descreveu a Zcash como sendo a moeda virtual mais difícil de rastrear.

- http://www.nytimes.com/2016/11/01/business/dealbook/zcash-a-harder-to-trace-virtual-currency-generates-price-frenzy.html?_r=1.

A equipe da **Zcoin (XZC)** está trabalhando em um novo algoritmo de mineração para permitir a mineração usando uma CPU comum e, ao mesmo tempo, para combater o problema das *botnets* (vários computadores infectados com *malware* tornando-se uma rede zumbi) controladas por *hackers* que geralmente acabam dominando a mineração CPU.

A **Vertcoin (VTC)** parece para ser bastante promissora em razão de sua comunidade emergente, ser resistente ao ASIC e contar com um núcleo fortemente descentralizado. Sua tecnologia de segurança também é um grande atrativo.

A **Worldcoin (WDC)** foi projetada para ser a mais rápida. Sua transação pode ser confirmada em 20 segundos.

A **QuarkCoin (QRK)** usa mineração CPU, é à prova de ASIC, gera um novo bloco a cada 30 segundos e implementa nove rodadas de hashing, escolhendo entre seis métodos de hashing diferentes.

Uma moeda que tem se tornado atraente em questões de mineração (dificuldade baixa) e ainda possui valor baixo, é o **CryptoEscudo (CESC)**.

A **VeriCoin (VRC)**, lançada em 2014, se proclama rápida (30x mais que o Bitcoin), gratificante (paga juros) e segura.

A **Lisk (LSK)** é a primeira criptomoeda que utiliza cadeias laterais modulares. Ela permite que qualquer pessoa possa usar a sua plataforma para construir suas próprias aplicações descentralizadas. A linguagem de escolha para Lisk para construção de aplicativos individuais é o JavaScript, uma das linguagens de programação mais populares do mundo. Lisk quer ser o padrão de fato para aplicações *blockchains* e serviços que são autônomas e descentralizadas, aplicativos baseados em *blockchain* desenvolvidos em JavaScript com aplicações descentralizadas (‘Dapps’) tem um grande potencial para ser integrado em uma ampla variedade de aplicações, incluindo armazenamento imutável, uma federação descentralizada de hospedagem, serviços Oracle ou cálculo dos contratos inteligentes, etc. Ex-membros do núcleo Ethereum juntaram-se ao Lisk. Lisk iniciou um o projeto de embaixador do País, tendo esta iniciativa para promover o ecossistema Lisk e ajudar a fornecer suporte técnico.

A **Waves (WAVES)** é uma das novatas que merece ser melhor estudada.

Uma forma óbvia de escolher em qual ou quais moedas digitais investir é acompanhar as cotações para saber quais estão sendo cada vez mais valorizadas e, pelo contrário, quais estão cada vez mais desvalorizadas. Mas essa estratégia não rende muitos lucros por ser muito óbvia para qualquer um e, principalmente, por implicar na compra da moeda quando ela já está sendo valorizada. Por outras palavras, a lucratividade é muito maior quando se “aposta” (investe ou aplica) na moeda quando ela ainda está iniciando, é desconhecida, praticamente sem valor e a mineração ou aquisição é bem mais fácil.

Para quem não tem tempo ou capacidade de pesquisar e estudar as moedas novatas, uma estratégia é confiar na avaliação e investimento feitos por outras pessoas. Desse modo, deve-se conferir quais são as moedas novatas que foram incluídas em *exchanges*, *wallets* e bancos tradicionais e de credibilidade; quais receberam grandes doações ou investimentos; quais possuem grandes ou fortes parceiros e/ou colaboradores; quais possuem uma comunidade pré-formada; etc. Por outras palavras, se uma moeda novata já

começa com apoio e parceiros de peso, isso a destaca das demais que ainda terão que “correr atrás” de conseguir esses apoiadores e parceiros.

A Apple, por exemplo, aprova em sua loja de aplicativos (*App Store*) os aplicativos que lidam com apenas 9 criptomoedas: Bitcoin, Dogecoin, Litecoin, Ethereum, DAO, Ripple, Lisk, Digicash e Steem.

CRIE SUA PRÓPRIA MOEDA VIRTUAL

Criar uma criptomoeda é algo bem simples e fácil para quem possui alguma compreensão de codificação (linguagem de programação); vez que se pode facilmente construir uma altcoin em cima (fazendo pequenos ajustes, modificações, adaptações ou personalizações) de códigos existentes, pois a maioria das plataformas são de código aberto e disponíveis para download em plataformas de compartilhamento de códigos como o GitHub, por exemplo. Desse modo, os desenvolvedores de uma altcoin podem escolher o algoritmo usarão como base e fazer uso do respectivo código-fonte para criar uma bifurcação (*fork*) e, assim, dar origem à sua própria altcoin.

Aqueles que não estão familiarizados com codificação, mas, mesmo assim, querem ter sua própria criptomoeda, podem fazer uso dos serviços online de criação, hospedagem e manutenção de uma altcoin. Entretanto, apesar de que criar uma altcoin é algo relativamente simples, isso não quer dizer que a nova altcoin funcionará, será viável, será aceita ou que prosperará. Por outras palavras, pode-se fazer uma comparação com o parto de um bebê, o qual pode ser natimorto. A criação de uma altcoin pode, ainda, ser comparada ao ato de plantar uma planta. Pode-se enterrar uma semente (ou um pedaço de uma planta como ocorre com a mandioca e a cana-de-açúcar) ou aterrar as raízes de uma muda. Simploriamente plantou-se, mas somente esse ato não quer dizer que a planta irá se desenvolver; vez que exige análise prévia do solo, do local específico nesse solo onde plantá-la (verificação da quantidade de luz e de sombra; bem como do risco de animais cavarem, pisotearem ou comerem a planta), a profundidade de aterramento, a época do ano, adubação, irrigação, podas, combate a pragas e infecções, etc. Outra analogia pode ser feita com um automóvel. Pode-se dizer que se construiu um veículo automotor desde que a criação consiga se locomover, nem que seja apenas com 5 Km/H e que faça 1 Km com 20 litros de combustível. Portanto, regra geral, qualquer pessoa pode ter filho, construir um motor que se locomove ou colocar terra sobre uma semente ou raízes de uma muda; mas dar certo e prosperar já vai além da simplicidade do ato básico. Por incrível que pareça, o fato de a altcoin funcionar, ser viável e possuir recursos interessantes não são as maiores dificuldades. O maior problema ou a parte mais difícil de criar um criptomoeda é ganhar aprovação popular e ser colocada em uso. Sem essa aprovação qualquer

criptomoeda é inútil e será extinta por falta de adesão. Por outras palavras, não adianta ter o melhor produto ou serviço; o que importa é conseguir popularidade e uso. E para conseguir cativar as pessoas, a maioria das altcoins são construídas em torno de uma ideia, para incentivar alguma coisa ou para resolver alguns problemas do mundo real ou defeitos de outras criptomoedas.

O primeiro passo é encontrar um grupo ou uma comunidade para poder construir uma moeda para eles ao invés de criar uma moeda e esperar que todo mundo apareça. Por exemplo, o fórum brasileiro L2JBRASIL (http://www.l2jbrasil.com/) é um fórum voltado para a programação em Java de servidores do jogo LineAge II desenvolvido pela NCSoft. Este fórum iniciou com tutorias traduzidos; entretanto, a iniciativa foi agregando adeptos e colaboradores e, assim, foi-se constituindo uma comunidade brasileira, com companheirismo e solidariedade.

- https://groupcurrency.org/.

Por outras palavras, deve-se formar um grupo de pessoas, ou ingressar em um, para começarem a discutir o projeto publicamente pela Internet e deixar que outras pessoas adiram ao mesmo. Ou seja, não é aconselhável apresentar uma moeda totalmente pronta para que as pessoas a aceite. Esse tipo de atitude é vista com desconfiança pelo fato de que muitos golpistas e oportunistas agiram dessa forma. Pode-se iniciar o debate através das qualidades e dos defeitos das moedas virtuais existentes, com o que se pode aproveitar o que já existe de bom em todas as moedas virtuais existentes e excluir o que se considera como erro ou fracasso. Por outras palavras, pode-se começar com uma enquete (questionamento ou pesquisa) sobe quais são as melhores e as piores características, qualidades, recursos, funções, componentes, itens, engrenagens, etc. das altcoins existentes. Através desse simples procedimento já se saberia de antemão (previamente) o que agrada e o que desagrada na comunidade altcoin.

Outra opção seria sugerir a ideia para uma comunidade ou grupo coeso, unido, solidário, harmônico, democrático, universal ou, até mesmo, fechado para estimular mais o comércio e integração entre seus membros ou para desenvolver o comércio em determinada localidade, área ou entidade.

Exemplos clássicos consideráveis de grupos que podem ser utilizados são as denominações religiosas, as confrarias, os clubes, as associações civis sem fins lucrativos, fundações, ONGs, ORGs, etc. Imagine uma moeda virtual com uma mensagem religiosa, moral, ética, cívica ou filosófica em resposta e contraposição à certas degradações da sociedade? Do mesmo modo que existem selos e moedas comemorativas, poder-se-ia criar uma moeda virtual como forma de manifesto, protesto, conclamação, proclamação, recordação ou divulgação de alguma mensagem, ideia, conceito, dogma, crença, credo, tese, projeto, ideal, sonho, vitória, conquista, recordação ou doutrinação. Mas, frisa-se, quanto mais dar a ideia de universalidade melhor será e, por outro lado, quanto mais der a impressão de ser um grupo restrito, regional ou fechado, pior será.

De modo similar poder-se-ia unir esforços, como, por exemplo, uma determinada entidade ou associação (comercial, de empresários, de agricultores, de fazendeiros, de profissionais liberais, de escritores, de artistas, de profissionais de informática, etc.) que poderia acordar que seus membros somente receberiam em determinada moeda virtual, possibilitando ao cliente comprá-la no local, com o que estar-se-ia divulgando-a e explicando como a mesma funciona. De início seria necessário aceitar as primeiras moedas das primeiras pessoas envolvidas na criação das mesmas, evitando-se que as moedas sejam acumuladas por estes; mas, pelo contrário, que sejam postas em circulação e se tornem de conhecimento e aceitação públicas.

Imagine uma localidade onde há enorme índice de furtos e roubos parar de usar a moeda convencional ou nacional, e outros meios equivalentes tradicionais, para passar a somente usar uma moeda virtual que só tem valor entre os membros daquela comunidade ou lugar? Como ficariam os ladrões que eram acostumados a pegarem as cédulas que haviam no caixa ou na máquina registradora?

- http://g1.globo.com/pi/piaui/noticia/2016/05/apos-criar-moeda-propria-cidade-do-piaui-nao-registra-assalto-ha-um-ano.html.

E se uma escola ou faculdade de informática e/ou de administração de empresas colocasse como parte do cronograma do curso, justamente participar do desenvolvimento de uma moeda virtual? Não seria uma forma

mais dinâmica, didática e real de ensino? E se os professores, ex-alunos, profissionais e qualquer pessoa interessada pudesse participar?

Enfim, a criação de uma moeda criptográfica pode ser benéfica para várias entidades, organizações, associações e grupos em geral (religiosos, ativistas, ideológicos, etc.). Um determinado grupo poderia, assim, criar uma moeda criptográfica com um percentual pré minerado (uns 10%, por exemplo), para esses créditos ficarem retidos numa conta (fundo) virtual para ir valorizando com o tempo até poder ser utilizada num objetivo ou causa prédeterminada. E essa conta virtual acetaria depósitos e doações para que os créditos do fundo aumentassem ainda mais. Por óbvio que esse fundo possuiria alguma destinação prévia de interesse do grupo criador da moeda digital e possuiria controle rígido de utilização desses créditos. Por exemplo, o fundo somente poderia ser utilizado através de múltiplas assinaturas (controle coletivo) ou mediante a aprovação (consenso) da maioria dos integrantes ou de alguns membros aleatórios da respectiva rede P2P. Além dessa conta virtual para guardar os fundos para futuro uso previamente estabelecido, poder-se-ia, também, ter outra com cerca de 10% (também fruto da pré mineração) para a diretoria utilizar na divulgação e promoção da própria moeda virtual. Ao invés dos membros, adeptos, simpatizantes e colaboradores do grupo realizarem serviços gratuitos ou efetuarem doações de bens, receberiam através da referida moeda virtual o pagamento de seus serviços e dos bens que fornecessem à entidade. Do mesmo modo, ao invés das pessoas realizarem doações em moeda convencional, efetuariam doações na moeda virtual; ou seja, a entidade se recusaria a aceitar a moeda convencional, nem que tivesse um guichê para a imediata conversão para os leigos poderem fazer as doações e aprenderem como funciona. Essas práticas ajudariam na divulgação, promoção, aprendizado, popularização e valorização da moeda digital. Ainda mais, a quantidade de serviços voluntários e doações de bens para a entidade aumentariam. Além dos 20% de moedas pré minadas acima exemplificadas, também poder-se-ia ter mais 10% para serem distribuídas gratuitamente nos eventos de lançamento e de divulgação da respectiva moeda digital para poder dar início às operações da mesma. Inclusive, poderiam ser feitos sorteios de unidades da moeda em todas as reuniões da entidade como forma de atrair novos adeptos para a causa. Também determinados bens e serviços da entidade poderiam ser vendidos com preços menores se pagos com a

referida moeda virtual para forçar o interesse em aprender e passar a utilizá-la; como, também, ser implementado algum sistema de recompensa ou de sorteios para quem pagar com a moeda digtal. Em determinados eventos internos ou fechados, poderia-se somente aceitar os pagamentos na moeda virtual. A mineração da moeda posterior ao seu lançamento somente poderia ser feita através de uma espécie de autorização temporária (com limites diversos de tempo); a qual seria vendida e também usada como forma de gratificação aos colaboradores como meio de aumentar a quantidade de colaboradores. Essa autorização ou permissão de minerador seria uma chave (código) de desbloqueio temporário da função mineradora do software. Alguns políticos já fizeram procedimento semelhante a esse sugerido para angariarem fundos para a campanha eleitoral. Em resumo, o político guardou parte das moedas consigo e os seus patrocinadores e correligionários foram comprando, minerando, divulgando, estimulando e usando as demais unidades da moeda virtual até que num determinado momento ela atingiu uma boa cotação e o político vendeu todas as suas unidades.

A criação de uma nova moeda digital necessita de uma pesquisa prévia das moedas que já existem, que já existiram, que ainda serão lançadas e daquelas que foram inventadas, mas nunca foram lançadas. Explica-se. Esse procedimento é necessário para não conflitar os nomes e/ou projetos, não criar confusão, não gerar descrédito, não sofrer algum tipo de processo judicial, etc. Também é útil para aprender com os acertos, qualidades, sucessos, erros, falhas, defeitos, fracassos... das moedas anteriores. Ainda mais, é possível estudar, comparar, aproveitar, adaptar e até misturar os códigos fontes das outras moedas.

Que tal, por exemplo, a **criação de uma criptomoeda que incentive o compartilhamento do conhecimento**? Mas não seria nada como um simples site de perguntas e respostas. O programa cliente possuiria um processador de textos embutido (o que ajuda a manter a rede ativa), onde o usuário iria escrever artigos, apostilas e *e-books*, com determinados requisitos pré-definidos (tais como, por exemplos, relação de temas permitidos e temas proibidos [conteúdo indesejável, criminoso, ofensivo, inútil, propaganda, etc.]; quantidade mínima de tópicos ou capítulos; a quantidade mínima de caracteres e/ou de páginas; etc.). O ISBN - *International Standard Book Number* da obra seria fornecido pela rede e a obra seria disponibilizada

exclusivamente na rede. Todos os usuários poderiam fazer a leitura gratuita online das obras através do programa cliente (o que ajuda a manter a rede ativa). A cada página lida da obra, o autor recebe alguns centavos da moeda. À cada *like* (gostei ou curti) da obra, cada comentário e de acordo com a avaliação de 0 (zero) a 5 (cinco) estrelas, o autor recebe mais créditos. Entretanto, a cada "não gostei" ou "não curti", comentário desfavorável, avaliação negativa (zero estrelas) ou erro detectado, o autor é punido com descontos em seus créditos. Se ficar comprovada a fraude ou o plágio, o autor perderá todos os seus créditos (inclusive os já recebidos), deverá pagar um valor como multa e a obra será excluída da biblioteca com todos os seus arquivos acessórios indexados (comentários, avaliações, críticas, perguntas e respostas). Ainda mais, a cada *feedback* prestado ou comentário respondido, ambos dentro de um determinado prazo limite, o autor recebe mais centavos da moeda. E quem fez a indagação ou pergunta também recebe. Portanto seria, também, uma rede social do conhecimento. Para poder entrar na rede e acessar sem limite de quantidade de obras ou de leituras, o usuário não paga nada. Seria o modo somente leitura. Mas para poder ativar as demais opções (comentar, fazer perguntas, avaliar, etc.), teria que pagar uma espécie de assinatura simbólica; que somente pode ser paga na respectiva moeda digital. Esse pagamento (assinatura de membro que interage) não daria o direito imediato às unidades da moeda, mas estas seriam consequência direta de sua interação no sistema. Por outras palavras, o interessado teria que antes comprar unidades da moeda de algum particular para depois usá-las no pagamento da assinatura ao sistema. Para poder enviar um artigo, apostila ou um *e-book* à rede ou para poder ser um jurado de aprovação das obras, o usuário teria que pagar um determinado valor na moeda digital conforme o tamanho da obra ou manter o sistema da *blockchain* por, digamos, 720 (setecentos e vinte) horas. Antes da obra ser incorporada à biblioteca digital, 5 (cinco) membros da rede analisam (julgam) se ela preenche os requisitos, se não é plágio, se já não existe obra igual ou muito semelhante, se não se trata de cópia de obra de domínio público, se tem originalidade, etc. Para facilitar o trabalho dos julgadores, poderia o próprio sistema fazer uma análise prévia antiplágio (programas farejadores utilizados em Monografias e TCCS - Trabalhos de Conclusão de Curso) para ser submetida à análise final pelos julgadores. Pelo simples fato de julgar (não só a publicação da obra, mas, também, sobre aprovações de pagamentos, deletamento de obras, retificações de obras, etc.), esses

membros recebem alguns centavos da moeda e por cada fonte (*link*, site, anexo, *print*, documento, foto, etc.) de informação (prova, pesquisa, conferência, verificação, etc.) sobre os itens de julgamento, recebe mais centavos. Quem conseguir provar plágio, cópia, fraude ou trapaça recebe um prêmio maior. Os usuários recebem centavos da moeda por fazerem comentários e avaliações das obras na biblioteca digital. A cada uma hora conectado na rede em combinação à velocidade da Internet e à capacidade no disco rígido reservadas (dedicadas) para o sistema da moeda, o usuário recebe tantos centavos da moeda; exceto quando utiliza esse tempo ou respectivos créditos para pagamento de tarifas do sistema. Os usuários que conseguirem detectarem erros, incorreções, equívocos ou enganos nas obras são contemplados também. Essas sugestões de revisões, retificações, correções, adendos e acréscimos são enviadas ao autor para aprovação ou inserção de nota de rodapé com tais observações críticas (caso aprove, ele substituirá o arquivo por outro revisado); caso o autor rejeite ambas opções (retificação ou nota de rodapé), as críticas serão enviadas à uma junta de especialistas para votarem o acréscimo de uma nota de rodapé na obra com a dita observação (substituição do arquivo original com a nota de rodapé). Para que algumas obras não sejam lidas de graça, mas sim vendidas, o autor terá que pagar um valor maior à rede. Em caso de mais uma obra sobre o mesmo tema, assunto ou questão, que sejam muito semelhantes no conteúdo, os usuários podem votar qual delas é a melhor ou a mais completa, com o que somente a vencedora continuará na biblioteca; as perdedoras serão deletadas com todos os seus acessórios. O envio de novas edições de uma obra, implica no deletamento da versão anterior (substituição). Seriam permitidas propagandas pagas nessa rede social para poderem ajudar a sustentar a moeda e os vários pagamentos aos usuários. Também haveria a opção paga de imprimir a obra, que seria calculada de acordo com a quantidade de páginas desejadas. Os usuários ainda teriam a opção de pagar as taxas através de doação de obra à rede; assim, a cada 1 (uma) obra doada, o usuário pode publicar uma gratuitamente para acesso gratuito e, à cada 3 (três) obras doadas, o usuário pode publicar outra de graça para ser vendido o acesso. De modo semelhante, a cada 30 (trinta) participações gratuitas como jurado de aprovação, o usuário poderá ser por 6 (seis) meses um jurado remunerado. A cada 300 avaliações ou 300 comentários o usuário poderá publicar uma obra de acesso gratuito e, à cada mil avaliações ou mil comentários poderá publicar uma obra para ser vendida. Os créditos do

autor (direitos autorais) podem ser cedidos à alguma entidade, instituição ou causa. De todas as obras seria permitida a transcrição de trechos de até 3 (três) páginas completas, desde que devidamente informados os créditos de autoria e o link de acesso direto à obra na biblioteca digital. Aos autores seria permitido divulgarem o link de acesso de suas obras para aumentar a visualização das mesmas. Inclusive, professores podem colocar suas apostilas de aula no sistema para que os seus alunos a visualizem. E, ainda, a biblioteca digital poderia ser integrada nas escolas para o uso durante as aulas. Na rede em si pode-se usar pseudônimos, codinomes ou nomes de usuários, mas a rede possuiria a identificação dos usuários para evitar a prática de crimes ou ilícitos; bem como permitir a punição aos criminosos e infratores. Não seria permitido o envio de obras de terceiros ou de qualquer documento aleatório; seria exigido que o conteúdo fosse criado pelo usuário dentro da plataforma do sistema (para ajudar a rede ficar ativa). Por óbvio o sistema exigiria capacidade em disco rígido e determinada mínima velocidade de Internet dedicadas (reservadas) ao sistema da moeda para poder participar; vez que seriam nos discos rígidos dos usuários que a biblioteca seria armazenada. Pode-se, ainda, ser ofertado o serviço de hospedagem na nuvem (*cloud computing*) para qualquer pessoa, pelo qual seria pago, de forma antecipada, um valor diário conforme a quantidade de dados e, ainda, diferenciada dita tarifa conforme tais dados seriam liberados ao público, de acesso a pessoas determinadas ou de acesso exclusivo do proprietário. A criação de cada unidade da moeda seria correspondente aos Megabytes (MBs) de dados inseridos no sistema (rede social combinada com biblioteca digital). O tamanho do bloco seria o equivalente ao tamanho mínimo de uma obra e cada linha da obra seria um centavo da moeda. Seria permitido o envio de várias linhas independentes desde que somadas atingissem o tamanho mínimo exigido; mas aos julgadores seria dado o privilégio de poderem construírem centavos soltos; ou seja, de enviarem obras de tamanho inferior ao mínimo. Os comentários, avaliações, críticas, perguntas e respostas na rede também são arquivos indexados, mas independentes, possuindo a finalidade de troco (centavos). Como cada arquivo é a moeda em si, existem arquivos que são de propriedade do próprio sistema e destes, há os que podem ser vendidos (mudada a titularidade) e os que não podem ser vendidos (manuais, tutoriais e FAQs [*Frequently Asked Questions*] da própria moeda). Já os arquivos particulares, em regra, podem ser vendidos pelos seus titulares; exceto se

doados com a cláusula de inalienabilidade que possuirá um limite de tempo definido pelo doador. Os rendimentos diferenciados e individuais de cada arquivo são os principais diferenciais dessa moeda digital sugerida. Haveria, ainda, a necessidade de os arquivos serem identificados tal como cédulas que não podem ser cortadas para serem divididas. Assim em cada bloco deve haver a identificação das partes independentes (e, portanto, divisíveis) que o formam. Seria necessária uma pequena pré mineração para poder existir créditos para os pagamentos iniciais para sustentar o sistema (existirem moedas para serem vendidas, dadas de trocos e fazer os primeiros pagamentos). Essa pré-mineração seria através da doação à rede dos manuais, tutoriais e FAQs [Perguntas Mais Frequentes] da própria moeda; bem como textos de domínio público e, inclusive, máximas e ditados populares, nomenclaturas e definições (tal como verbetes de um dicionário ou de uma enciclopédia), brocardos forenses, frases de grandes pensadores, leis da física, leis da matemática, artigos de legislação e versículos bíblicos para servirem de centavos. Inicialmente não existiria limite de quantidade de moedas emitidas (o deletamento de certas obras e seus acessórios já serve de controle da quantidade de moedas existentes e do respectivo valor da mesma); o que poderia ser revisado depois conforme o sistema exigisse para não entrar em pane (por exemplo, por falta de espaço em disco rígido ou de velocidade em banda larga) e, depois, novamente aumentado conforme a capacidade dos equipamentos dos usuários. Também poderia ser implementado um sistema onde seria submetido à votação a queima (destruição) de alguns por centos da moeda; e, ainda, a possibilidade de o autor deletar sua obra que não agradou aos outros usuários, em troca de 10% de sua quantidade de bytes. O próprio sistema não venderia e nem compraria a moeda, mas tão somente os usuários é que a negociariam. Como o sistema faz e recebe pagamentos, por óbvio deve possuir uma conta própria, a qual também permite doações diretas ao sistema. Os pagamentos feitos pelos usuários são aprovados (manualmente e com justificativa) por 3 (três) julgadores enquanto que os feitos pelo sistema são aprovados por 10 (dez) julgadores e as decisões denegatórias são revisadas através de votação com exposição de razões do interessado e dos julgadores. Ideia semelhante poderia ser adaptada para a criação e compartilhamento de fotos e de vídeos; ou melhor, serem incorporados na referida biblioteca digital sugerida. Fica aqui, portanto, uma de nossas ideias de moeda digital; a **$¥₪@₱$€** em referência à sinapse dos neurônios, mas escrita com símbolos

de moedas com o símbolo de eletrônico bem no meio. Já seu símbolo seria ¤ (teclas Alt + 0164 e Unicode: U+00A4) por ser similar ao neurônio, lembrar conexões e, também, se tratar de uma representação genérica de unidade monetária. A Decente (https://decent.ch/) já faz algo muito semelhante a isso e poder-se-ia aproveitar seu código fonte. A Steem (https://steem.io/ e https://steemit.com/) também possui alguma similitude com o aqui proposto.

Urge fazer uma observação sobre as postagens nos fóruns correlatos (sobre bitcoin, altcoins, criptomoedas, criptografia, engenheiros e desenvolvedores de software, *hackers*, etc.). Elas devem ser, no mínimo, na língua inglesa; vez que a maioria das pessoas integrantes dessa comunidade sabe o inglês e quase nenhuma delas sabe o português brasileiro. Além do que, infelizmente, o Brasil e os brasileiros não gozam de boa reputação e de credibilidade.

Um exemplo é a **MXT - MarteXCoin** (https://martexcoin.org/), uma moeda digital brasileira que faz apenas a chamada inicial em inglês (deveria ser o site por completo com opções de outros idiomas) e comete o erro de estampar que é brasileira: "Somos uma criptomoeda brasileira, queremos elevar o Brasil no mercado das criptomoedas!". Outro exemplo, é a Fundação Ethereum, uma organização sem fins lucrativos registrada na Suíça (https://ethereum.org/foundation), mas que utiliza completamente o idioma inglês no seu site e não fica dando ênfase, enfoque, destaque ou notoriedade e nem fica exibindo ou ostentando que é suíça ou feita na suíça; apenas informa de forma sútil, discreta, sem nenhum alarde e quase imperceptível. Por outras palavras, não são dados destaques à nacionalidade, origem ou sede da moeda; muito menos são usados qualquer meio nacionalista, restritivo, regionalista, discriminatório ou xenofóbico. Algumas das especificações da MarteXCoin são: algoritmo X13; PoW / PoS com 50% anual; *Proof-of-Stake* com tempo mínimo de 2 horas; *Proof-of-Stake* com tempo máximo de 8 horas; tempo de bloco: 60 segundos; quantidade máxima: 5 milhões total de moedas com 2% pré minerado para promoções iniciais; dificuldade reiniciada a cada bloco; número de confirmações para Transações 3 e para mineração 5; e, taxa de transação 0.0001 MXT. *Exchanges*: chameleonbit.trade, coinexchange.io, yobit.net e bleutrade.com.

Pode ser comprada no próprio site institucional através do PagSeguro e do Paypal. Todo computador conectado na rede minerando ou com no mínimo 5 MXT se torna um *seed* (*node* ou nó) automaticamente, fazendo assim a rede fluir mais rapidamente. Qualquer computador com um poder de processamento médio e/ou uma placa gráfica (GPU) consegue produzir moedas.

- Faucet: http://martexcoin.org/faucet;
- Paperwallet: http://martexcoin.org/paperwallet;
- WalletOnline: http://wallet.martexcoin.org/;
- Block Explorer: http://be.martexcoin.org;
- Fórum: http://martexcoin.org/forum;
- Grupo do Telegram: https://telegram.me/martexcoin;
- Facebook: https://pt-br.facebook.com/martexcoin/;
- Twitter: https://twitter.com/martexcoin;
- Pool: http://bitcoinpool.us / http://www.zpool.ca;
- Cálculos de mineração: https://bitmakler.net/MarteXcoin mining;
- Anúncio no Fórum Oficial: http://martexcoin.org/forum/d/9-martexcoin-minera-o-hybrida-pow-pos-50-de-juros-anuais;
- Anúncio no Fórum BitcoinTalk: https://bitcointalk.org/index.php?topic=1354130.0;
- Anúncio no Fórum CryptoCoinTalk: https://cryptocointalk.com/topic/11210- ★ ★ ★ ★ ★ -mxt-martexcoin- ★★★★★ -website-martexcoinorg/;
- Wallet Windows: http://martexcoin.org/releases/martexcoin-qt_2.5.4.1.exe;
- Wallet Linux: http://martexcoin.org/releases/martexcoin-qt_2.5.4.1;
- Wallet Raspiberry: http://martexcoin.org/releases/raspi-mxt.tar;
- Source: https://github.com/martexcoin/martexcoin;
- Cotação: https://yobit.net/en/trade/MXT/BTC.

O ideal é tais postagens serem poliglotas (usarem mais de dois idiomas), estando divididas por frases ou parágrafos. Por outras palavras, cada trecho

estaria repetindo a mesma frase ou parágrafo nessas diferentes línguas. Sugere-se, no mínimo, os idiomas inglês norte-americano, espanhol e português brasileiro. Em complemento, pode-se escolher mais duas das seguintes línguas: mandarim (chinês), russo, árabe e até japonês. O critério utilizado para escolher esses idiomas foi uma combinação das línguas mais faladas pelo número de pessoas, pela quantidade de países e por países ricos e onde há aficionados por informática e tecnologia; em razão disso excluímos as línguas hindi e bengali. Por óbvio que não pode ser muitos idiomas e que os textos terão que ser muito bem elaborados para não usarem muitos caracteres, senão a postagem será imensa. Uma estratégia, portanto, é dividir as informações em tópicos, tais como, por exemplos, com uma introdução ou apresentação genérica ou superficial (dando origem ao tópico no fórum) e depois cada item é melhor explicado ou apresentado em postagens separadas. Sim é um trabalho sério e não uma brincadeira de adolescentes. Ao utilizar um padrão poliglota, além de facilitar o contato com a comunidade dos desenvolvedores, também dará uma conotação de universalidade. Por óbvio no final de cada postagem deve ter uma frase pedindo para revisarem os idiomas usados, bem como para traduzirem a mensagem para mais outros idiomas.

Outro detalhe é o idioma Esperanto; uma língua artificial adotada de forma secundária ou auxiliar em mais de 120 países.

- https://pt.wikipedia.org/wiki/Esperanto;
- http://esperanto.org.br/info/;
- http://www.kurso.com.br/index.php?pt;
- http://easp.org.br/portal/.

Como discorremos exaustivamente, uma moeda virtual só vale dinheiro se alguém acreditar na sua legitimidade. E dificilmente as pessoas irão acreditar ou confiar numa moeda desconhecida que surgiu repentinamente do nada por uma única pessoa ou por um estranho; pior ainda se malfeita. Mas, possivelmente, irão dar crédito numa moeda que teve todo um trabalho prévio de pesquisa, consulta, estudos, comparações, debates, críticas, testes e, enfim, ampla participação democrática, pública e universal. Enfim, quanto

mais rápida e fácil a criação de uma moeda virtual, mais célere é a sua morte.

E para que uma moeda virtual dure, é preciso que o time de desenvolvedores esteja comprometido em corrigir falhas, analisar críticas e sugestões, e manter a segurança e o aprimoramento da moeda.

Conforme visto alhures, além de criar do nada ou do zero uma criptomoeda, é possível utilizar-se do procedimento de *fork* (bifurcação) de uma já existente e em uso; bem como simplesmente aproveitar os vários códigos fontes (*source codes*) do Bitcoin e das altcoins existentes para poder agilizar o procedimento. E, por fim, para quem não saiba fazer ou não queira ter o trabalho de fazer, existe a opção de contratar alguém ou alguma empresa para tal finalidade.

As plataformas Ethereum (https://www.ethereum.org/token) e NXT (https://nxt.org/what-is-nxt/monetary-system/) possuem o recurso de criar uma nova criptomoeda.

- https://blog.ethereum.org/2015/12/03/how-to-build-your-own-cryptocurrency/;
- https://cryptojunction.com/how-to-create-your-own-cryptocurrency/.

Sites como CryptoCoinCreator (https://www.cryptocoincreator.com/), CryptoNoteStarter (https://cryptonotestarter.org/), CryptoGen (http://www.cryptogen.org/), CryptoLife (https://dev.cryptolife.net/) e Bitclone (https://www.bitclone.net/), permitem a qualquer pessoa criar uma moeda digital.

- http://www.yourownbrokerage.com/solutions/consulting-solutions/create-coin-like-bitcoin/.

Desse modo, existem formas de construir a própria criptomoeda sem tocar em nenhuma linha de código sequer. No caso do serviço do Ethereum, por exemplo, a primeira coisa a fazer é criar uma conta Ethereum (https://www.ethereum.org/); que é feita através do software da Carteira Ethereum (*Ethereum Wallet*), clicando-se em "ADD ACCOUNT". A segunda coisa, é adquirir alguns éteres; seja comprando ou minerando. O software

mineiro AlethOne (https://github.com/ethereum/webthree-umbrella/releases) é uma ferramenta simples com dois botões: um para iniciar a mineração (*start mining*) via GPU e o outro ícone para depositar as recompensas em uma carteira. Sugere-se o *download* do Turbo Suíte (https://github.com/ethereum/webthree-umbrella/releases); um conjunto de ferramentas para desenvolver aplicações ethereum. Tokens no ecossistema Ethereum podem representar qualquer bem fungível negociáveis: moedas, pontos de fidelidade, certificados de ouro, IOUs, em itens de jogo, etc. (https://www.ethereum.org/token). Através do software da Carteira Ethereum (Ethereum Wallet), na aba “CONTRACTS”, clica-se em “DEPLOY NEW CONTRACT” ("implantar novo contrato"). Desse modo, através da rede Ethereum comprar-se-á um contrato inteligente consistente em um símbolo. Assim, obter-se-á o *token code* (código de token: https://ethereum.github.io/browser-solidity/), qual será copiado e colado no campo “Solidity source field” ("fonte de solidez"). Se o código for compilado sem qualquer erro, aparecerá a frase: “pick a contract” (escolher um contrato) no menu suspenso à esquerda. Seleciona-se o contrato "MyToken". Na coluna da direita, constarão os parâmetros de personalização do token; os quais devem ser ajustados conforme o gosto do freguês: quantidade de unidades, nome, símbolo e quantidade de casas decimais. No final da página constará uma estimativa do custo computacional do referido contrato e o cliente pode selecionar uma taxa de quanto éter está disposto a pagar por isso. Qualquer excesso de éter será devolvido ao cliente. Pressiona-se “deploy” (implantar), digita-se a senha (*password*) da conta e aguarda-se alguns segundos para que a transação seja processada. Será feito um redirecionamento de página, onde pode-se ver a transação à espera de confirmações. Clica-se na conta denominada "Etherbase" (“your main account” ou a sua conta principal) e depois de cerca de um minuto, pode-se ver que na conta vai mostrar a existência de 100% das ações recém-criadas. Para enviar aos outros, basta selecionar "enviar" (*send*) e depois escolher a moeda que quer enviar (éter ou uma quota da recém-criada), fornecer o endereço do favorecido no campo "para" (“to”) e pressionar “send” ("enviar"). Os destinatários ou beneficiários ainda não conseguirão visualizar nada nas carteiras deles porque a carteira só controla os tokens que ela conhece. Desse modo, deve-se adicionar manualmente essa nova moeda. Na aba "Contratos" deve constar um link para o contrato recém-criado; clicasse nele para ir para a sua página, onde

se clica em “copy address” ("endereço de cópia") e cola-se o endereço do contrato (“contract address”) com um editor de texto. Para adicionar um token para visualização, acessa-se a página de contratos e, em seguida, clica-se em “Watch Token” (Visualizar token). Uma janela *pop-up* aparecerá e será precisa colar o endereço do contrato. O nome do símbolo, símbolo e número decimal devem ser preenchidos automaticamente. Depois de fazer isso, a nova moeda será automaticamente mostrada e processada pela carteira.

Ao pesquisar na Internet pela expressão "Make your Own cryptocurrency", “Create your own crypto-currency” ou “Create your own digital coin”, encontrar-se-á tutoriais de como criar a própria moeda virtual.

Os **detalhes essenciais da criação de uma altcoin**, mesmo que seja uma mera bifurcação ou um clone de outra moeda digital já existente, são "Name of your Coin" (nome da moeda), "Coin abbreviation" (abreviatura ou sigla da moeda), "Port Number" (número de porta; ou seja, um elo de ligação entre o software e a conexão com a rede), "Block Time" (tempo do bloco; duração das transações em minutos), "Block Reward" (recompensa por bloco; quantidade por bloco minado), "Genesis Timestamp" (carimbo de data e hora do primeiro bloco), "Address Prefix" (prefixo de endereço) e "Maximum Money" (quantidade máxima de unidades a serem emitidas).

O **nome** e o símbolo devem ser muito bem pensados e conferidos para não dar a impressão de ser mera brincadeira, zoação, coisa de adolescentes, regionalismo, exclusivismo, seletismo, grupo fechado, sociedade secreta, fanatismo, extremismo e, muito menos, ser algo ridículo, imbecil, ofensivo, indecoroso, inapropriado, escandaloso, depreciativo ou desagradável. Uma palavra em um idioma pode significar algo totalmente diferente em outra língua. Muitas vezes uma sigla acidental pode ser uma palavra em outro idioma ou coincidir com uma sigla de alguma entidade ou instituição. Imagine usar ingenuamente a sigla “KKK” sem saber que significa *Ku Klux Klan*. No Brasil o símbolo de “OK” feito com a mão significa um palavrão. Na Itália o símbolo de *heavy metal* significa chamar a pessoa de corna. Outro exemplo do que não fazer, é a empresa asiática “Bosta”.

- http://bosta.com/;

- http://www.bosta.org/;
- http://www.bostahouston.com/;
- http://www.bosta.co.uk/;
- http://en.bosta.cn/about/&i=2&comContentId=2.html.

O WordSafety (http://wordsafety.com/) é uma ferramenta de verificação para comprovar em uma base de dados de 19 idiomas, se o nome escolhido possui significados impróprios em algum país.

- http://noticias.uol.com.br/tabloide/ultimas-noticias/tabloideanas/2014/03/03/papa-francisco-se-confunde-e-fala-palavrao-durante-bencao-dominical.htm.

Uma sugestão de nome é o **spesmilo (símbolo: □)**, que foi a moeda internacional do idioma internacional Esperanto. O spesmilo foi proposto em 1907 por René de Saussure e utilizado antes da Primeira Guerra Mundial por alguns bancos britânicos e suíços, principalmente o esperantista Cekbanko. Também podem ser usados os nomes de antigas moedas universais da antiguidade, tais como, por exemplos: thaler ou táler, denarius ou denário, moneta, dracma e estáter. Detalhe, já foram lançadas moedas digitais com os nomes BitDrachma (DRA), DRACHMacoin (DRAC) e eTaler (TALER); resta saber se ainda estão em atividade.

Para ser mais fácil a escolha e uso de um **símbolo**, pode-se usar a lista de caracteres unicode (*unicode characters*: http://unicode-table.com/en/#control-character) existente no Microsoft Word através da função inserir símbolo. Detalhe, cada símbolo possui um código para facilitar sua localização. Também existe a Tabela ASCII - *American Standard Code for Information Interchange* (Código Padrão Americano para o Intercâmbio de Informação) que se utiliza da tecla ALT pressionada com a digitação de alguns números (https://pt.wikipedia.org/wiki/ASCII).

Criar uma criptomoeda é um projeto de engenharia de software que exige conhecimentos em programação e criptografia e não simplesmente saber informática ou usar um computador. É necessário ter alguns conhecimentos básicos de programação ou compilação em linguagem de programação C, C++, Java, Python, Perl, etc. O Bitcoin e o Litecoin, por exemplos, foram

escritos em linguagem C; já o Ethereum foi escrito em Golang. Não há necessidade de ser um especialista, mas deve-se ter uma boa noção e saber entender os erros básicos de compilação e como corrigi-los.

- https://www.visualstudio.com/;

Clonagem, bifurcação ou uma inédita? Qual moeda de base (código fonte) usar ou não se basear em nenhuma? Qual linguagem de programação usar? Qual algoritmo de criptografia usar: SHA-256, scrypt, X11, híbrida, outra existente ou inventar uma? Qual método de consenso utilizar? Usar a *blockchain* alheia (do Bitcoin, NXT, etc.) ou ter a própria *blockchain*?

Quais serão os atrativos, diferenciais, vantagens e benefícios que a nova moeda trará? A nova moeda proporcionará maior comodidade, novas emoções ou a capacidade de lucrar sem muito investimento?

O grande problema de **criar uma *blockchain* própria** é a rede (nós ou computadores) para a manterem funcionando. Por outras palavras, ao utilizar a *blockchain* de alguma criptomoeda com uma boa quantidade de adeptos, já se tem uma rede pronta, operante e estável. Uma *blockchain* própria exige uma preparação para o lançamento para que já se inicie com uma quantidade considerável de adeptos para mantê-la em atividade.

- http://www.oqueeblockchain.com.br/como-implementar-uma-blockchain/.

A Stratis (https://stratisplatform.com/) é uma plataforma de desenvolvimento *blockchain*.

As mais famosas *blockchains* de código aberto são Bitcoin Blockchain (https://github.com/bitcoin/bitcoin) e HyperLedger Blockchain (https://www.hyperledger.org/). Outras opções são:

- https://monax.io/;
- https://github.com/HydraChain/hydrachain;
- http://www.multichain.com/;
- https://www.openchain.org/;

- https://github.com/ElementsProject/elementsproject.org;
- https://www.walletbuilders.com/.

É essencial pensar no **logotipo da moeda**.

- http://www.tecmundo.com.br/imagem/806-gimp-criando-moedas.htm.

Será preciso, ainda, definir qual será a recompensa pelo bloco gerado (*block reward*) e escolher se os mineiros usarão "prova de trabalho" (*proof of work*), "prova de estaca" (*proof of stake*), outro tipo de prova ou criar um novo tipo de prova. Também devem ser definidas qual será a quantidade de dados permitida em cada transação; o tamanho do bloco; a quantidade máxima de emissão de moedas; a existência, ou não, de taxa de transação, seu respectivo valor e qual será o destino dessa taxa (ao mineiro que validou a transação, dividida a todos os mineiros, dividida a todos os membros da rede, revertida a alguma causa ou fundo, doação à alguma instituição, destruição, etc.); o grau de dificuldade e como este vai mudar ao longo do tempo para controlar a velocidade a que as novas moedas são emitidas; como as primeiras unidades da moeda serão geradas e distribuídas; como será a mineração; e assim por diante.

É extremamente recomendável somente iniciar o sistema assim que existir uma quantidade considerável de nós completos e de mineiros para dar alguma estabilidade, robustez, confiabilidade e segurança.

Se o leitor não está entendendo nada do que foi dito logo acima, provavelmente não leu os capítulos anteriores.

Se o desenvolvedor do projeto deseja ter controle total sobre o código fonte e respectivos software e sistema pelos quais a criptomoeda funcionará, bem como possuir a capacidade ilimitada para definir todos os seus parâmetros, então deverá projetar do zero, inclusive, com sua própria *blockchain*. Em https://bitcointalk.org/ pode-se contratar um *freelancer* (profissional autônomo) para este tipo de trabalho.

Deste modo, para quem não possui nenhuma aptidão para entender disso tudo ou, se tiver mesmo preguiça, é possível contratar os serviços de algum

profissional ou de alguma empresa como, por exemplos:

- https://www.bitclone.net/;
- https://cryptonotestarter.org/;
- http://www.cryptocoincreator.com/create.php;
- https://www.ethereum.org/token;
- https://dev.cryptolife.net/;
- http://www.coincreator.net/.

Portanto, é bem mais fácil aproveitar o que já existe. Assim, basta escolher uma criptomoeda *open source* como base, localizar no GitHub (https://github.com/) ou outro repositório, fazer o download e forjar o *fork* ou o clone.

- https://github.com/bfroemel/smallchange/commit/947a0fafd8d033f6f0960c4ff0748f76a3d58326.

Depois muda-se o código fonte trocando o nome da moeda, ícones e siglas. Também se deve mudar a versão do *address* (endereço) e o *magic number* (número mágico) da *blockchain*. Alterar as portas de conexão protocol.h, init.cpp, rpc, bitcoinrpc.cpp e init.cpp. Depois se define e altera os parâmetros em main.cpp (tempo entre blocos, etc.) e, por fim, cria-se o bloco genesis.

- Exemplo de clonagem do Litecoin - https://vcoin-project.github.io/cloning-litecoin/.

MSYS é uma coleção de utilitários GNU, que permite a construção de aplicações e programas que dependem tradicionalmente ferramentas UNIX para estar presente. Destina-se a complementar MinGW e as deficiências do shell cmd. MSYS por si só não contém um compilador ou uma biblioteca C.

- https://sourceforge.net/projects/mingw/files/Installer/mingw-get-setup.exe/download;
- https://sourceforge.net/projects/mingw/?source=typ_redirect.

Infra uma relação de orientações e recursos pertinentes:

- https://bitcointalk.org/index.php?topic=149479.0;
- https://bitcointa.lk/threads/ann-easywinbuilder-the-easy-way-to-build-bitcoin-on-windows.148836/;
- https://bitcointa.lk/threads/complete-guide-on-how-to-create-a-new-alt-coin.134252/;
- https://github.com/MaxGuevara/quark/blob/master/doc/gitian-building.md;
- https://www.youtube.com/watch?v=86jqAfySi64;
- https://github.com/iquidus/explorer/blob/master/README.md;
- https://github.com/zone117x/node-open-mining-portal;
- http://blockgen.net/setup-your-own-mining-pool/;
- https://bitcointa.lk/threads/pedido-tutorial-completo-de-criacao-de-moedas.589934/page-2;
- https://cryptojunction.com/how-to-create-your-own-cryptocurrency/;
- https://altcoinsfoundation.com/forum/developers/56-how-to-create-your-own-cryptocurrency-altcoin-1-dev;
- https://pt.scribd.com/document/155418578/Create-Your-Own-Currency.

É recomendável, ainda, colocar a descrição e detalhes da moeda nas wikis e enciclopédias on-lines (exemplos: https://pt.wiktionary.org/ e https://pt.wikipedia.org/) em diferentes idiomas.

Depois de desenvolver a moeda virtual será preciso criar um site (recomenda-se indexá-lo nos sites de buscas) e páginas institucionais (cada uma com um idioma diferente e constando estar localizada no respectivo país do idioma) nas redes sociais para as pessoas poderem encontrar informações, tutoriais e fazerem o download dos programas; bem como

divulgar (fazer anúncios e propagandas) sobre a moeda para que as pessoas comecem a minerá-la. Assim, com alguma sorte, ela pode acabar conquistando usuários, formando uma comunidade de adeptos e ganhando valor no mercado. Uma boa forma de começar, e já é metade do caminho, envolve construir confiança, expressar a visão e intenções à comunidade de criptomoedas e cativá-los. Depois de criada a moeda, deve-se trazer mineradores e ter usuários com ela na carteira. Em seguida, é necessário convencer comerciantes a aceitá-la como forma de pagamento; e, principalmente, uma *exchange* a negociá-la. Depois conseguir criar um ecossistema em torno dessa moeda digital (empresas, serviços e produtos relacionados) e, por fim, conseguir ter e manter um grupo de desenvolvedores para manterem o sistema operante e em constante aperfeiçoamento.

Saiba mais no capítulo seguinte.

CONSIDERAÇÕES SOBRE *START-UP* OU PROJETO DE *SOFTWARE*

Não é recomendável fazer um projeto em código aberto sem estar resguardado como criador ou respaldado por uma licença; vez que qualquer pessoa pode pegá-lo e dizer que foi ela quem fez ou registrá-lo como sendo dela. Desse modo, é necessário tornar público ou, até mesmo, provar a autoria ou a propriedade sobre o mesmo. Portanto, quem deseja desenvolver algum *software*, seja livre ou não, deve primeiramente garantir os direitos sobre o mesmo. Por outras palavras, não só a autoria ou a criação, mas que não o desenvolveu a serviço de outrem.

Nos Estados Unidos, o registro de direitos autorais (http://www.copyright.gov/) exige que tenha sido feita a prévia divulgação (publicado anteriormente); o que pode ainda ser considerado um requisito ético na academia. Desse modo, a primeira medida é dar ampla publicidade com crédito de autoria e registro de data; ou seja, publicando em algum periódico ou site dedicado ao ramo ou atividade. Cita-se, por exemplo, publicar um anúncio ou divulgação (ANN - *announcement*) do lançamento (*launch*) com a correlata hospedagem do código fonte no GitHub (https://github.com/).

O **GitHub** é uma rede social para programadores e desenvolvedores criada com o objetivo de compartilhar códigos, programas e *plug-ins*; bem como permitir o acesso online e simultâneo de múltiplos desenvolvedores trabalhando simultaneamente no mesmo projeto. O GitHub funciona a partir de repositórios, que funcionam como pastas criadas para armazenar os arquivos disponibilizados para o download. Dentro destas pastas, pode-se criar novas pastas, contendo vários tipos de arquivos: html, css, JavaScript, documentos de texto, php, PDF, imagens, gráficos, json, markdown, etc. Na versão gratuita do GitHub todos os repositórios serão públicos e acessíveis a qualquer pessoa. O GitHub, ainda, permite hospedar websites inteiros gratuitamente, mas somente estáticos e construídos em linguagem (html, css e js) de navegadores (*web browsers*) e não de servidores. Não são permitidos arquivos em php e nem o uso de base de dados (por exemplo, MySQL). Pode-se utilizar o subdomínio do GitHub (nome-do-usuario.github.io) ou um domínio próprio (suaempresa.com).

Existem outros sites alternativos ao GitHub:

- https://bitbucket.org;
- https://git-scm.com;
- https://netbeans.org;
- https://www.codeplex.com;
- https://www.codebasehq.com;
- https://www.assembla.com;
- https://codeplane.com.br;
- https://www.visualstudio.com/pt-br;
- http://www.whitesourcesoftware.com.

O Nubera (http://nubera.com) é um ecossistema de plataformas de aplicativos de negócios e de descoberta de software. Sua missão é aconselhar profissionais para ajudá-los a encontrar o software e aplicações que melhor atender às suas necessidades. O site Getapp (https://www.getapp.com) é da Nubera.

SourceForge (https://sourceforge.net) é uma comunidade *Open Source* dedicada a ajudar projetos de fonte aberta a serem bem-sucedidos.

Geeklist (https://geekli.st) é uma plataforma social para desenvolvedores descobrirem e conectarem-se a outros desenvolvedores e compartilharem seus trabalhos.

O Stack Overflow (http://pt.stackoverflow.com) dispõe de perguntas e respostas sobre uma ampla gama de tópicos de programação de computadores. Stack Overflow serve como uma plataforma para os usuários fazerem perguntas e responderem-nas e, por meio da associação e participação ativa, os membros podem dar votos de *up* (subir, *like* ou curtir) e *down* (abaixo ou não curtiu) nas perguntas e respostas e editá-las de forma similar a uma wiki.

Google Developers (https://developers.google.com/?hl=pt) é o site do Google para ferramentas de desenvolvimento de software, interfaces de programação de aplicativos (APIs), e recursos técnicos. O site contém a documentação sobre o uso de ferramentas para desenvolvedores do Google além de grupos de discussão e blogs para desenvolvedores que usam produtos de desenvolvedor do Google. Já a IBM tem o developerWorks (http://www.ibm.com/developerworks).

DEVX (http://www.devx.com) é um gigantesco portal sobre os tópicos de programação mais populares, tais como Java, C++, programação de banco de dados, Visual Basic, programação em dispositivos móveis, etc.

Planet Source Code (http://www.planet-source-code.com) possui uma enorme biblioteca de exemplos de código muito úteis. O site abrange a maioria das principais línguas.

No Workana (http://contrata.workana.com) a pessoa publica o projeto de software e os programadores *freelance* (profissionais autônomos) enviam propostas; depois basta escolher a proposta que melhor se adapta à necessidade. O Toptal (https://www.toptal.com) é uma rede exclusiva dos principais desenvolvedores de software *freelance* e *designers* do mundo. Também existe o site https://www.br.freelancer.com/find/software-developers.

Entretanto, a maneira mais garantida de proteger os direitos sobre o software, é através de um registro oficial. No Brasil esse registro é feito junto ao INPI - Instituto Nacional da Propriedade Industrial (http://www.inpi.gov.br):

- http://www.inpi.gov.br/menu-servicos/programa-de-computador;
- http://www.inpi.gov.br/menu-servicos/programa-de-computador/legislacao-programa-de-computador;
- http://www.inpi.gov.br/menu-servicos/programa-de-computador/documentacao-tecnica-para-registro-de-programa-de-computador;
- http://www.inpi.gov.br/menu-servicos/programa-de-computador/documentacao-formal-para-registro-de-programa-de-computador.

O reconhecimento do registro de programa de computador é internacional. Assim, programas nacionais não precisam ser registrados nos demais países, desde que haja o registro no INPI. Trata-se do acordo TRIPs (*Trade Related Intellectual Property Rights*). O PCT - *Patent Cooperation Treaty* (Tratado de Cooperação de Patentes) é um acordo internacional administrado pela OMC - Organização Mundial do Comércio ou *World Trade Organization* (https://www.wto.org) que define as normas mínimas para muitas formas de propriedade intelectual.

- https://www.wto.org/english/tratop_e/trips_e/trips_e.htm;
- https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.

Mas se o criador quiser registrar no exterior, infra alguns links sobre o registro nos Estados Unidos e na Europa:

- https://www.uspto.gov/;
- https://euipo.europa.eu/;
- http://www.epo.org/;
- http://www.marcasepatentes.pt/;
- https://www.tmdn.org/;
- http://europa.eu/youreurope/business/start-grow/intellectual-property-rights/index_pt.htm#.

O regime jurídico para a proteção aos programas de computador no Brasil é disciplinado pela Lei de Software (Lei n.º 9.609/1998) e, subsidiariamente, pela Lei de Direito Autoral (Lei n.º 9.610/1998). Desse modo, os direitos autorais incidem sobre o software, assim como incidem sobre as obras literárias.

- Lei 9.609/1998: http://www.planalto.gov.br/ccivil_03/leis/L9609.htm;
- Decreto 2.556/1998: http://www.planalto.gov.br/ccivil_03/decreto/d2556.htm;
- Lei 9.610/1998: https://www.planalto.gov.br/ccivil_03/leis/L9610.htm;
- Decreto 8.469/2015: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8469.htm;

- Demais normas: http://www.inpi.gov.br/menu-servicos/programa-de-computador/legislacao-programa-de-computador.

Em Portugal existe o Código de Direito de Autor e Direitos Conexos (Decreto-Lei nº 63/1985):

- http://www.wipo.int/wipolex/en/text.jsp?file_id=199767;
- https://ciist.ist.utl.pt/docs_da/codigo_direito_autor_republicado.pdf;
- http://www.erc.pt/pt/direito-de-autor-e-direitos-conexos;
- https://www.parlamento.pt/Legislacao/Paginas/Cultura_DireitoAutor_CodigoDireitoAutorDireitosConexos.aspx.

Ressalta-se que registrar um programa de computador (software) é algo distinto do registro de marcas e patentes. Desse modo, em regra, a proteção ao nome comercial do software somente pode ser obtida através das providências relativas ao respectivo registro.

Marca é a representação de uma entidade, tal como um ícone é para um software dentro de um sistema operacional ou como o nome e a fisionomia (aparência física) é para uma pessoa física. Desse modo, é uma forma de prontamente (de imediato) identificar uma empresa, um produto ou um serviço. A marca, portanto, é uma identificação distintiva e exclusiva, seja através de um nome, uma palavra, um símbolo, um sinal, um emblema, uma insígnia, um brasão, um logotipo, etc.

- http://www.inpi.gov.br/servicos/perguntas-frequentes-paginas-internas/perguntas-frequentes-marca;
- http://www.inpi.gov.br/menu-servicos/marcas;
- http://www.inpi.gov.br/menu-servicos/marcas/e-marcas.

Inobstante isso, recomenda-se informar dito nome comercial como sendo o título do programa no ato da apresentação do pedido de registro do software. Por óbvio que este nome deve ser original e inconfundível com o de outro software já existente.

O termo **patente**, por sua vez, versa sobre os direitos exclusivos que o Estado concede ao inventor, por um certo período de tempo, para a divulgação, a fabricação, a exploração, a distribuição e a alienação da sua invenção ou modelo de utilidade. Desse modo, quem quiser fazer qualquer uma dessas coisas, necessita de autorização do titular (proprietário) da referida patente. Deste modo, enquanto a marca é registrada, a invenção é patenteada.

Frisa-se que o autor do software é quem o produziu por si mesmo ou por conta própria; ou seja, aquele que não o fez como contratado ou funcionário de outrem, pois se o fez em nome alheio, os direitos e a respectiva propriedade é do contratante. E o proprietário possui suprema autoridade sobre seu produto.

Cabe ao criador (proprietário ou detentor dos direitos), ao licenciar o seu uso, estipular o regime de exercício dos direitos, bem como dos limites e da forma de utilização de sua obra, produto e/ou serviço pelos licenciados. Portanto, a licença de software especifica os direitos e as restrições sobre o uso do respectivo programa de computador. Por outras palavras, a razão da licença é especificar a liberdade que o utilizador possui sobre o software. Por outras palavras, deve-se explicitar se outras pessoas possuirão direito de usá-lo, copiá-lo, transferi-lo, estudá-lo, vende-lo, modificá-lo e/ou redistribuí-lo.

A maioria dos softwares comerciais são distribuídos segundo termos e condições de uso bastante restritivos, tais como, por exemplo, não inclusão do código fonte do software.

Código fonte é o conjunto de instruções que formam o programa de computador, tal como o DNA é para os seres orgânicos ou biológicos. Esses comandos são primeiramente escritos num código compreensível por humanos, que depois são transformados em linguagem de máquina para que o computador possa efetivamente seguir as referidas instruções. Isto faz com que se torne bastante difícil, senão impossível, para outras pessoas conseguirem modificar ou adaptar o software à medida das suas necessidades. Uma pessoa com conhecimentos adequados, ao ter acesso ao

código fonte, pode estudá-lo ou, até mesmo, alterá-lo conforme sua necessidade ou interesse.

Em oposição ao modelo proprietário de "software fechado", existem os projetos colaborativos que dão origem aos softwares de licenças livres e abertas (FOSS - *Free and Open Source Software*).

- http://www.fsf.org/;
- http://www.freeopensourcesoftware.org/.

Todas as licenças aprovadas pela OSI - *Open Source Initiative* (https://opensource.org/) permite a redistribuição do código fonte. A maioria dessas licenças permitem a modificação do código fonte sem qualquer notificação. Algumas licenças liberam todos os direitos e permitem que qualquer pessoa pode fazer qualquer coisa com o código fonte, desde que faça a atribuição dos créditos do criador.

A maioria das licenças de código aberto absolvem (exoneram ou isentam) os autores do projeto de qualquer responsabilidade se alguém usar o código e ele causar algum dano.

Recorda-se que um software *freeware* (programa meramente gratuito) é aquele que pode ser usado sem pagar nada. Entretanto, um programa de computador gratuito pode ser livre ou fechado (restrito); ou seja, somente o autor ou a entidade desenvolvedora tem acesso ao código fonte. Por outras palavras, apesar de gratuito, somente pode ser utilizado da forma como foi disponibilizado. Muitas vezes, ainda, há limitações quanto à sua distribuição. Já um software livre, não significa necessariamente que seja gratuito, mas sim que o código fonte é acessível e passível de alterações e redistribuição. Em síntese, um software livre pode ser comercializado.

Ressalta-se, assim, que o software livre é uma questão de liberdade (similar à "liberdade de expressão"), mas não necessariamente de preço (no sentido de "almoço grátis"; vez que a GNU-GPL não coloca quaisquer entraves à comercialização de software livre. Pertinente, pois, o famoso ditado (brocardo) norte americano "There is no free lunch" (não existe almoço grátis).

Embora os termos "código aberto" (*open source*) e "software livre" (*free software*) sejam usados como sinônimos, eles não querem dizer exatamente a mesma coisa: o código é aberto quando a pessoa que recebe o binário (se existir algum), também tem o direito de receber o código fonte. Entretanto, o que a pessoa pode fazer com o código fonte, varia de licença para licença.

Apesar de que o conceito de software livre é sujeito a interpretações, em geral ele é considerado como sendo um programa de computador no qual o usuário tem direito de estudá-lo e modificá-lo (o que implica na necessidade do recebimento do código fonte) e redistribuí-lo para quem quiser, tudo sem a necessidade de permissão prévia ou adicional do autor e/ou de pagamento de ***royalties*** (quantia paga ao proprietário pelo direito de usar, produzir, explorar, distribuir ou comercializar). Entretanto, algumas modalidades de licenciamento (***copyleft***) exigem que qualquer obra derivada (modificações feitas no código fonte original do programa ou outros programas que foram incluídos para interagirem com o original), seja licenciada da mesma forma, ou de modo bastante similar, ao original. Já outras licenças (***copyfree***), não impõem essa restrição.

Em março de 2000, a FSF (*Free Software Foundation*) lançou a primeira versão da GNU FDL (*Free Documentation License* ou Licença de Documentação Livre). Esta licença destina-se aos programadores de software que pretendem elaborar manuais e redigir documentação sobre os seus programas. Contudo, também pode ser usada com outros tipos de textos. Tal como a GPL, a FDL também é uma licença *copyleft* no sentido viral na medida em que:

- Permite que qualquer pessoa copie e redistribua os textos disponibilizados segundo a licença, com ou sem modificações, tanto para fins comerciais e não comerciais;

- Obriga que as cópias e obras derivadas com tiragem superior a 100 sejam acompanhadas do documento ou código-fonte original;

- Obriga a que as obras derivadas sejam distribuídas de acordo com a mesma licença;

- Proíbe os editores de incluírem medidas de proteção tecnológica como DRMs (*Digital Rights Management* ou GDD - Gestão de Direitos Digitais) para controlar ou impedir a distribuição ou edição do documento.

O *copyleft* funciona como um termo adicional a uma licença. Por exemplo, uma licença livre visa garantir a quem receba uma cópia da obra licenciada às seguintes liberdades:

1) A liberdade para usar o trabalho;

2) A liberdade para estudar o trabalho;

3) A liberdade para copiar e compartilhar o trabalho com os outros;

4) A liberdade para modificar o trabalho e também para distribuir os trabalhos modificados e derivados.

Porém essas liberdades por si sós não garantem que um redistribuidor ou autor de trabalho derivado da obra livre irá distribuí-lo com as mesmas liberdades. Para que haja esse requisito e a licença seja considerada *copyleft*, requer-se um termo adicional que garanta que o autor do trabalho derivado só possa distribuí-lo sob a mesma licença ou sob uma que seja equivalente. Desse modo, as licenças copyleft também criam impedimentos, tais como, por exemplos, que os direitos sobre o trabalho não podem ser revogados e que o trabalho, e suas derivações, devem ser fornecidos de forma que facilite modificações futuras. No caso dos softwares, é necessário que o código fonte do software derivado seja fornecido junto com ele.

O *copyleft* denomina genericamente uma ampla variedade de licenças que permitem, de diferentes modos, liberdades em relação a uma obra intelectual. Seu nome se origina do trocadilho com o termo "copyright"; literalmente, *copyleft* pode ser traduzido como "esquerda da cópia" ou "permitida a cópia".

Copyleft ou livre direito de cópia é uma forma de usar a legislação de proteção dos direitos autorais com o objetivo de retirar barreiras à utilização, difusão e modificação de uma obra criativa devido à aplicação clássica das normas de propriedade intelectual (*intellectual property*), exigindo que as mesmas liberdades sejam preservadas em versões modificadas. Por outras palavras, uma obra, seja de software ou outros trabalhos livres, sob licença *copyleft* requer que suas modificações, ou extensões, sejam livres, passando adiante a liberdade de copiar e modificar novamente. *Copyleft* difere do domínio público, que não apresenta tais exigências; enquanto o domínio público permite qualquer utilização de uma obra, o *copyleft*, tem, via de regra, a única exigência de se poder copiar e distribuir uma obra. O *copyleft* também não proíbe a venda da obra pelo autor, mas implica a liberdade de qualquer pessoa fazer a distribuição não comercial da obra.

Uma das razões mais fortes para os autores e criadores aplicarem *copyleft* a seus trabalhos é por esperarem criar as condições mais favoráveis para que mais pessoas se sintam livres para contribuir com melhoramentos e alterações a essa obra, num processo continuado.

O *copyleft* pode ser considerado forte (*strong copyleft*) se todos os tipos de derivações do trabalho sob a licença *copyleft* tenham que estar sob essa licença *copyleft* também. No caso dele ser fraco (*weak copyleft*), a derivação não necessariamente precisará estar sob a mesma licença, dependendo do tipo de trabalho derivado. O *copyleft* fraco geralmente é aplicado em projetos de criação de bibliotecas de softwares. Quando é criado um outro software que apenas linka a essa biblioteca para utilizar seus recursos disponíveis, esse novo software não precisa herdar a licença *copyleft* da biblioteca, ele pode ser distribuído sobre outra licença qualquer. Apenas as mudanças feitas às bibliotecas em questão estariam sujeitas ao licenciamento *copyleft* na sua distribuição, as mudanças feitas em softwares que linkam a elas não estão sujeitas a essa obrigação. A diferença entre *copyleft* completo (*copyleft complete*) e *copyleft* parcial (*copyleft partial*) se refere a uma outra questão: o *copyleft* completo é aquele em que todas as partes de um trabalho (exceto a licença em si) podem ser modificadas por autores secundários. O *copyleft* parcial exime algumas partes do trabalho

das obrigações do *copyleft* ou de alguma forma não impõe todos os princípios do *copyleft*.

O compartilhamento pela mesma licença (*share-alike*) obriga que qualquer obra derivada seja distribuída com a mesma licença do trabalho original. Assim, qualquer licença *copyleft* é automaticamente uma licença de compartilhamento pela mesma licença.

- *Copyleft* – Manual de Uso: https://copyleftmanual.wordpress.com/.

No Brasil há algumas comunidades que lidam bastante com o tema e sua aplicação, como por exemplos:

- http://softwarelivre.org/;
- http://www.creativecommons.org.br/;
- http://br-linux.org/;
- http://www.eletronicbrasil.com.br/;
- http://www.culturabrasil.pro.br/;
- http://www.culturalivre.org.br/;
- http://baixacultura.org/;
- http://copyleftmanual.wordpress.com/.

A *permissive software license* (licença permissiva de software), às vezes também chamado BSD-like ou BSD licença, é uma licença de software livre com requisitos mínimos sobre como o software pode ser redistribuído. A *Open Source Initiative* define uma licença permissiva como um "não-licença copyleft".

O Noosfero (http://noosfero.org/) é uma plataforma web para redes sociais que possui as funcionalidades de Blog, e-Portfolios, RSS, discussão temática e agenda de eventos num mesmo sistema. Confira o manual online do Noosfero em http://softwarelivre.org/doc.

O Projeto Software Livre Brasil (http://softwarelivre.org/) é uma rede de pessoas, mantida pela Associação Software Livre.Org (http://softwarelivre.org/), que reúne universidades, empresários, poder público, grupos de usuários, *hackers*, ONG's (Organizações Não Governamentais) e ativistas pela liberdade do conhecimento. Possui como objetivo a promoção do uso e do desenvolvimento do software livre como uma alternativa de liberdade econômica, tecnológica e de expressão (http://softwarelivre.org/asl/documentos/estatuto).

A OSD - *Open Source Definition* (https://opensource.org/), definiu um conjunto de 10 de requisitos necessários para que uma licença de software seja designada *open source* (https://opensource.org/osd-annotated). Entre os princípios definidos na OSD encontram-se a livre distribuição do código fonte, a possibilidade de criar obras derivadas, o respeito pela integridade do código-fonte do autor e a não discriminação de pessoas, grupos ou setores profissionais. Embora a GPL seja considerada *open source* à luz da OSD, esta não exige que as obras derivadas sejam disponibilizadas nos mesmos termos. Daí que nem todas as licenças *open source* sejam compatíveis entre si.

- https://opensource.org/licenses/category;
- https://opensource.org/licenses/alphabetical.

O GitHub lançou um site, o http://choosealicense.com/, como uma forma de simplificar a seleção de uma licença *open source* para projetos e adicionou novas opções para configurações de licenças quando novos repositórios forem criados para esses projetos. A empresa já foi criticada por não lembrar usuários que disponibilizar um código publicamente não o coloca no **domínio público**, mas o deixa protegido com direitos autorais e sem licença.

No caso do software livre, o desenvolvedor poderia deixar seu programa em domínio público (sem direitos autorais, pertencente à coletividade ou comunidade em geral, podendo ser livremente utilizado); isto é, sujeito a toda e qualquer forma de utilização, alteração e distribuição. Porém, esta situação pode fazer com que indivíduos ou entidades modifiquem esse software e o disponibilizem mediante uma série de restrições, ignorando as

liberdades que o tornariam livre. É para evitar problemas como esses que surgiu o *copyleft*; através dele, as liberdades de modificação e distribuição são garantidas, tanto em um projeto original quanto em um derivado. Isso significa que uma pessoa ou uma organização não poderá obter um software livre, modificá-lo e distribuí-lo de maneira restrita, devendo compartilhar o programa (seja ele alterado ou não) pelas mesmas condições em que o obteve (compartilhamento pela mesma licença ou *share-alike*).

Existem mais de 200 licenças diferentes de código aberto, cada uma com seus próprios termos e condições. Um exemplo de licença de software livre que usa o *copyleft* forte é a GNU GPL (*General Public License*); já de *copyleft* fraco, são exemplos, a GNU LGPL (*Lesser General Public License* ou Licença Pública Geral Menor) e a MPL - *Mozilla Public License*. Também existem licenças de softwares livres sem *copyleft* como a licença X11, a licença Apache (*Apache license*) da ASF - *Apache Software Foundation* (https://www.apache.org/) e as licenças BSD (*Berkeley Software Distribution*), originalmente utilizada nos sistemas operacionais do tipo *Berkeley Software Distribution* (um sistema derivado do Unix).

- https://www.mozilla.org/en-US/foundation/trademarks/policy/;
- https://www.mozilla.org/pt-BR/about/legal/terms/mozilla/;
- https://www.mozilla.org/en-US/MPL/;
- https://www.mozilla.org/en-US/MPL/2.0/;
- https://www.apache.org/licenses/LICENSE-2.0;
- https://www.freebsd.org/doc/pt_BR/articles/explaining-bsd/article.html;
- https://opensource.org/licenses/bsd-license.php;
- https://www.gnu.org/licenses/bsd.pt-br.html.

Outras licenças livres são Latex, PHP, Python, EPL, etc.

- http://www.gnu.org/licenses/license-list.html;
- http://escolhaumalicenca.com.br/licencas/;
- https://opensource.org/licenses/bsd-license.php;

- https://opensource.org/licenses/isc-license.txt;
- https://opensource.org/licenses/mit-license.php;
- https://www.freebsd.org/copyright/freebsd-license.html.

GNU - GPL (*General Public License* ou Licença Pública Geral) é a designação da licença para software livre no âmbito do projeto GNU da FSF - *Free Software Foundation* (http://www.fsf.org/). A FSF - *Free Software Foundation* (https://www.fsf.org/pt-br) é uma organização sem fins lucrativos com o objetivo de promover a liberdade dos usuários de computador e defender os direitos deles. Por outras palavras, a GNU GPL é uma licença *copyleft* livre, criada pela FSF, para software e outros tipos de trabalhos. Originariamente, o projeto GNU (https://www.gnu.org/) foi lançado em setembro de 1983, por Richard M. Stallman, para criar um sistema operativo completo de Software Livre. GNU significa "GNU's Not Unix" (GNU Não é Unix). As principais licenças do projeto GNU são a GNU GPL - *General Public License* (Licença Pública Geral) e a GNU LGPL - *Lesser General Public License* (Licença Pública Geral Menor), originalmente designada GNU *Library General Public License* (Licença Pública Geral de Bibliotecas).

Ao contrário de outras licenças abertas, a GPL exige que o software disponibilizado segundo esta licença venha acompanhado com o seu código fonte. Esta condição destina-se a facilitar o desenvolvimento e a modificação de software. A característica mais polêmica da GPL é a exigência de que qualquer programa copiado ou derivado de software protegido pela licença deve ser distribuído nos mesmos termos do original. Daí a rotulação de viral em razão do software originariamente publicado "contaminar" as demais licenças abertas.

Em resumo, a GNU-GPL concede aos utilizadores quatro liberdades:

1) A liberdade de executar o software, para qualquer uso (liberdade 0);

2) A liberdade de estudar o funcionamento de um programa e de adaptá-lo às suas necessidades (liberdade 1). O acesso ao código-fonte

é um pré-requisito para isto;

3) A liberdade de redistribuir cópias e assim ajudar o nosso vizinho (liberdade 2);

4) A liberdade de melhorar o programa e de tornar as modificações públicas de modo que a comunidade inteira beneficie da melhoria (liberdade 3). O acesso ao código fonte é um pré-requisito para isto.

Ressalta-se que um programa não necessita obrigatoriamente de uma licença GPL para ser um software livre. É possível o uso de outras licenças, desde que compatíveis com as liberdades em questão.

A principal diferença entre a GPL e a LGPL é que esta permite também a associação com programas que não estejam sob as licenças GPL ou LGPL, incluindo software proprietário. Exemplificando, é possível parte do código sob a LGPL e o restante sob a GPL. Outra diferença significativa é que os trabalhos derivados, que não estão sob a LGPL, devem estar disponíveis em bibliotecas. A LGPL, desse modo, acrescenta restrições ao código fonte desenvolvido, mas não exige que seja aplicada a outros softwares que empreguem seu código, desde que este esteja disponível na forma de uma biblioteca. Logo, a inclusão do código desenvolvido sob a LGPL como parte integrante de um software só é permitida se o código fonte for liberado. Em resumo, a LGPL visa à regulamentação do uso de bibliotecas de código, mas pode ser empregada na regulamentação de aplicações, como OpenOffice.org e Mozilla.

A GPL (V2 ou V3) é uma licença *copyleft* que exige que quem distribui o seu código ou uma obra derivada deve disponibilizar o código fonte sob os mesmos termos.

- https://opensource.org/licenses/gpl-license;
- https://opensource.org/licenses/BSD-2-Clause;
- https://opensource.org/licenses/BSD-3-Clause;
- https://opensource.org/licenses/alphabetical;

- https://www.gnu.org/licenses/gpl-3.0.en.html;
- http://gplv3.fsf.org/.

A GNU LGPL (*Lesser General Public License*) é uma licença de software livre aprovada pela FSF e escrita como um meio termo entre a GPL e licenças mais permissivas, tais como a licença BSD e a licença MIT.

A *Apache Software License* (**licença de software Apache**) foi criada originalmente pela *Apache Software Foundation* para o licenciamento do servidor Web Apache. A licença Apache apresenta características similares às licenças BSD na medida em que não adota o princípio *copyleft*. Todo o software desenvolvido no âmbito da Fundação Apache é considerado como pertencente à ASF (*Apache Software Foundation*); logo aos seus membros, pelo que se terceiros efetuarem mudanças ao Apache, o resultado não pode ser chamado de Apache. A licença Apache é uma licença permissiva, similar à do MIT, mas que também prevê uma concessão expressa de direitos de patente dos contribuintes para os usuários.

A **licença MIT**, também chamada de licença X ou licença X11, é uma licença de programas de computadores (software), criada pelo MIT - *Massachusetts Institute of Technology* (http://web.mit.edu/). Ela é uma licença não *copyleft* utilizada em software livre; isto é, ela permite a reutilização de software licenciado em programas livres ou proprietários. Essa também é uma licença permissiva e considerada equivalente a BSD Simplificada sem a cláusula de endosso. Porém, seu texto é bem mais explícito ao tratar dos direitos que estão sendo transferidos, afirmando que qualquer pessoa que obtém uma cópia do software, e seus arquivos de documentação associados, pode utilizá-los sem restrição; incluindo sem limitação nos direitos de usar, copiar, modificar, mesclar, publicar, distribuir e vender cópias do software. As condições impostas para tanto são apenas manter o aviso de *copyright* e uma cópia da licença em todas as cópias do software. Em resumo, a licença MIT permite que as pessoas façam o que quiserem com código, desde que forneçam uma atribuição ao criador e não o responsabilize.

O Litecoin (https://litecoin.org/pt/), por exemplo, é um programa de código aberto lançado sob a licença MIT/X11, que garante a qualquer um

poder executar, modificar e copiar o programa, bem como distribuí-lo, a seu critério, versões modificadas do mesmo. Os códigos fonte do Litecoin e de outros projetos relacionados encontram-se disponíveis em: https://github.com/litecoin-project. Já o Bitcoin Core (https://bitcoin.org/pt_BR/download) é um projeto livre e de código aberto, também sob a licença MIT.

A **licença BSD** (*Berkeley Software Distribution*) impõe poucas restrições quando comparada àquelas impostas por outras licenças, como a GNU GPL (*General Public License*) ou mesmo as restrições padrões determinadas pelo *copyright*, colocando-a relativamente próxima do domínio público. A BSD é mais permissiva que a GPL. De fato, a licença BSD tem sido chamada de ***copycenter***, ou "centro de cópias", em comparação com o *copyright* padrão e o *copyleft* da licença GPL. A licença BSD permite que o software distribuído sob a licença, seja incorporado a produtos proprietários. Trabalhos baseados no material podem até ser liberados com licença proprietária. Também é possível que softwares sejam distribuídos pela licença BSD junto de outra licença. O texto da licença é considerado como de domínio público e pode ser modificado sem nenhuma restrição. Para satisfazer as necessidades de indivíduos ou organizações em particular, deve-se trocar as referências aos termos "Regents of the University of California", "University of California, Berkeley" e "Regents" pelo nome do próprio indivíduo ou organização. Em contraposição à GPL, as licenças BSD não obrigam à distribuição de obras derivadas nos mesmos termos que o programa original. Do mesmo modo, também não exigem que o código fonte seja disponibilizado juntamente com o executável. Enquanto que a licença GPL requer que os trabalhos derivados sejam licenciados sob o mesmo tipo de licença, a licença BSD requer apenas o reconhecimento (devida referência ou atribuição) do autor (ou detentor de direitos original) e possui outras pequenas restrições. As licenças estilo GPL são chamadas de licenças *copyleft* enquanto as licenças estilo BSD são chamadas de licenças permissivas. Os defensores do GPL argumentam que a obrigatoriedade dos softwares derivados serem licenciados através da GPL fomenta o crescimento do software livre e que as licenças BSD permitem as pessoas se apossarem do trabalho alheio sem terem que dar nada em troca. Apesar da BSD ser evidentemente mais livre que a GPL, a GPL é mais livre no sentido de garantir a liberdade nos trabalhos derivados. Por causa desse conceito de

liberdade do *copyleft*, pode-se dizer, então, que a BSD é mais liberal que a GPL.

A ***Mozilla Public License*** ou licença pública Mozilla (https://www.mozilla.org) emprega uma forma suave de *copyleft*. Exige a atribuição devida ao autor do software original e a inclusão da documentação dos ficheiros modificados. Além disso, todo o software derivado necessita ser distribuído nas mesmas condições da licença original. No entanto, ela pode ser combinada com software protegido por *copyright*. Daí que seja popular junto dos programadores que pretendem lançar versões fechadas e abertas do seu software. Contudo, isso torna-a incompatível com a GPL.

CC - **Creative Commons** (https://creativecommons.org/) é, na verdade, uma entidade sem fins lucrativos (NPO - *nonprofit* ou *non-business entity*) criada para permitir maior flexibilidade na utilização de obras protegidas (*protected works*) por direitos autorais (*copyright*). A ideia é fazer com que um autor/criador possa permitir o uso mais amplo de seus materiais por terceiros, sem que estes o façam infringindo as leis de proteção à propriedade intelectual (*intellectual property*). Estas licenças (*licenses*) permitem que os autores autorizem determinados usos das suas obras sem terem que abdicar do controle de outros usos. Daí o lema "alguns direitos reservados" (*some rights reserved*) em lugar do tradicional "todos os direitos reservados" (*all rights reserved*) do regime convencional de *copyright* (direitos autorais). A Creative Commons oferece um conjunto de seis licenças base à escolha aos detentores de direitos (*rightsholders*) que permitem que estes concedam aos utilizadores diferentes combinações dos quatro direitos que podem se situar num eixo que parte do *copyright* total ("todos os direitos reservados") até chegar ao domínio público (*no copyright* ou "nenhum direito reservado"). Esta flexibilidade faz com que as licenças CC sejam mais atrativas para os autores (*authors*) do que as licenças abertas do software que se se regem por um princípio do "tudo ou nada" (*everything or nothing*).

No site http://producingoss.com/pt-br/ existem mais orientações sobre como produzir um software *open source*.

Git é um sistema de controle de versão distribuída e de gerenciamento de código fonte, que é usado para desenvolvimento de software e outras tarefas de controle de versão. Como um controle de revisão distribuída visa a velocidade, a integridade dos dados e o suporte para fluxos de trabalho distribuídos, não-lineares. Já a palavra inglesa ***build*** (construir), que advêm do verbo *building* (construção), no contexto do desenvolvimento de software, é uma versão "compilada" de um software, ou parte dele, que contém um conjunto de recursos que poderão, ou não, integrar o produto final. *Build*, portanto, significa "em construção" ou "em obras" e quer dizer que o software está em processo de desenvolvimento, revisão, reformulação ou aperfeiçoamento e, desse modo, está em fases de testes.

Dentro da pasta base do projeto, e do respectivo software, deve existir um arquivo de texto denominado *license* (licença), no qual conterá o teor da respectiva licença, com os dados correlatos, ano e autor. Ainda mais, no cabeçalho de cada arquivo de código, deve constar uma nota sobre o *copyright* e a licença.

Detalhe, não se pode ir copiando o teor de licenças alheias, pois até mesmo os textos das licenças podem estar protegidos por direitos autorais.

- http://escolhaumalicenca.com.br/licencas/gpl-v2/;
- https://www.prestashop.com/pt/osl-licenca.

Uma observação, sem receita, seja direta ou indireta, nenhum projeto de software consegue prosperar. Desse modo, o pedido de ajuda, colaboração, trabalho voluntário, doações e patrocínio são imprescindíveis para um projeto.

Existem muitos sites para pedidos de doações (*donations*), "vaquinhas" online ou financiamento coletivo (*crowdfunding*):

- https://www.vakinha.com.br/;
- http://www.vaquinhasocial.com.br/;
- http://www.arrekade.com.br/;
- https://www.kickante.com.br/;

- http://bemdoado.com/;
- http://www.idea.me/;
- https://www.startando.com.br/;
- https://benfeitoria.com/;
- http://www.e-solidario.com.br/;
- https://www.broota.com.br/;
- http://juntos.com.vc/pt/projects;
- http://meufinanciamentocoletivo.com.br/;
- http://ppl.com.pt/pt;
- https://www.gofundme.com/;
- https://fondeadora.mx/;
- https://doare.org/br/arrecade;
- http://pt.wikihow.com/CCriar-Um-Site-Para-Receber-Doações;
- https://www.paypal.com/br/cgi-bin/webscr?cmd=_donate-intro-outside;
- https://www.catarse.me/;
- http://kapipal.com/;
- https://www.justgiving.com/;
- http://www.networkforgood.com/;
- https://www.kickstarter.com/;
- https://www.indiegogo.com/;
- http://www.startupcrowdfunding.com/.

O ***crowdfunding*** é uma alternativa de financiamento colaborativo que conta com a ajuda da comunidade para doações anônimas, de forma a financiar determinado projeto através da Internet.

Existem pessoas denominadas de **investidores anjos (*angel investors*)**, que investem em empresas nascentes com um alto potencial de crescimento.

- http://www.anjosdobrasil.net/;
- http://www.floripaangels.org/;
- http://www.gaveaangels.org.br/;
- http://astellainvest.com/;
- http://www.confrapar.com.br/;
- http://www.fundocriatec.com.br/.

Também existe a hipótese de fazer igual ao criador da NextAgro (NextAgro) e ir no programa de TV "Shark Tank" (Negociando com tubarões), do canal Sony, para tentar conseguir dinheiro para o empreendimento (http://www.sharkt.com.br/tag/nextagro/).

Além disso existem ONGs/ORGs que disponibilizam verbas para projetos de seus interesses.

Ainda mais, os governos (Municipais, Estaduais e a União) costumam liberar verbas como incentivos, subsídios ou subvenção econômica para fins diversos.

A Lei n.º 10.973/2004 (http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm), regulamentada pelo Decreto n.º 5.563/2005 (http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/Decreto/D5563.htm), por exemplo, visa o incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação e ao alcance da autonomia tecnológica e ao desenvolvimento industrial do país.

- https://www.brasil.gov.br/;
- https://www.governoeletronico.gov.br/;
- http://bibspi.planejamento.gov.br/;
- http://www.planejamento.gov.br/;

- http://www.mct.gov.br/;
- http://fndct.mcti.gov.br/;
- http://www.cnpq.br/;
- http://www.finep.gov.br/;
- http://www.bndes.gov.br/;
- http://embrapii.org.br/;
- http://www.sp.senai.br/;
- http://www.protec.org.br/.

Ainda mais, o artigo 21 da Lei n.º 11.196/2005 (http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11196.htm), conhecida como Lei do Bem, regulamentada pelo Decreto n.º 5.798/2006 (http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5798.htm), prevê a subvenção para apoio à parte do valor da remuneração de pesquisadores, com título de mestre ou doutor, empregados em atividades de inovação tecnológica em empresas localizadas no território brasileiro.

A GlobalSign (https://www.globalsign.com/pt-br/) oferece certificados SSL grátis para projetos *Open Source* (*Free SSL Certificates for Open Source Projects*). Para se qualificar a um Certificado Wildcard SSL grátis da GlobalSign, o projeto de software deve usar uma licença aprovada pela *Open Source Initiative*. A GlobalSign também exigirá que os projetos mantenham configurações SSL seguras. Os projetos podem rapidamente e facilmente avaliar a força do SSL usando o Verificador de Configuração SSL GlobalSign, que atualmente verifica a existência de mais de 30 problemas comuns relacionados à configuração e fornece recomendações sobre como corrigi-los, tornando, assim, mais fácil alcançar uma configuração segura. Os participantes da comunidade de software Open Source que estiverem interessados na obtenção de um Certificado Wildcard SSL grátis da GlobalSign podem se inscrever para tal ao acessar https://www.globalsign.com/ssl/ssl-open-source.

Depois de existir um código fonte básico ou um rascunho ou versão inicial (beta) para estudos, debates, aprimoramentos e testes pela comunidade, pode-se, e sugere-se, proceder ao registro do software básico. Por óbvio que a pessoa jurídica e a marca devem ser preexistentes. Depois que o software estiver revisado, atualizado, reformulado e pronto para ser utilizado, faz-se uma atualização das suas informações no órgão de registro. Por fim, a licença só deve ser concebida quando o software estiver pronto para ser disponibilizado ao público e estar com todos os demais registros protocolados.

É recomendável que o titular da marca e da licença do *software*, bem como da conta bancária ou equivalente, seja uma pessoa jurídica e, preferencialmente, uma pessoa jurídica sem fins lucrativos ou uma ONG/ORG (organização não governamental), tais como, por exemplos, uma associação civil, uma fundação, etc. Explica-se. Desta forma se terá maior credibilidade, maior aceitação, menor rejeição e menos desconfiança pelas pessoas. Ainda mais, entidades sem fins lucrativos usufruem de tratamento diferenciado pela tributação dos entes públicos e, além de poderem receber doações, também podem usufruir de produtos e serviços gratuitos de várias empresas. Por exemplo, as instituições sem fins lucrativos podem receber o Office 365 como doação (https://products.office.com/pt-br/nonprofit/office-365-nonprofit-plans-and-pricing).

- https://www.microsoft.com/brasil/ong/;
- http://www.abong.org.br/;
- http://portalongfacil.com.br/.

Por fim, é necessário calcular o ICO (*Initial Coin Offering* ou Oferta Inicial de Moedas); ou seja, o valor inicial de venda da moeda. A definição do valor inicial da moeda pode parecer insignificante, mas o seu preço inicial é parte integrante de como as moedas se desenvolvem. Embora não seja o fator mais importante no início de uma altcoin, ainda é uma boa maneira de medir o sucesso de uma moeda. Essa valoração segue praticamente o procedimento de *valuation* ou *pre-money value* de uma *startup* (*startup value*); ou seja, é o valor de um negócio em fase inicial e antes que um investidor faça seu investimento (*Post-Money Value*).

Recapitulando: *Pre-money* é o valor da *startup* antes de receber qualquer investimento; já o *Post-money* é o valor da *startup* depois de receber o investimento.

DO ASPECTO RELIGIOSO

Por questões religiosas existe muita resistência ao avanço dos pagamentos eletrônicos.

Não é de hoje que a possibilidade de implantação de um chip no corpo humano assusta os leigos e incautos. E muitos pregadores aproveitando-se disso para aterrorizar e manipular as pessoas.

No meio cristão, tanto entre católicos e evangélicos, é muito difundida a crença de que o uso de chips como meio de identificação e/ou forma de pagamentos seria a marca da Besta, o principal adversário (inimigo) de Deus e grande enganador do mundo para levar as pessoas à perdição (inferno); ou seja, o Anti-Cristo que finge ser um enviado (mensageiro ou representante) de Deus, mas se trata do próprio diabo (Satanás ou Lúcifer) encarnado (em forma humana) para enganar e desviar toda a humanidade de Deus.

Referida crença sobre o chip ser a marca da Besta se baseia na interpretação equivocada do livro bíblico de Apocalipse.

> "E fez que a todos, pequenos e grandes, ricos e pobres, livres e escravos, lhes fosse posto um sinal na mão direita, ou na fronte, para que ninguém pudesse comprar ou vender, senão aquele que tivesse o sinal, ou o nome da besta, ou o número do seu nome. Aqui há sabedoria. Aquele que tem entendimento, calcule o número da besta; porque é o número de um homem, e o seu número é seiscentos e sessenta e seis." (Apocalipse 13:16-18).

> "Seguiu-os ainda um terceiro anjo, dizendo com grande voz: Se alguém adorar a besta, e a sua imagem, e receber o sinal na fronte, ou na mão, também o tal beberá do vinho da ira de Deus, que se acha preparado sem mistura, no cálice da sua ira; e será atormentado com fogo e enxofre diante dos santos anjos e diante do Cordeiro. A fumaça do seu tormento sobe para todo o sempre; e não têm repouso nem de dia nem de noite os que adoram a besta e a sua imagem, nem aquele que recebe o sinal do seu nome. Aqui está a perseverança dos santos, daqueles que guardam os mandamentos de Deus e a fé em Jesus." (Apocalipse 14:9-12).

Desse modo, muitas pessoas, ingenuamente, têm entendido que o sinal do Anti-Cristo seria uma marca literal (física, material ou visível) e pessoal na "mão direita” ou na "testa" (literalmente fronte) de cada pessoa (ser humano). Entretanto, a Bíblia não diz nada disso. Pelo contrário, a Bíblia mostra que a simples associação, simpatia, afeição, aprovação, anuência,

concordância, conivência, convívio, interação, participação, consórcio, parceria, ligação, subordinação, etc. à instituição, ao sistema ou à doutrina anticristã gera automaticamente uma marca espiritual.

> "MAS o Espírito [Santo] expressamente diz que nos últimos tempos apostatarão alguns da fé, dando ouvidos a espíritos enganadores, e a doutrinas de demônios;" (I Timóteo 4:1). Colchetes nossos.

Outra variação das crenças sobre a marca da Besta são que a "testa" seria o computador, que a "mão" seria o mouse e que o número 666 estaria nos códigos de barras, nos códigos ASCII, etc.; mas tudo isso não passa de coincidências parciais e intencionais provocadas pelos filhos espirituais das trevas (diabo).

De forma semelhante, existem as teorias de conspirações de que o chip seria estratégia de controle e dominação pela Nova Ordem Mundial (*New World Order*), pela elite maçônica *Illuminati*, etc.

Para que pessoas como Bill Gates (fundador e dono da Microsoft), Paul Hewson, popularmente conhecido como "Bono Vox" (o vocalista do U2), Príncipe Charles da Inglaterra, etc. possam ser, pelo menos, cogitadas como sendo O Anti-Cristo, elas têm que, antes, poderem concorrer ao trono de Satanás (cargo de liderança da Babilônia, a falsa igreja, falsa vinha, a grande meretriz e mãe das abominações). Assim, como nenhuma dessas pessoas é sacerdote ou ministro religioso (muito menos, cardeal católico), tais especulações não passam de falácias, devaneios e delírios. Claro que se um deles, "da noite para o dia" (como no passado a Igreja Católica já fez), se tornar um cardeal católico (e, portanto, ser candidato à sucessão papal), aí o contexto muda. Mas, isso nunca acontecerá porque estes famosos servem apenas para distrair a atenção/foco do verdadeiro Anti-Cristo. Mais abaixo explicamos melhor sobre o que e quem é O Anti-Cristo.

Estas especulações são inspiradas pelos demônios, como manobras de diversão, para desviar/afastar a atenção das pessoas do verdadeiro Anti-Cristo, da verdadeira marca da Besta na mão e na fronte (testa), do verdadeiro perigo da ação espiritual diabólica e do que ela contribui para a Perdição das almas.

A marca da Besta não tem nada a ver com nenhum chip implantado nas mãos das pessoas. A associação do chip com a marca da Besta visa confundir o conteúdo com a forma e o material com o espiritual, lançando uma polêmica na sociedade, fazendo com que alguns seguidores e amantes de Deus caiam na defesa de um postulado ridículo e falso; lançando, assim, no descrédito as suas posições e as da doutrina de Deus neste caso. Estas teorias de que o chip é a marca da Besta não é mais do que uma armadilha do diabo para fazer cair no descrédito e no ridículo algumas pessoas bem-intencionadas que defendem esse princípio ou teoria. A verdadeira marca da Besta de que nos fala o Apocalipse é uma marca espiritual; não material ou física. **Há um pertinente ditado chinês muito perspicaz: "Quando o dedo aponta para a Lua, o tolo olha para o dedo".**

Os chips atualmente utilizados não são do Estado, não são de nenhuma igreja ou religião, não são obrigatórios e não são a única forma possível de se identificar, de ter atendimento médico e nem para poder pagar ou receber pagamentos.

Os chips (de computador ou de informática em geral) em si são meras peças tecnológicas, fruto da inteligência e da ciência do homem. O uso que se faz de um determinado chip é que pode ser bom ou mau, lícito ou ilícito, moral ou imoral, etc. Portanto, conforme a enorme maioria dos objetos, aparelhos e demais coisas, pode ser utilizada para fins menos claros e, mesmo maus; mas, também, pode ser uma coisa muito boa e utilizada para fins altruístas, humanitários e, até mesmo, para a divulgação do Evangelho (Palavra de Deus). Tudo depende da intenção e do uso que a pessoa faz das coisas; assim, por exemplo, um simples lápis pode ser usado para matar os outros enquanto que uma arma de fogo pode ser usada para salvar vidas do ataque de animais selvagens e carnívoros. As mesmas estradas do império romano por onde transitavam os soldados romanos, facilitaram a pregação do Evangelho pelo apóstolo Paulo. Ainda mais, apesar de Paulo ser um cidadão romano (portando marcado pelos homens como pertencente a um império demoníaco), ele era cristão, pregou a Palavra de Jesus e lhe foi dado o ingresso para o Reino dos Céus (paraíso). A tecnologia de chips simplesmente permite o armazenamento e processamento de informações, a troca das chaves e de controles remotos convencionais, o controle de

estoque e o rastreamento de cargas, veículos, celulares, animais (bovinos, equinos, suínos, animais domésticos, etc.), presos, etc.

Os animais utilizam chips de identificação e rastreamento porque ainda não existe outro método que possa ser usado em relação a eles; vez que não possuem impressões digitais e nem sequer há estudos dos ângulos de seus rostos ou dos seus globos oculares. E, detalhe, os animais não usam celulares. Inclusive, a MasterCard e a Alibaba estão testando sistemas de pagamentos (respectivamente, “ID Check” e “Smile to pay”) que detecta e reconhece o rosto do cliente.

A tecnologia de identificar e rastrear pessoas através de chips é algo ultrapassado e defasado; vez que através de alguma pancada ou descarga elétrica, magnética ou radioativa o chip pode ser totalmente inutilizado o perder seus dados. E, inclusive, além de outra pessoa poder se apossar do chip de outrem, também existe todo um trabalho e despesa com fabricação, inserção de dados, implantação subcutânea e aparelhos leitores. Mediante o simples cadastramento de impressões digitais, dos ângulos do rosto ou da íris, o governo (humanos) pode identificar facilmente qualquer um através de vários dispositivos já existentes e em funcionamento (câmeras de vigilância e de segurança, caixas eletrônicos, *smartphones*, etc.). E, melhor ainda, todos os dados da pessoa (quem é, quem são seus parentes, onde moram, o que fazem da vida, quais são as suas fontes de renda e patrimônios, etc.) além de não precisarem estarem num reles chip, estão salvas num *data center* (banco de dados) compartilhado em vários servidores (ou na nuvem) para dificultar a perda. Outro detalhe, não é preciso fabricar e nem inserir nenhum tipo de equipamento ou aparelho nas pessoas; vez que as pessoas já possuem digitais, ângulos nos rostos e íris nos olhos. Por que iriasse desperdiçar tempo e dinheiro para utilizar um sistema ultrapassado? Um exemplo recente no Brasil é a implantação do uso das digitais dos eleitores nas urnas eletrônicas. Pela crença desses religiosos, deveria ser a implantação de chips.

Até o presente momento a única leitura de identificação que ainda (nem mesmo em teoria ou em ficção) existe meios de falsificar, é a da íris e retina do globo ocular. Se a pessoa está morta ou teve o globo ocular arrancado, a íris e a retina ficarão alteradas (não se mexerão mais, a pressão intraocular

estará alterada, não terá mais circulação sanguínea, etc.) e não se conseguirá a identificação pelo leitor. E a Bíblia não fala nada de marca da Besta nos olhos. Essa é a evolução da identificação segura e prática. Já senha, *login*, código de barras, crachá, cartão de identificação, QR-code, chip, digitais, leitura de digitais, etc. isso já existe há décadas e todos nós, sem nenhuma exceção, temos e usamos diariamente!

Um chip subcutâneo não costuma exigir uma senha e, assim, qualquer criminoso munido de uma simples máquina leitora pode obrigar (forçar) uma vítima a aproximar seu braço do leitor para roubar-lhe seus créditos (valores ou dinheiro). Na verdade, nem precisa usar de violência, basta passar com o leitor perto com a máquina leitora para furtar os valores. Anda mais, basta levar a vitma consigo, extrair-lhe o chip ou cortar-lhe a mão para pode abrir fechaduras, trancas, cofres e efetuar saques e pagamentos diversos. Já referido chip dentro de um smartphone ou de um relógio inteligente exige uma senha ou alguma forma de identificação para poder ser acessado e usado. Ainda mais, o chip dentro de aparelho permite maior controle; inclusive pode ser momentaneamente desativado ou até desativado. Outro detalhe é que um smartphone ou um relógio inteligente podem ser rastreados enquanto um chip subcutâneo não.

Os governos e empresas já possuem amplo acesso a tudo sobre as pessoas; pois em quase tudo o que fazemos existem programas espiões e/ou de vigilância. Assim, por exemplo, todo acesso à Internet, todas as comunicações telefônicas e todos os usos de cartões bancários são monitorados. Além disso, existem uma infinidade de câmeras por todos os lados, em todos os ambientes e lugares (empresas, instituições privadas, órgãos governamentais, bancos, locais públicos, aeroportos, praças, ruas, rodovias, etc.) e em tudo quanto é equipamento (*smartphones*, *tablets*, computadores, *notebooks*, smart TVs, caixas eletrônicos, veículos, drones, radares, satélites, aviões, uniformes de policiais e soldados, etc.). E todas as câmeras estão sujeitas a invasões (terceiros acionarem sem o proprietário saber) e a eficiência de muitas câmeras é tal que consegue tirar do espaço, uma foto com nitidez de uma moeda no chão. Desse modo, é muito fácil para essas câmeras, mesmo de longe, conseguirem identificar pessoas pelo rosto, pela íris e até pelas impressões digitais. Outra observação, a imensidão de smartphones contendo câmeras, linhas de celular, Internet e GPS facilitam

muito o trabalho de rastreamento e monitoramento através de programas de computadores. Desse modo, mesmo que a pessoa não tenha um celular e tome outros cuidados para não ser rastreada, sempre haverá perto dela alguma câmera com zoom que a indentificará, conhecerá sua exata localização e conseguirá acompanhá-la e observá-la em tempo real.

O FBI - *Federal Bureau of Investigation* (polícia federal dos Estados Unidos) usa drones (mini aeronaves não tripuladas com acesso remoto) de vigilância desde 2006 sem nenhuma regra de privacidade. Já a CIA - *Central Intelligence Agency* (agência central de inteligência dos Estados Unidos; equivalente à ABIN - Agência Brasileira de Inteligência) e outros órgãos de inteligência, segurança e militares dos Estados Unidos, utilizam drones muito mais potentes e com muitos mais recursos; inclusive armados com mísseis, operando até em outros países. No YouTube existem vários vídeos feitos de e por esse drones.

Para se ter uma noção, compare com os drones disponíveis para qualquer pessoa. As câmeras embutidas possuem alta resolução e grande poder de zoom. O Sunflower Home Awareness System da empresa Sunflower Labs (https://sunflower-labs.com/), por exemplo, permite a vigilância automatizada por drones. Através de luminárias com 12 (doze) sensores cada, analisam, em tempo real, cada vibração, movimento e som que está passando pelo local. Conseguem identificar e reconhecer quando é um carro, um animal ou uma pessoa. E se o visitante for um ser humano não identificado pelo sistema, ele enviará um drone, no piloto automático, para vigiá-lo. E, assim, o drone enviará as imagens do suspeito diretamente para o smartphone ou tablet do proprietário para que responda se é uma ameaça ou não. Já a empresa Aptonomy (http://www.aptonomy.com/) possui drones guarda-costas. Eles também são capazes de voarem sozinhos e vigiar determinada região. Se identificarem uma atividade suspeita, mandam imagens para seus donos, jogam luz nos suspeitos e ligam alto-falantes alertando risco.

O programa **Google Street View**, por exemplo, com a desculpa de mapear o mundo em 3D (três dimensões), possui não só fotos em 360 graus de todas as ruas do mundo; mas, também, invadiu todos as redes sem fio de Internet por onde passou seus veículos mapeadores.

- https://maps.google.com.br/;
- https://www.google.com/intl/pt-BR/maps/about/;
- https://www.google.com.br/intl/pt-BR/streetview/understand/.

Segundo a FCC - *Federal Communications Commission* (Comissão Federal de Comunicação), a companhia utilizou o Wi-Fi dos carros do Street View para coletar informações particulares sem autorização. No processo n.º 0025125-44.2013.8.07.0001 (antigo 2013.01.1.096604-4), da 23ª Vara Cível de Brasília, movida pelo IBDI - Instituto Brasileiro de Política e Direito da Informática contra o Google Brasil Internet Ltda, uma decisão judicial determinou ao Google apresentar os dados coletados de redes wi-fi pelos seus carros de mapeamento fotográfico Street View no Brasil, sob pena de multa de R$ 100 mil por dia de desobedecimento. Também há ação civil coletiva do IBDI contra o Google, objetivando o pagamento de indenização por danos morais coletivos em razão de coleta indiscriminada de dados dos cidadãos brasileiros. Trata-se do processo n.º 0000188-96.2015.8.07.0001 (antigo 2015.01.1.000575-6), da 23ª Vara Cível de Brasília.

- http://www.tjdft.jus.br/.

O que mais possui rejeição entre esses religiosos é a identificação das pessoas cumulada com uma carteira de créditos através de um chip de computador implantado no dorso (oposto da palma) da mão.

O anúncio do **Verichip** (https://pt.wikipedia.org/wiki/VeriChip) aterrorizou essas pessoas. O Verichip foi um chip RFID produzido pela PositiveID para identificação e localização por radiofrequência a curto alcance.

O **RFID** - *Radio Frequency Identification* (identificação por radiofrequência) é um sistema de captura de dados que utiliza o sinal (frequência) de rádio para realizar tarefas (identificação, localização, rastreamento, etc.). Um dos primeiros sistemas passivos de RFID surgiu durante a Segunda Guerra Mundial quando os aviões eram detectados à

longa distância pelos radares. Depois, na década de 80, a tecnologia foi aperfeiçoada para os circuitos dos cartões bancários e de créditos.

Em resumo, o RFID é um nome genérico para uma série de tecnologias que permitem identificar objetos através de ondas de rádio (RF - radiofrequência). Isso significa que, basicamente, tudo que se comunica sem fio pode ser considerado RFID; incluindo o telefone celular que possui vários transceptores de rádio, cada um com identificadores exclusivos (endereços MAC - *Media Access Control* [endereço de controle de acesso], IMEI - *International Mobile Equipment Identity* [Identificação Internacional de Equipamento Móvel], etc.).

Uma ideia que expandiu consideravelmente as possibilidades de uso da tecnologia são as chamadas *tags* (etiquetas) NFC - *Near Field Communication* (também conhecidas como NFC Sticker, SmartTag NFC, Adesivos NFC ou etiquetas NFC). Em formato de uma etiqueta (adesivo), tatuagem ou chaveiro, esses pequenos dispositivos NFC podem ser configurados para realizar diversas atividades.

Uma etiqueta (*tag* em inglês) RFID é um transponder (junção das palavras em inglês "transmit" e "responder" pelo fato de transmitirem uma resposta ao sinal do leitor), pequeno objeto que pode ser colocado em uma pessoa, animal, equipamento, embalagem ou produto, dentre outros.

A Etiqueta TWC é uma tag RFID que grava e transmite dados dos chips por ondas de rádio frequência permitindo controlar e monitorar objetos de forma segura e inteligente.

As etiquetas (*tags*) NFC são formadas, basicamente, por um pequeno chip de rádio (de silício identificador de radiofrequência), acompanhado de uma antena simples (que lhe permite responder aos sinais de rádio enviados por uma base transmissora) e alguma quantidade de memória para armazenamento de dados. Normalmente, esses dispositivos funcionam no modo passivo; ou seja, não é necessário deixá-los ligados constantemente à uma fonte de energia.

RFID sem chip é um termo genérico para sistemas que usam energia de rádio frequência para transmitir dados, mas não armazena um número serial em um microchip de silício no transponder. Algumas *tags* (etiquetas ou adesivos) sem chip usam plásticos ou polímeros condutivos em vez de microchips de silício. Outras *tags* sem chips usam materiais que refletem de volta uma parte das ondas de rádio irradiadas para eles. Um computador faz uma fotografia instantânea das ondas transmitidas de volta e usa-as como uma impressão digital para identificar o objeto com a *tag*. Empresas estão experimentando a incorporação de fibras refletoras de rádio frequências em papel para evitar fotocópias não autorizadas de determinados documentos. Há tintas que refletem as ondas de rádio em determinadas frequências, permitindo que os agricultores, por exemplo, tatuem um transponder RFID sem chip em um animal para fins de identificação.

As etiquetas RFID, portanto, são geralmente passivas (sem alimentação), que podem variar em frequência, capacidade de memória e características de funcionamento. As *tags* passivas são alimentadas pela energia das ondas eletromagnéticas emitidas pela antena do leitor. A antena da *tag* captura essa energia, utilizando parte dela para a alimentação da etiqueta e a outra parte para o envio das informações ao leitor. Portanto, a antena da *tag* passiva só consegue enviar um sinal caso ela receba o sinal enviado pela antena do leitor. Dito de outra maneira, ela só responde caso ouça a um chamado. Caso contrário, ela não emite nenhum sinal ou, por outra, permanece “em silêncio”. Já as *tags* ativas não precisam ser alimentadas pela emissão das ondas eletromagnéticas, pois elas possuem uma bateria interna que desempenha essa função. Elas, também, possuem um modulador de radiofrequência, com o que conseguem criar um novo sinal de radiofrequência sem a necessidade da presença do leitor. A antena das *tags* ativas fica, portanto, emitindo sinais o tempo todo esperando que a antena de um leitor os encontre. Isso significa que o sinal das *tags* ativas tem maior alcance, apresentando maior probabilidade de ser captado. Suas desvantagens, consistem no fato de que a bateria tem vida útil limitada, além de aumentar o custo e o tamanho das *tags*. Ainda existem as *tags* semi-passivas ou semi-ativas. É o meio termo entre a ativa e passiva. Elas, tal como as ativas, possuem uma bateria interna para sua alimentação. Entretanto, como as passivas, elas precisam da presença do leitor para comunicar suas informações; pois elas não possuem um modulador e não

são, portanto, capazes de criar um novo sinal de radiofrequência. Em resumo, além das etiquetas passivas que somente respondem ao sinal enviado pela base transmissora, também existem as etiquetas semipassivas e as ativas, dotadas de bateria, que lhes permite enviar o próprio sinal.

Existem transponders do tipo somente leitura (*read only*), que possuem um código pré-gravado de fábrica em sua memória e transponders do tipo leitura / escrita (read / write), onde é possível ler e gravar dados na memória.

Normalmente uma *tag* RFID não carrega mais de 2 kilobytes (KB) de dados. A maioria dos leitores UHF custam de US$ 500 a US$ 2.000, dependendo das características do dispositivo. De modo geral, as *tags* ativas custam de US$ 25 para mais. *Tags* ativas com embalagem especial de proteção, baterias de longa duração ou sensores podem custar US$ 100 ou mais. Os códigos de barras são mais baratos e mais eficazes para determinadas tarefas do que o RFID.

Ao contrário de um leitor para código de barras que exige linha direta e proximidade; um leitor RFID não necessita de contato visual com a etiqueta para ler os dados e a leitura pode ser feita através de diversos materiais como plástico, madeira, vidro, papel, tecido, etc. Entretanto, certos obstáculos (água, metal, líquido, corpo humano, madeira, etc.) existentes entre a etiqueta e a antena podem interferir e, até mesmo, obstruir o sinal. O dispositivo pode, inclusive, realizar a leitura simultânea de milhares de microchips e armazenar o resultado em uma memória para posterior envio ao servidor do sistema.

Em razão de os leitores não precisarem de linha de visão ou visão direta da etiqueta, isso torna possível para qualquer pessoa (concorrentes, criminosos, governo, etc.) com um leitor apropriado acessar o chip RFID com suas informações. Desse modo, dispositivos não autorizados podem, não só ler, mas, também, alterar os dados dos chips RFID sem o conhecimento do seu proprietário, possuidor ou usuário. Ainda mais, o denominado ataque de canal lateral permite interceptar dados (identificações, senhas, endereços e demais informações) de RFID à medida que passa do chip para o leitor. Pior, ainda não foi desenvolvido nenhum

sistema à prova de interceptações. Mesmo as etiquetas passivas, que possuem alcance de apenas alguns metros, ainda se encontram vulneráveis a leituras indevidas de dados. Desse modo, é possível copiar a assinatura de um cartão RFID através de leitor RFID e um computador.

O alcance de leitura das *tags* (etiquetas) constitui a maior e mais determinante vulnerabilidade desta tecnologia tanto quanto a ataques por clonagem como ataques à privacidade. Conforme dito supra, um simples *scan* (leitor) é suficiente para criar um clone. De forma a impedir leituras a longo alcance foram desenvolvidas bolsas rádio opacas para transportar as *tags* RFID em segurança; contudo, estas bolsas apenas atenuam a distância (enfraquecem o sinal) a que as *tags* conseguem ser lidas e, assim, não garantem a total segurança contra *scans* (leituras) indevidos e dependem ainda de atitudes pessoais preventivas.

Outro detalhe, através de um leitor o criminoso consegue saber o endereço da pessoa, sua situação financeira e copiar, além de outras senhas, as chaves de acesso do portão e das portas e, assim, ir facilmente furtar a residência ou a empresa da vítima.

Diante disso, especialistas em segurança alertam contra o uso de RFID para autenticação de pessoas devido ao risco de roubo de identidade. Seria possível, por exemplo, alguém roubar a identidade de uma pessoa em tempo real. Devido a alto custo, seria praticamente impossível se proteger contra esses ataques, pois seriam necessários protocolos muito complexos para saber a distância do chip e, quanto mais complexo o algoritmo, exige maior poder de processamento, mais energia gasta e mais bateria necessita.

Existem vários **tipos de ataques *hackers*** possíveis:

- ***Cloning*** (clonagem) significa duplicar ou manipular uma *tag* RFID para criar uma cópia idêntica, ou uma variação, que possa ser aceite por uma aplicação RFID como válida;

- ***Spoofing*** é uma variação de *cloning* na medida em que não necessita de replicar fisicamente uma tag RFID. Neste tipo de

ataques, um atacante simula uma tag RFID válida para ganhar os seus privilégios;

- ***Eavesdropping*** (espionagem) é a técnica de recolher informação secreta através de leitores especiais ou antenas sensíveis. Esta informação pode ser de carácter pessoal, como informações pessoais ou a localização do indivíduo, ou de carácter empresarial, espionagem empresarial. Este tipo de ataque pode ocorrer em ambas direções: da *tag* para o leitor ou do leitor para a *tag*. Como os leitores emitem informação com maior potência que as *tags*, o leitor está sujeito a este ataque a partir de uma distância muito superior à das *tags*, tendo por isso um maior risco;

- ***Man-in-the-middle*** (homem no meio). Nesse método, o atacante fazer-se passar por um leitor legítimo, ou *tag*, com o fim de recolher informação ou metadata RFID, ou manipular a informação enviada entre uma *tag* e o sistema *backend*. Isto pode permitir ao atacante realizar ações como, por exemplo, injetar código maligno no sistema e ganhar acesso a áreas restritas;

- ***Code Injection Attack*** (injeção de código maligno). Este tipo de ataque caracteriza-se pela manipulação da informação RFID e introdução de código maligno ou fragmentos de código (vírus) com a intenção de alterar os processos contidos no sistema *backend* (visões do usuário final ou execução dos programas do sistema operacional em resposta à solicitação do usuário) ou como a informação RFID é tratada. Este *malware* pretende explorar as vulnerabilidades de implementações desleixadas, podendo fazer com que o sistema atinja um estado não definido ou simplesmente *crashe*, quando, por exemplo, não existem *missing error handlers* (faltando manipuladores de erro), pouco ou nenhum controle de *overflow* (transbordar) de *buffers* e formato dos dados. Particularmente, estes ataques podem ser feitos a bases de dados SQL - *Structured Query Language* (linguagem de consulta estruturada) para alterar qualquer registo, sendo assim possível ganhar acesso ilegal ao sistema *backend* (sistema responsável pela

regra de negócios, webservices e APIs de uma aplicação), desativá-lo ou destruí-lo completamente;

- ***DoS - Denial of Service*** (negação de serviço). Quase todos os componentes num sistema RFID podem ser alvo de um ataque DoS, incluindo a *tag*, o leitor ou o sistema *backend*. Ataques à interface de comunicação podem incluir: blindagem de *tags*, inundação do leitor com uma infinidade de *tags* virtuais (falsas) ou congestionar o leitor de uma forma mais seletiva. O objetivo deste tipo de ataque é, normalmente, sabotar os recursos de um sistema RFID, uma cadeia de abastecimento, por exemplo, tornando-o indisponível para os utilizadores para os quais o sistema foi projetado;

- ***TID cloning***. As *tags* do tipo EPC contém um campo na sua data com o Tag Identifier (TID), este identificador pode constituir um perigo na segurança das *tags* RFID na medida em que se este não for definido de fábrica qualquer pessoa pode, com as ferramentas adequadas, clonar dispositivos RFID definindo o *tag* como aquele do dispositivo que se pretende copiar. Já se este TID for definido de fábrica torna-se teoricamente impossível clonar as *tags*, vez que já que não será possível definir o TID como aquele do cartão que se pretende copiar, mantendo-se, assim, cada cartão uma identidade única e permanente. Ainda assim, e apesar disso, mesmo nos cartões de segunda geração o modelo standard Gen-2 apenas obriga que o TID identifique o fabricante e outra informação para determinar as capacidades da *tag*. Existem duas classes de *tags* definidas quanto ao TID, a classe E0h e a classe E2h, a primeira define que o TID consiste num ID do fabricante e um número de série de 48-bit, a segunda define que apenas é necessário que o TID contenha o ID do fabricante e o modelo da *tag*. É possível clonar com sucesso *tags* da classe E2h por não terem um identificador único em cada chip (mas um identificador comum a todos) com informações do fabricante e modelo que se torna irrelevante para a segurança anti-clonagem. Ainda assim a grande ameaça a segurança das *tags* não reside na anticlonagem, mas na sua capacidade de evitar a emulação de sinal; isto é, a

capacidade de, mesmo sendo captado um sinal, a informação que ele tenha não possa ser reutilizada ou não possa ser descodificada;

- ***Kill PIN*** (matar o PIN) consiste em, à distância, reprogramar ou desativar permanentemente uma *tag* RFID. Alternativamente o atacante pode usar esse método para identificar a *tag*, definindo o que quiser nesse espaço e assim marcando a *tag* para a localizar ou identificar mais tarde a partir de qualquer outro aparelho de leitura.

Os componentes elétricos do próprio chip RFID pode conflitar com outros dispositivos eletrônicos ou sofrerem interferências ou danos com água, descarga estática, raios e imãs de alta potência. Qualquer dispositivo (empilhadeiras, *walkie-talkies*, etc.) que utiliza parte do espectro eletromagnético da frequência de rádio do RFID pode interferir com a sua funcionalidade. Inclusive, o sinal de um leitor pode interferir com o sinal de outro, onde há sobreposição de cobertura. Como proteção, os leitores podem usar blindagem, mas isto complica as implantações e as tornam mais caras. O padrão EPC Gen 2 inclui algo chamado "dense reader" (leitor denso) de modo a evitar a colisão de leitores.

Outro problema é a vida útil de uma bateria para etiquetas ativas de RFID, que ainda é muito curta, o que geraria um certo transtorno ao invés de comodidade, pois ela precisaria ser reposta em pouco tempo. E isso também impede também o desenvolvimento de processos mais elaborados utilizando a RFID porque demandaria ainda mais energia de seus dispositivos.

Algumas **desvantagens e dificuldades na implantação do RFID** segundo Orlando Norio (http://www.afixgraf.com.br/rfid-vantagens-desvantagens/):

- Custo total maior considerando a infraestrutura necessária para que a solução funcione: antenas, leitoras, software para tratamento da informação capturada, desenvolvimento de aplicativos, sistema de comunicação, etc.;

- Custo da tag RFID, mesmo sem considerar encapsulamento especial é ainda bem maior do que etiqueta de

código de barras;

- O campo magnético de um metal interfere na propagação da onda RF, diminuindo muito a distância de leitura. Para resolver esta questão é necessário encapsular o chip com material especial que aumentam mais o custo da tag;

- Para assegurar grande distância de leitura é preciso usar frequência mais alta (HF ou UHF) dependendo ou não da existência de algum obstáculo entre a tag e a antena, que se traduz em mais custo;

- Em algumas aplicações a etiqueta RFID necessitará que o código gravado no chip seja também impressa no corpo da etiqueta com o código de barras precavendo uma situação em que necessite fazer a identificação visual;

- O código gravado no chip só pode ser lido por uma antena. Significa que se não possuir ou não dispor de uma leitora RFID no momento não tem como identificar o objeto de controle;

- Dependendo do tamanho do chip utilizado, o tamanho da etiqueta fica muito grande tanto no comprimento, largura e altura (espessura). Isto pode dificultar a fixação da tag no objeto, tornar vulnerável, antiestético, etc.;

- No projeto RFID é necessário considerar o obstáculo entre a etiqueta e a antena: líquido, água, metal, corpo humano impedem a propagação da onda de rádio, gerando ponto cego, local onde não acontece a leitura RFID.

O uso mais comum é das etiquetas de rastreamento com leitores com alarme para evitar furtos (saída de produtos não pagos) em estabelecimentos comerciais.

Nos cartões bancários (de débito e de crédito), constam os chips RFID, onde a tarja magnética contém a ID (*identity* ou identidade do usuário).

O chamado “Bilhete Único” de São Paulo, o RioCard do Rio de Janeiro, o Cartão Mais Aracaju de Aracaju e região metropolitana, o “Cartão Transporte” como é conhecido em Curitiba e vários outros cartões bilhetes de passagens são cartões inteligente (*smartcard*) pré-pagos, que facilitam o pagamento de passagens nos meios de transporte coletivo. Referidos cartões, contendo chip ou microprocessador, memória, antena de transmissão e chaves criptográficas, funcionam como um cartão de débito no qual são armazenados os créditos. Dependendo da modalidade, pode ser descartável ou recarregável. O usuário aproxima o cartão de um leitor eletrônico e, caso tenha crédito suficiente para a passagem, a roleta é liberada. Entretanto, é possível clonar à distância referidos cartões de transporte. Através de um leitor, em frações de segundo, o *hacker* coleta os dados do cartão eletrônico e os repassam para um computador ou notebook que os usará para serem gravados em um novo cartão. Toda essa operação leva menos de três minutos.

A tecnologia também é comum nos pedágios de algumas rodovias. Ao invés de os carros pararem, um cartão provido com o microchip RFID é colocado no para-brisa do veículo, enviando seu código de identificação para as antenas ou leitores eletrônicos localizados na cabine de cobrança. Uma vez reconhecido o código, a passagem é liberada.

- https://www.semparar.com.br/como-funciona/.

Um implante subcutâneo, de um chip do tamanho de um grão de arroz, além de poder conter informações pessoais, permite abrir portas, acender luzes e acessar computadores apenas com um aceno de mão.

- http://www.projectcompany.org/faq-implante-nfc.

Para que uma pessoa, usando um microchip RFID, possa ser detectada por um satélite é necessário que ela porte um dispositivo transmissor GPS - *Global Positioning System* (Sistema de Posicionamento Global) ou GLONASS (Sistema de Navegação Global por Satélite da Rússia), que ainda é relativamente grande e necessita de uma bateria de longa duração para funcionar, associado ao microchip, que contém as informações

pessoais. Somente dessa forma sistemas RFID com chips implantados em pessoas permitem a rastreabilidade a longas distâncias.

Durante a GITEX (http://www.gitex.com/) 2016, feira de inovação realizada em Dubai, a Etisalat - *Emirates Telecommunications Corporation* (http://www.etisalat.ae/) demonstrou no como um chip do tamanho de um grão de arroz, colocado na mão de um cliente, armazena todos os dados de seu cartão de crédito, identidade e cartão de visita. A tecnologia denominada de *biohacking* utiliza o NFC (*Near Field Communication*), já utilizado em alguns smartphones e pulseiras, para a realização de pagamentos através da proximidade da mão chipada com o leitor. A empresa teria dito que possui um acordo com a Visa para emitir os primeiros cartões de crédito em formato de chip no Oriente Médio. Possivelmente até 2020 estariam disponíveis para todos os interessados. O kit da seringa e o chip injetável deverá custar cerca de 100 dólares.

- http://www.id.gov.ae/en/media-centre/news/2016/10/20/etisalats-chief-executive-briefed-on-emirates-id-services-at-gitex-2016.aspx.

O NFC é uma tecnologia criada para permitir a comunicação entre dois dispositivos. Um deles faz o papel de *initiator* (iniciador); ou seja, inicia a comunicação e controla a troca de informações. O outro faz o papel de *target* (alvo), devendo responder às solicitações do initiator. Para tentar assegurar que os dados do cartão permanecerão em segurança, as conexões NFC são estabelecidas através de um canal seguro, que criptografa os dados à medida em que eles passam do cartão para o leitor. Uma das proteções do NFC é o protocolo SWP (*Single Wire Protocol*); um padrão que oferece comunicação segura entre o cartão SIM (chip de celular) e o chip NFC do aparelho. O problema é que o SWP não é amplamente adotado por precisar de mais testes e não ter implementação simples.

Saiba mais sobre o NFC ("Near Field Communication") nos capítulos DA MOEDA MUNDIAL CONTEMPORÂNEA, A FICÇÃO SE TORNOU REALIDADE e OUTROS MEIOS DE PAGAMENTO ELETRÔNICO OU DIGITAL.

No Japão, o sistema de metrô permite que passagens sejam compradas com a aproximação do aparelho de telefone com NFC às catracas.

Recorda-se que os cartões com NFC são compostos por um chip e uma antena para comunicação sem fio. Cada um deles contém um complexo sistema de armazenamento de dados que podem ser ativados, selecionados e copiados a muitos metros de distância, sem que o seu portador perceba.

Explica-se. Considerando que um cartão NFC é *contactless* (sem contato) e não precisa de código de acesso (senha), isso o torna vulnerável. Desse modo, o número de cartão lido pela aplicação pode ser usado em plataformas online que não pedem o código CVC - *Card Verification Code* (código de verificação de cartão), CVV - *Card Verification Value* (valor de verificação do cartão), CSC - *Card Security Code* (código de segurança do cartão), CVD - *Card Verification Data* (dados de verificação do cartão), CVN - *Card Verification Number* (número de verificação do cartão), CVVC - *Card Verification Value Code* (código de valor de verificação do cartão), V-code (*verification code* ou código de verificação), etc. Portanto, basta ao criminoso trazer consigo um aparelho leitor TPA (Terminal de Pagamento Automático) ou POS (*Point of Sale* [ponto de venda] ou *Point of Service* [ponto de serviço]) Móvel na mão contendo o aplicativo Credit Card Reader NFC; ou seja, a "maquininha" de ler cartão NFC, e, assim, de forma ardilosa ele furta as pessoas sem tocar na carteira das mesmas. Simplesmente o criminoso digita um valor a receber na leitora e sai andando com ela próxima dos bolsos, bolsas, pastas e valises dos outros para que algum cartão receba o sinal e, assim, lhe transfira o valor requisitado.

Ressalta-se que não se confunde POS (acima descrito) com PoS - *Proof of Stake* (prova de jogo ou de participação).

Porém, a carteira Secrid (https://www.secrid.com/pt/protect-your-cards/), vem equipada com um Cardprotector: um sistema ultrafino fabricado em alumínio que funciona como um *firewall* para proteger cartões de danos físicos e roubo de dados; evitando-se, assim, o furto de dados dos cartões RFID (*Radio Frequency Identification*) e NFC (*Near Field Communication*). Existem outras carteiras blindadas no mercado: http://comprarinternetblog.weebly.com/blog/top-10-mejores-rfid-carteras-en-2016-criticas. Também é possível, através de um corte mínimo, de cerca

de 5 mm na margem ou contorno do cartão, cortar-lhe a antena e, assim, jamais o sistema RFID e/ou NFC será acionado.

O acatamento ou aceitação da crença de que o chip é a marca da Besta, implicaria em nenhum Cristão poder ter sequer Certidão de Nascimento, CPF (Cadastro de Pessoa Física), Carteira de identidade/identificação ou RG (Registro Geral), CNH (Carteira Nacional de Habilitação), Passaporte, Certificado Digital, celular, *smartphone*, GPS, cartões bancários, computador, *tablet*, notebook, Internet (pois tudo na Internet é fiscalizado pelo Carnívoro [super computador] dos americanos), prestar declarações à Receita Federal, etc. Explica-se. Todos esses exemplos envolvem identificação, controle, vigilância e rastreio de pessoas e de compras.

- https://exateus.com/2016/06/21/a-uniao-europeia-propoe-o-uso-da-identidade-digital-para-acessar-a-internet/.

Por exemplo, Andrea Hernandez, com 15 anos de idade, no final de 2012 foi suspensa e, em janeiro de 2013 foi expulsa, da escola de ensino médio John Jay, em San Antonio, Texas, Estados Unidos, por ter se recusado a usar um crachá (*Smart ID card*) com chip RFID alegando ser a marca da Besta.

Poderíamos ir mais além e dizer que nem mesmo poder-se-ia tocar em dinheiro, pois a Bíblia condena o apego ao dinheiro (Mateus 10:9, 19:21,24 e 22:19-21, Marcos 10:21, Lucas 12:15-21, 16:13, 18:25 e 20:24-25, Atos 8:20, I Timóteo 6:10, etc.). Em regra, quem consegue comprar algo ou adquirir um serviço sem o deus Mamon (dinheiro, Lucas 16:13)? Ninguém! Mas, por exceção, existem o escambo, pagamento com serviços, caridade, etc.

Explica-se. O chip nada mais é do que um aperfeiçoamento do que já existe a muito tempo. A profecia bíblica de não poder comprar e nem vender nada mais é do que os antigos castigos de banimentos, excomunhões, rejeição social, não dar abrigo, etc.

Durante os períodos de *apartheid* (separação) na África do Sul e de discriminação e segregação raciais nos Estados Unidos, havia uma separação social entre as pessoas de cútis (pele) branca e negra. Desse modo, existiam lugares privativos (exclusivos) para os brancos onde

constavam cartazes com frases como "For use by white persons" (Para uso de pessoas brancas) e, igualmente, os cartazes escritos "colored" (de cor) indicando os locais (cantinhos, portas dos fundos ou assentos reservados) destinados para os negros. Mas, alguns estabelecimentos somente atendiam pessoas brancas e, assim, possuíam cartazes, tais como, "We do not serve black people" (Não atendemos pessoas negras). De modo semelhante, os religiosos da igreja do Anti-Cristo irão discriminar e rejeitar todas as pessoas que não fizerem parte da igreja do Anti-Cristo. Desse modo, esses religiosos irão se recusar a vender e a prestarem serviços para quem não for membro da igreja deles. De igual modo, também não irão comprar e nem aceitar serviços de quem não for membro da igreja do Anti-Cristo. E como saber quem faz parte ou não? Pelo fato de os membros frequentarem as periódicas reuniões, todos os membros se conhecem. Ainda mais todos os membros são cadastrados (possuem ficha) na instituição religiosa. E, mesmo que não fosse assim, os membros da religião do Anti-Cristo possuem a sua própria e exclusiva forma de se cumprimentarem, podendo ser algo semelhante à "Salve o Anti-Cristo" ou "Heil Hitler". E, detalhe, as pessoas se cumprimentam com a mão direita. Outro detalhe, os estabelecimentos comerciais dos membros da religião do Anti-Cristo também poderão colocar alguma indicação na fachada (frente) e em todos os documentos do estabelecimento para facilitar sua identificação como membro da igreja do Anti-Cristo, como algo semelhante à frase “O Anti-Cristo é fiel”, o logotipo da instituição religiosa ou a foto do Anti-Cristo.

Se nem mesmo o Estado (homens) precisam de uma marca material, física ou visível para saber quem é quem, onde mora, onde trabalha, o que faz da vida, que patrimônio e renda possui, quais são as compras que faz, etc. muito menos os seres espirituais precisam de tal recurso (Atos 16:16-17). Explica-se. As Certidões de Nascimento, os CPFs (Cadastro de Pessoas Físicas), RGs (Registros Gerais ou carteira de identidade), Censos, Declarações de IR (Imposto de Renda), Guias Informativas das empresas (INSS, FGTS, SD...), etc. já prestam as informações necessárias para o Estado. Quem consegue abrir uma conta corrente ou uma empresa sem ter CPF? Quem consegue ter CPF sem ter Certidão de Nascimento? Até mesmo para poder ter uma linha de celular ou assinar qualquer contrato, é necessário possuir CPF. O rastreio e controle das pessoas pelo Estado começou através dos censos para se saber quantos súditos o rei tinha; depois instituiu as certidões

de nascimento e de casamento, depois o RG e CPF, etc. Assim o Estado já sabe que você existe, o que você faz da vida, sua graduação, seu estado civil, onde você mora, seus familiares, suas digitais, sua renda, seu patrimônio, seus gastos, etc.

Recorda-se, ainda, que as instituições financeiras, os contadores e outros profissionais e empresas prestam informações de seus clientes ao governo.

Portanto, o eventual e suposto implante subcutâneo de chip (tecnologia ultrapassada) seria apenas uma melhora do cartão bancário e/ou de crédito (que já possuem chip). Facilitaria o Estado identificar e rastrear mais fácil as pessoas? Talvez sim, talvez não. Mesmo que facilitasse, não usar o chip não impediria o Estado de identificar e rastrear as pessoas. Pelo celular, acessos à Internet, uso de caixas eletrônicos e utilização de cartões bancários e de créditos, os Estados Unidos, há anos, rastreiam em tempo real todo mundo. Anonimato, teoricamente, é só para quem nunca fez Certidão de Nascimento e nenhum outro documento de identificação, não cursou escola, não tem empresa, não usa celular, não acessa a Internet, não tem conta e nem cartões bancários, etc. Só assim o Estado não sabe da existência, mas já inventou o RG escolar para as crianças, as carteirinhas de vacinação, a carteirinha do SUS (Sistema Único de Saúde), as carteirinhas de membros de igreja, as certidões de batismo, a Nota Fiscal Paulista, o CPF para crianças... tudo para forçar todos terem vários meios de serem identificados e rastreados em tempo real. Desse modo, a pessoa dizer que o chip é a marca da Besta seria o mesmo que dizer que todo mundo que tem Certidão de Nascimento, RG, CPF, CNH, conta ou cartão bancários ou de crédito tem a marca da Besta! E, detalhe, a Bíblia fala em marca da Besta (criatura espiritual) e não marca do Estado (homens).

Uma prova de que o chip subcutâneo é totalmente ineficaz para poder controlar quem pode e não pode comercializar ou celebrar contratos, é que o chip subcutâneo pode ser facilmente removido ou inutilizado pelo próprio usuário ou portador. Ainda mais, bastaria aos cristãos, com certa frequência (periodicidade) tirarem na sorte para ver quem iria colocar o chip provisoriamente somente para poder fazer uma grande compra para todos os irmãos (membros) locais terem alimentos, produtos de higiene e limpeza,

medicamentos, roupas, calçados, combustível, materiais escolares e de escritório, ferramentas e demais suprimentos para estocarem.

Ainda mais, o chip subcutâneo é inviável por questão de saúde. Por todo o lado estamos expostos às radiações emitidas por emissões de rádio e TV, das comunicações telefônicas (telefones sem fio e celulares), de Wi-Fi, de GPS e as produzidas pelas instalações e fiações elétricas. Em casa, pelas ruas, nos locais de trabalho ou de lazer, espaços comerciais e até nos hospitais. Toda esta radiação dos campos eletromagnéticos (CEM) é captada pelo nosso corpo induzindo correntes elétricas e campos oscilatórios que atrapalham nosso sistema bioelétrico, afetando o cérebro, o coração, o sistema circulatório e criando um ambiente hostil ao nosso sistema celular. As radiações dos CEM são genotóxicas e podem alterar o DNA de células débeis levando a doenças graves como o câncer. A irradiação eletromagnética prolongada sobre o corpo humano resulta em problemas como insônia, cansaço, dor de cabeça ou nas costas, alergia, distúrbios gastrintestinais, reumatismo, problemas pulmonares, depressão, falta de energia, fraqueza imunológica, distúrbios hormonais e do metabolismo, nervosismo, problemas cardíacos, falta de concentração, etc.

A pesquisa dos efeitos biológicos das radiações não-ionizantes (que não portam suficiente energia para poder romper os enlaces químicos) tem revelado que órgãos e sistemas orgânicos afetados por micro-ondas e radiofrequência são suscetíveis de distúrbios funcionais ou alterações estruturais. A maior parte da energia da radiação de micro-ondas ou radiofrequência absorvida por um sistema biológico se converte em calor (efeito térmico igual ao do aparelho micro-ondas), causando interferência no funcionamento do sistema vivo. Prejuízos resultantes de exposições a altos níveis de radiação foram estudados em animais, notando-se variações de lesões locais e necrose, até intensos estresses por hipertermia. Os efeitos não-térmicos ou específicos são mais difíceis de serem detectados que os térmicos. Nos testes com animais, lesões foram encontradas nos órgãos internos de animais expostos por prolongados períodos de tempo, durante os quais não se constatou nenhum aumento significativo da temperatura corporal nem foram observados sinais de desconforto. Os efeitos desse tipo mais frequentemente relatados são de ordem neurológica. Em animais, incluem mudanças nos reflexos condicionados, alterações da sensibilidade à luz, som

e estímulo olfativo, alterações nas biocorrentes do córtex cerebral e mudanças de comportamento. Inclusive, muitos sintomas subjetivos foram descritos em trabalhadores que lidam com equipamentos de micro-ondas.

Até mesmo a plaqueta militar de identificação (ou chapa de identificação), consistente numa chapinha de metal, com borda de borracha, presa numa corrente metálica para ser colocada no pescoço, é mais eficaz e prática do que o chip para fins de identificação humana em caso de acidente ou morte. Ressalta-se que as plaquetas de identificação usadas por militares possuem informações médicas básicas para tratamento (tipo sanguíneo e histórico de tratamentos: substâncias químicas, vacinas, alergias e afins). Poder-se-ia acrescentar um número identificador de prontuário médico, como, por exemplo, o número do Cartão do SUS - Sistema Único de Saúde (https://portaldocidadao.saude.gov.br/portalcidadao/index.htm). É muito melhor do que um simples crachá de plástico num colar de também de plástico ou de um chip subcutâneo porque o metal é bem mais resistente ao calor e ao fogo.

Outro detalhe. Se você usa um computador tipo PC (do inglês *Personal Computer*; ou seja, computador pessoal), saiba que ele é invenção da IBM, a qual inventou o sistema (máquina *hollerith*) de identificação, cadastramento, seleção, controle... dos judeus para os nazistas exterminarem nos campos de concentração. Assim, por esse prisma, você está usufruindo (e compactuando) da evolução de uma empresa e de um sistema co-responsável pelo holocausto. Do mesmo modo, considerando que na época do Nazismo os bancos informaram aos Nazistas quais clientes eram judeus e depois bloquearam todas as suas contas, poupanças, pagamentos, créditos, investimentos e aplicações financeiras e, posteriormente, repassaram todos esses valores para os nazistas; você, mesmo hoje, ser cliente de um banco te faria cúmplice dos nazistas e/ou te colocaria dentro do banco de dados do Anti-Cristo.

Também, o fato de você ser empresário, profissional liberal (autônomo), servidor público ou empregado de alguma pessoa, física ou jurídica, te coloca dentro do banco de dados do Estado e, portanto, do Anti-Cristo (futuro governante mundial); vez que tem que repassar ao Estado informações de identificação, localização, etc., que são cruciais para saber

que você existe, quem você é, o que você faz da vida, onde você pode ser encontrado, qual é o seu sustento, quem são seus familiares/parentes, qual é seu patrimônio, quais são e onde estão suas economias, etc.

Portanto, quem acredita que a marca da Besta é um microchip, é um hipócrita se possui ou usa computador, se tem conta bancária, se tem cartão de crédito, se tem *smartphone*, etc.

O Anti-Cristo não vai precisar de que você tenha cadastrado suas digitais eletronicamente (pelo Detran, pelo TSE, etc.). Uma, porque o Estado já tem suas digitais na ficha cadastral do RG (você já as forneceu, por isso de nada adianta agora se recusar a escaneá-las) e, assim, é só o Estado as escanear (o que nos Estados Unidos já é assim há décadas). Duas, porque mesmo que você não possua nenhum documento de identificação (com ou sem digitais), o ministro/líder espiritual da sua denominação religiosa (pessoa jurídica com CNPJ) vai te "dedurar" (delatar o denunciar) ao Estado; ou seja, os dados que você passa para a denominação religiosa para poder ter a carteirinha de membro serão repassados ao Estado.

Em maio de 2011, o governo norte-americano rastreou e localizou o esconderijo de Osama bin Laden e o matou sem ser necessário um chip. O recurso utilizado consistiu em identificar uma voz num telefonema de celular durante alguns segundos.

Em junho de 2013, Edward Joseph Snowden, revelou ao mundo que o governo norte-americano espionava tudo e todos; ou seja, não havia nenhuma privacidade, sigilo ou restrição. E, detalhe, não foi preciso implantar microchips em ninguém para isso.

Nem mesmo os governos conseguem ter sigilo. **WikiLeaks** (https://wikileaks.org/) é uma organização independente e sem fins lucrativos, liderado pelo australiano Julian Assange, que publica postagens de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis. Desde que a WikiLeaks surgiu, em 2006, uma série de documentos importantes, e constrangedores para governos de muitos países, principalmente para o governo dos Estados Unidos da América (EUA), vieram à tona. Dentre esses documentos,

destacam-se os que divulgaram as instruções de como tratar os prisioneiros da base norte-americana de Guantánamo, em Cuba; um vídeo que mostra um helicóptero americano alvejando repórteres estrangeiros que cobriam a Guerra do Iraque, ou, ainda, os inúmeros documentos acerca das operações militares dos EUA no Afeganistão e no Iraque, nos quais há relatos de torturas e de ataques a alvos civis. O OpenLeaks (http://www.openleaks.org/) é outro site semelhante ao WikiLeaks.

O **jogo Pokémon GO**, por exemplo, já espiona facilmente todo mundo. Ele foi idealizado pelo desenvolvedor Satoru Iwata e pelo CEO - *Chief Executive Officer* (diretor executivo ou presidente) da Pokémon Company, Tsunekazu Ishihara, que convidou John Hanke para fazer parte do projeto. John Hanke, que fundou a Niantic (responsável pela tecnologia de realidade aumentada utilizada em Pokémon GO) e a Keyhole, Inc. (criada em 2001 com o propósito de desenvolver um software que visualizava dados geoespaciais). Até então a Niantic havia lançado o jogo Ingress, que tem como objetivo utilizar a realidade aumentada para encontrar portais fictícios em lugares reais, como monumentos, igrejas, entre outros. Foi com os dados do *game* (jogo) *Ingress* que a equipe de Hanke decidiu quais seriam os melhores *pokestops*.

- http://www.pokemongobrasil.com/;
- https://play.google.com/store/apps/details?id=com.nianticlabs.pokemongo&hl=pt_BR.

A Keyhole é um projeto de mapeamento de superfícies, foi comprada pelo Google e usado para fazer o Google Maps/Earth e Street View. Essa Keyhole foi patrocinada pela empresa In-Q-tel, que foi fundada pela CIA em 1999.

A In-Q-tel é uma incubadora de startups com o objetivo dessas tecnologias serem aproveitadas pela central de inteligência americana (CIA). A Keyhole recebeu investimentos da In-Q-tel em 2003 especificamente para que a CIA utilizasse a tecnologia da *startup* para fazer mapeamentos durante a Guerra do Iraque. Em 2004, a empresa de Hanke foi comprada pelo Google e o software desenvolvido por ela foi utilizado para criar o Google Street View (que coletou imagens completas de vários países

e informações a partir das redes de Wi-Fi (wireless) dos usuários [Wi-Spy]). Portanto, a CIA indiretamente já tinha acesso a todos os mapas do planeta, mas, ainda, não conseguia entrar dentro das residências e demais estabelecimentos. Para poder jogar o Pokémon GO é necessário dar permissão para o aplicativo poder acessar a identidade e localização, bem como usar a câmera, GPS, microfone, conexão Bluetooth e até os dispositivos USB que estiverem conectados ao smartphone. E, ainda, nos termos do jogo consta que: "Nós cooperamos com agências do governo e companhias privadas. Podemos revelar qualquer informação a seu respeito ou dos seus filhos; Nosso programa não permite a opção 'Do not track' ('Não me espie') do seu navegador".

Entretanto, todas as redes sociais (Facebook, WhatsApp, Twitter, Google +, etc.) sondam, espiam, analisam, coletam dados, traçam perfil, vendem informações dos usuários e fornecem tais dados, inclusive a localização, para os governos, a Justiça e investigações policiais. E, as permissões concedidas para a instalação do Pokémon GO são idênticas as requeridas em aplicativos como, por exemplo, o Facebook, Instagram e muitos outros.

O **Facebook** permite que o usuário edite com certa liberdade os detalhes que coleta sobre a sua personalidade. Para ter acesso ao "dossiê", basta ir até https://www.facebook.com/ads/preferences e conferir suas Preferências de Anúncios.

Portanto, quem quer privacidade não pode ter aparelho celular e, muito menos, uma conta no Facebook ou qualquer outra rede social. Até mesmo um simples acesso à Internet revela informações do usuário.

Quais dessas pessoas paranoicas com o microchip não utilizam *smartphones* e nem as redes sociais? Se fossem sinceras com dita crença, não usariam nenhuma dessas coisas. Mas são hipócritas. Como podem elas não viverem o que professam, mas quererem que os outros vivam?

Ao contrário das previsões desses religiosos, os sistemas de pagamentos evoluíram para a desmaterialização e métodos não invasivos (vez que num implante de chip há possibilidade de rejeição do organismo e até mesmo contaminações). Os caixas eletrônicos já possuem leitores de impressões

digitais e os aparelhos celulares já viraram agências bancárias completas. Mas até agora não há sequer nenhum rascunho de projeto de implante de chip na testa das pessoas.

Justamente as criptomoedas, por serem descentralizadas (não serem emitidas ou controladas por nenhum banco central), serem privadas (particulares e não estatais ou governamentais) e nem sequer serem regulamentadas, não sofrem o controle estatal (regras, imposições, restrições, declarações, rastreios, etc.). Desta forma são ideais para quem tem medo de ser proibido de comprar e de vender; ainda mais que referidas moedas envolvem anonimato e sigilo, com o que não se sabe sequer a identidade do usuário, muito menos qual é a sua crença religiosa ou sua aparência. Portanto, os partidários do pavor coletivo de serem proibidos de comprar e de vender (a turma da chipfobia) deveriam ser os maiores apoiadores, entusiastas e patrocinadores das criptomoedas. Mas, contraditoriamente, ou eles sequer imaginam que tais coisas existam, ou as abominam completamente. Provavelmente, após décadas professando que os chips seriam a marca da Besta, devem estar reformulando a interpretação equivocada para ajustá-la às criptomoedas. Esse procedimento é muito comum na Mídia / Imprensa vendida e na militância comunista; ou seja, sempre procuram algo sensacionalista, comovente ou atrativo para prender e desviar a atenção das pessoas para que não percebam o que está acontecendo "bem debaixo de seus narizes". Por outras palavras, quem defende a tese de um Anti-Cristo *high-tech* ou é mal-intencionado ou é, no mínimo, ignorante. Até poderíamos considerar como plausível a tese de que os demônios poderiam incorporar-se em máquinas para poderem matarem os humanos (apesar de que os demônios não precisam desse recurso para poderem matar os humanos), mas acreditar que o Anti-Cristo iria obrigar a todos instalarem um chip subcutâneo ou uma tornozeleira eletrônica ou rastreadora já beira à insanidade. Falsos profetas são conhecidos por terem o hábito de rapidamente retificarem, revisarem ou reajustarem suas profecias furadas para não dar tempo para as pessoas perceberem que não aconteceu o que eles pregaram como sendo a Palavra de Deus. Uma pessoa sincera e bem-intencionada iria admitir seu erro e confessar que estava enganada.

Qual o efeito prático contra o Anti-Cristo da pessoa não ter sua digital escaneada voluntariamente ou não ter um chip de identificação? Nenhum!

Sem sua digital escaneada voluntariamente ou sem você ter um chip de identificação, por acaso, isso te tornará invisível ao Anti-Cristo? Não! Porventura isso impediria o Anti-Cristo de saber que você existe, quem você é, onde pode te encontrar, o que você faz da vida, qual é seu sustento...? Não!

Por ventura o Anti-Cristo não sabe identificar quem é cristão e quem não é? Claro que sabe! Qualquer reles demônio saber fazer isso.

A marca da Besta é invisível e espiritual. Por ser espiritual, pode passar despercebida e levar à condenação das almas. A marca da Besta é imposta às pessoas por Satanás e não pelos homens. Também não é feita para ser usada pelos homens, mas sim para levar espiritualmente as almas a se condenarem. **Se o chip é para ser implantado na mão, porque é que então o Apocalipse nos diz que será implantado também na fronte?**

A lenda do chip ser a marca da Besta não explica nada sobre a marca na testa/fronte. Portanto, despreza parte da Palavra profética de Deus. Só se prende nas frases "marca na mão" e "não poder comprar" e ignora todo o restante da profecia bíblica. Atitude nada cristã. Qual seria o sinal da testa pela ótica de quem condena a biometria? Será que pensam que algumas pessoas iriam implantar um chip na testa?

Deus não dá revelações pela metade! Quem aplica e usa as Palavras de Deus pela metade é o diabo! Como Deus colocou essa parte (sinal na testa) do texto profético é porque ele tem significado e não está ali sem motivo, sem razão, sem importância, à toa, etc. Está ali para evitar que demos ouvidos a interpretações equivocadas! Toda interpretação da marca da Besta que não explica o sinal na testa, está errada!

O deixar implantar o chip na mão, não é prova e motivo inequívoco de condenação. Da mesma maneira que usar o cartão de crédito, não é motivo de condenação. Da mesma maneira que, muitos que não foram ainda implantados como chip se condenaram ao inferno. Não há uma relação de causa e efeito, logo, o chip não é a marca da Besta.

Quem a credita de que o chipezinho é a marca da Besta, com ele se preocupa, e sem dar por isso, é capaz de se deixar marcar com a verdadeira marca da Besta, se já não está marcado.

Estando as pessoas a ser bombardeadas com a advertência de não deixarem implantar o Verichip na mão, porque se condenarão, não estão advertidas para o verdadeiro perigo da marca espiritual que o demônio aplica na mão e na fronte, em termos espirituais e simbólicos.

O cristão que tiver sua digital escaneada voluntariamente ou ter um chip de identificação vai poder comprar e vender? Não!!! Vai estar com a marca da besta? Não!!!

Quando a Bíblia fala sobre o julgamento divino diante do trono branco e em separar as ovelhas dos bodes, o joio do trigo, os justos dos injustos... não menciona nada sobre as pessoas terem, ou não, uma marca física, material ou visível na mão ou na testa; mas, pelo contrário, fala expressamente que somos julgados pelas nossas crenças (cabeça) e frutos/obras (mãos)! Ou, por caso, o chip ou a leitura biométrica vai/vão existir nas almas/espíritos dos ímpios mortos para poderem ser identificados e condenados por Deus? Claro que não!

Claro que é mais fácil o Anti-Cristo impor aos seus que usem um símbolo distintivo do que impor aos de Deus que usem um símbolo diferenciador, mas esse sinal não precisa ser material ou físico, pois um soldado do Anti-Cristo facilmente reconhece o outro pelo linguajar, pelos hábitos, pela exteriorização da fé, etc. Na verdade, como todos os demônios se conhecem, falam a mesma língua, estão do mesmo lado (fazem parte do mesmo exército ou jogam no mesmo time) e se identificam de longe, não existe nenhuma necessidade de precisarem de crachás.

Hitler (nazismo), apesar de ter colocado a estrela de Davi nos ombros dos judeus, não precisava disso, pois sem grandes dificuldades conseguia identificar um judeu pela sua fisionomia, pelo seu nome, pelos seus hábitos, pela exteriorização de sua fé, etc. Além do que bastava os agentes do governo nazista irem até as sinagogas (templo judaico). Outra observação, a Bíblia diz que a Besta marcará apenas os seus e não os de Deus. Hitler

marcou suas vítimas e não seus seguidores. Os nazistas não precisavam usar uma suástica para serem reconhecidos como nazistas, nem os judeus precisavam da estrela de Davi para serem tidos como judeus.

É muito mais fácil e prático ao Anti-Cristo impor aos seus que usem um símbolo distintivo do que impor aos de Deus que usem um símbolo diferenciador; mas esse sinal não precisa ser material ou físico, pois um soldado do Anti-Cristo facilmente reconhece o outro pelo linguajar, pelos hábitos, pela exteriorização da fé, pelos locais que frequenta, etc.

No passado quando os católicos promoveram as inquisições e cruzadas, não precisaram colocar nenhuma marca física nem em seus adversários para poderem reconhecê-los e nem neles mesmos para serem reconhecidos, pois pela exteriorização de suas crenças conseguiram facilmente identificar e serem identificados.

Nos conflitos entre árabes, palestinos, mulçumanos... contra os judeus/Israel, os inimigos de Israel normalmente não usam marcas físicas ou materiais distintivas; mas, pelo contrário, se infiltram no meio dos judeus e acionam bombas. Os inimigos de Israel não precisam e nem usam nenhuma marca ou sinal para poderem saber identificar um judeu. Do mesmo modo, os judeus não precisam e nem usam nenhuma marca ou sinal para poderem saber identificar seus inimigos.

Durante as inquisições e cruzadas não foi preciso nenhum meio sofisticado para poder excomungar os ditos hereges e infiéis da ICAR (Igreja Católica Apostólica Romana). Bastava apenas o papa excomungar a pessoa, que nenhum dos fiéis da ICAR os concedia abrigo, comida, trabalho, ajuda...

Besta é um animal ou um poder. E na profecia um animal simboliza um reino ou poder estatal (Daniel 7:17, 23 e 8:20-21); bem como o seu líder principal. Existiu um período em que “a Besta não é” um reino. E o último período em que “a Besta voltou a ser” um reino. A Besta “não é”, ela “era”, mas agora “não é”. O que isto significa? Está se referindo a um cargo ou título de autoridade ou poder que possui sucessão. Entretanto, a Igreja cristã primitiva tinha unicamente a liderança do Espírito Santo e não uma liderança

humana (Salmos 48:18; João 16:13; Romanos 8:14 e Mateus 15:14). Não existe, portanto, tal coisa de sucessão do "trono de Pedro". Pedro nunca reinou ou teve trono na Igreja (Salmos 45:6 e Hebreus 1:8) e nunca foi considerado autoridade máxima na Igreja (Gálatas 2:2,11,14 e II Pedro 3:15-16), como também Davi não foi (II Samuel 12:1-14); ambos e todos, eram submissos à Palavra de Deus é principalmente na forma de revelação Divina. Quando Israel quis um rei (um homem), para governar sobre eles (como as nações [pagãos] ao redor deles tinham – I Samuel 8:5,19-20), eles estavam desprezando a liderança do Espírito Santo sobre eles (I Samuel 8:7; 12:12 e Isaías 33:22), além de desobedecerem Levítico 20:23. Portanto, não há eleição, votação, sucessão... feita pelos homens em relação aos ungidos de Deus. É Deus quem escolhe quem Ele vai usar, ungir, manifestar sua Palavra, dar a revelação Divina, etc., como, onde e quando, e não os homens por eleição humana, como na política (I Samuel 16:1-13 e Atos 26:15-18). Prosseguindo, um rei precisa ter três coisas para ser rei: Primeiro, uma coroa. Rei sem coroa não é Rei. Segundo, o rei precisa ter súditos, afinal de contas ninguém pode ser rei dele mesmo. Rei é quem governa sobre outras pessoas. Terceiro, por fim, ele tem que ter um território reconhecido, autônomo e soberano. A ICAR (Igreja Católica Apostólica Romana) foi a primeira denominação religiosa (pessoa jurídica religiosa) da cristandade, contrariando os cristãos e os apóstolos que nunca erigiram nomenclaturas, denominações, pessoas jurídicas, organizações, etc. ("tens nome de que vives, mas está morto" – Apocalipse 3:1 e Efésios 5:14). Em outras palavras, a ICAR foi a primeira rejeitar o Espírito Santo ao se tornar uma organização religiosa (leia-se: liderança humana - Mateus 15:8-9, Jeremias 17:5, II Timóteo 4:3-4 e Colossenses 2:8), o que significa desprezo à liderança do Espírito Santo (João 16:13, Atos 10:19-20, 13:2 e 16:6 e Romanos 8:14).

- http://igrejacibernetica.blogspot.com.br/2015/05/a-denominificacao-da-igreja-nomes-de.html.

O **prefixo "anti"** também possui o significado: "em lugar de", "o que aniquila os efeitos de", "do, ou pelo lado oposto" ou "face oposta". A **palavra anti-Cristo** significa aquele que é contra Cristo, ou seja, seu opositor, inimigo, adversário, adverso, contrário, oposto, concorrente, rival, sabotador, antagônico, incompatível, inconciliável, combatente, avesso, contendor, hostilizador, antipático, que ou quem prejudica ou causa dano.

A Bíblia apresenta uma **variação de nomes e títulos específicos para o Maligno** (é descrito com pronomes pessoais - Jó [e não João] 1:6). Vejamos alguns:

1) Satanás ou Satã = "adversário" (Mt 4:10 e Jó 1) ou "opositor" (Zacarias 3:1). É uma transliteração do hebraico satan, indicando um acusador no sentido legal, um queixoso que tem uma acusação a apresentar. Em Zacarias [Zc] 3:1 lemos: "Deus me mostrou o sumo sacerdote Josué, o qual estava diante do Anjo do SENHOR, e Satanás estava à mão direita dele, para se lhe opor." Numa palavra, Satanás se opõe a nós, trabalha contra nós, ou "nos persegue", na tentativa de nos derrotar espiritual e moralmente;
2) Diabo = difamador, acusador ou caluniador (Mateus [Mt] 4:1, I Pedro [Pe] 5:8, Ap 12:10, Zacarias 3:1-5 e Jó 2:4-5);
3) Belzebú (Baalzebub) = "senhor da casa" (Mt 12;26-27). O nome passou por várias modificações entre os pagãos, como: "deus das moscas", "o senhor do esterqueiro". Entre os judeus do tempo de Cristo, era considerado o príncipe dos demônios (Mt 10:25 e 12:24,27 e Marcos [Mc] 3:22);
4) Demônio = anti-Deus. O prefixo vertido para o grego significa: "em lugar de". Assim, sem ser Deus, quer passar-se por Deus e receber o culto divino. Isaias 13:21-22 e 34:12-14 referem-se aos demônios com os nomes ou expressões: "feras do deserto", "horríveis animais", "feras que uivarão umas às outras", "dragões", "cães bravos" e "animais noturnos". A versão grega do Velho Testamento (Septuaginta), verte como demônios;
5) Sacir = "bode peludo, hirsuto". É o texto hebraico, que na Septuaginta é traduzido por demônio, mas com esta característica;
6) Lúcifer - velha palavra latina que originalmente significava "portador da luz" ou “filho da Alva” (Isaías 14:12);
7) Adversário – “O diabo, vosso adversário, anda em derredor, como leão que ruge procurando alguém para devorar" (I Pedro [Pe] 5:8);
8) Belial = desprezível (II Coríntios 6:15 e II Samuel [Sm] 23:6);
9) Maligno (Mt 13:19, João 17:15 e II Coríntios [Cor] 6:15);
10) Tentador (Mt 4:3 e Tessalonicenses [Ts] 3:5);
11) Príncipe/deus deste mundo (João 12:31 e 16:11);
12) Príncipe das potestades do ar (Efésios 2:1-2);
13) deus deste século (II Coríntios [Cor] 4:4);
14) Acusador de nossos irmãos (Apocalipse [Ap] 12:10);
15) Ladrão (João [Jo] 10:10);
16) Homicida e Mentiroso (Gênesis [Gn] 4:8 e João 8:44);
17) Pai da mentira (João 8:44);
18) Destruidor ou Apoliom (Ap 9:11);
19) Manipulador = ele tenta levar-nos a pensar que ele e/ou Deus não existe(m) (Ap 20:10);
20) Governador das trevas (Efésios [Ef] 6:12);
21) Amo/senhor dos pecadores (Atos 8:23 e 26:18);
22) Príncipe dos demônios (Mateus [Mt] 12:24);
23) Dragão (Ap 12:3,7,9);
24) Serpente (Ap 12;9);
25) Inimigo (Mt 13:28);
26) Besta;
27) Falso profeta;
28) Anti-Cristo.

Lúcifer era um querubim da guarda real (Ezequiel [Ez] 28:14, Gênesis [Gn] 3:24 e Ez 1:4-24 e 10:1-2). Estava na sala do trono de Deus. Estava dentro da corte celestial (Jó 1:6). Fazia parte do Exército do Senhor. Estava, portanto, continuamente junto a Deus... mas, seu coração o levou à pensar que poderia tomar o trono de Deus, por lhe estar tão próximo, conhecê-lo intimamente (face à face) e saber seus desígnios e, por, também, conhecer as fraquezas, desejos, limitações e insatisfações de seus anjos... (tais como não sentirem os prazeres da carne - sexo, paladar, adrenalina, tato, etc. - e terem que servirem a criaturas inferiores = homens), mas fracassou sua rebelião e ele, com todos os que lhe deram ouvidos (um terço dos anjos), foram banidos das regiões celestes (Isaías [Is] 14:12-14, Apocalipse [Ap] 12:7-9, Lucas [Lc] 10:18, Mateus [Mt] 25:41, II Pedro [Pe] 2:4 e Judas [Jd] 6). **Este histórico da atitude de Satanás nos ajuda a visualizarmos sua presença e atuação na Igreja de Jesus Cristo desde antes de sua fundação**.

Depois do Criador (Deus) e seus anjos (corte celestial), não há quem mais saiba de cor e salteado, de trás para frente, não só o teor das Escrituras, mas o seu significado como Satanás e seus demônios; vez que eles eram anjos de luz e estavam continuamente na presença de Deus e, inclusive, testemunharam a Criação. Assim, por outras palavras, desde o primórdio da Criação, o Opositor estava presente, não só presenciando tudo, mas ciente dos desígnios/planos de Deus e, como uma cobra pronta para o bote, ficava vigilante aguardando pelo momento propício de, sorrateiramente, sabotar, envenenar, corromper, contaminar, destruir, atrapalhar, etc.

Satanás é um traidor e a traição sempre vem de dentro! Ele estava o tempo todo com Deus, mas em seu coração já planejava liderar uma rebelião contra Deus. Recorde-se de Judas Iscariotes que estava o tempo todo com Cristo e quando julgou pertinente mostrou sua verdadeira natureza.

O querubim transformou-se em Satanás quando tentou usurpar a autoridade de Deus, competir com Deus e assim tornou-se adversário de Deus. A inveja e a rebeldia foram algumas das causas da queda de Satanás.

> "**Como caíste desde o céu, ó estrela da manhã**, filha da alva! Como foste cortado por terra, tu que debilitavas as nações!

E tu **dizias no teu coração: Eu subirei ao céu, acima das estrelas de Deus exaltarei o meu trono**, e no monte da congregação me assentarei, aos lados do norte.

Subirei sobre as alturas das nuvens, e serei semelhante ao Altíssimo.

E contudo levado serás ao inferno, ao mais profundo do abismo.

Os que te virem te contemplarão, considerar-te-ão, e dirão: É este o homem que fazia estremecer a terra e que fazia tremer os reinos?

Que punha o mundo como o deserto, e assolava as suas cidades? Que não abria a casa de seus cativos?" (Isaías 14:12-17). Grifos nossos.

"7 E houve batalha no céu; Miguel e os seus anjos batalhavam contra o dragão, e batalhavam o dragão e os seus anjos;

8 Mas não prevaleceram, nem mais o seu lugar se achou nos céus.

9 E foi precipitado **o grande dragão, a antiga serpente, chamada o Diabo, e Satanás, que engana todo o mundo**; ele foi precipitado na terra, e os seus anjos foram lançados com ele.

10 E ouvi uma grande voz no céu, que dizia: Agora é chegada a salvação, e a força, e o reino do nosso Deus, e o poder do seu Cristo; porque já o **acusador de nossos irmãos** é derrubado, o qual diante do nosso Deus os acusava de dia e de noite." (Apocalipse 12:7-10). Grifos nossos.

"E disse-lhes: **Eu via Satanás, como raio, cair do céu**." (Lucas 10:18). Grifos nossos.

"E aos **anjos que não guardaram o seu principado**, mas deixaram a sua própria habitação, reservou na escuridão e em prisões eternas até ao juízo daquele grande dia;" (Judas 1:6). Grifos nossos.

Usurpação é o apoderamento ilícito de coisas, bens, títulos, estado, autoridade, etc.; ou seja, é se apoderar por violência ou meios injustos daquilo que não lhe pertence ou a que não tem direito. É exercer cargo, função, título, etc., indevidamente (pela força, sem direito, por fraude, por artifício, etc.). Assim, por exemplo, os termos "estrela da manhã" e "estrela da alva" se aplicam a Jesus (Apocalipse 22:16); mas, como Lúcifer tenta usurpar o poder, autoridade, trono, adoração... de Deus, também tenta atribuir a si os títulos de Deus, como estes (Isaias 14:2).

Não se pode confundir a palavra "vigário" com "sacerdote" ou "ministro". A palavra "vigário" significa "aquele que substitui outro"; ou seja, que toma o lugar de outra pessoa. Sacerdote é quem oferece sacrifícios à divindade e ministra os sacramentos. Já a palavra "ministro" deriva do termo latino "minister" (de *minus*, menor), que indicava genericamente uma pessoa subordinada a outra, a qual era o magister (mestre, de *magis*, maior). Na Bíblia os principais alunos ou aprendizes (discípulos) de Cristo eram chamados de apóstolos e os demais de seguidores, discípulos ou servos de Cristo. Por causa disso Jesus disse em João 5:43 que como Ele veio no nome de seu Pai, ou seja, Jesus (João 17:11), os ímpios (filhos do Diabo, os

que não são eleitos de Deus, os que não reconhecem a Luz e nem a voz de Deus) não o aceitaram; mas aceitariam (e aceitaram) outro que viesse (e veio) em seu próprio nome (um homem usurpando o lugar de Deus), e não no nome de Deus. Uma vez que o Cristo não possui um próprio nome, mas o de seu Pai; um homem vindo, em seu próprio nome, exigindo reverência a si, está colocando-se no lugar de Cristo.

Por outras palavras, como Deus se fez carne e habitou entre nós, o diabo quer fazer sua versão pervertida; ou seja, o diabo quer tomar uma forma carnal e assumir o governo mundial.

Desse modo, trata-se de uma batalha entre seres (pessoas) espirituais; os quais são muito superiores aos seres humanos em longevidade, inteligência, conhecimento, ciência e poder.

> "Nós somos de Deus; aquele que conhece a Deus ouve-nos; aquele que não é de Deus não nos ouve. Nisto conhecemos nós o **espírito da verdade e o espírito do erro**." (I João 4:6). Grifo nosso.

> "Porque nós **não estamos lutando contra gente feita de carne e sangue, mas contra pessoas sem corpo – os reis malignos do mundo invisível**, esses poderosos seres satânicos e grandes príncipes malignos das trevas **que governam este mundo**, e contra um número tremendo de maus espíritos no mundo espiritual" (Efésios [Ef] 6:12). Grifo nosso.

Durante a grande tribulação promovida pelo Anti-Cristo, os seus soldados não irão fazer como nos filmes de ficção evangélicos onde os mostram forçando a pessoa a dizer literalmente que nega a Jesus. Acaso a Igreja Católica Apostólica Romana (ICAR) fez isso durante a Inquisição? Não! Ela forçava a aceitarem o conceito (dogma, credo, doutrina, catecismo, etc.) dela de Jesus e do Cristianismo. Assim o Anti-Cristo irá impor o conceito dele de Deus e religião sob inúmeras desculpas, tais como: promover a paz mundial, em prol dos direitos humanos, combater a violência, proteger o meio ambiente, proteger os animais, combater o terrorismo e as guerras, combater a descriminação e o preconceito, o fanatismo religioso, os radicais, o satanismo, as heresias, etc. **Irá discreta e sutilmente impor um deus e evangelho diferentes dos que pregaram os apóstolos (Gálatas 1:8 e II Coríntios 11:4). A bem da verdade, já está pregando isso há muito tempo, mas o Anti-Cristo ainda não se manifestou (se revelou) em forma humana.**

É muito mais fácil e comum negar a Jesus do que se pensa. Quantas pessoas negam Jesus todos os dias? Chamar Jesus de Senhor, mas ignorar ou desprezar a Sua Palavra, é negar-Lhe! Não acreditar em Sua Palavra é negar-Lhe! Acreditar na palavra do diabo é negar a Jesus! Colocar algo (dinheiro, emprego, cargo, empresa, poder, fama, títulos, instituição, pátria, família, etc.) ou alguém acima de Jesus é negar-Lhe (Marcos 12:30, Mateus 6:24, Lucas 16:13)! Amar a si mesmo ou a outrem mais do que a Jesus, é rejeitá-Lo (Mateus 10:37)! Não viver a Palavra de Jesus, é negá-lo! Invocar outro nome em oração, graças, louvor ou adoração, é negar a Jesus! Não negar a si mesmo é recusar a Jesus (Mateus 16:24, Marcos 8:34 e Lucas 9:23)! Não se sujeitar totalmente a Jesus, é negá-Lo! Se entregar ou satisfazer a vontade da carne, é negar a Jesus! Amar a este mundo atual (secular ou material) é negar a Jesus (I João 2:15)!

> **"Nem todo o que me diz: Senhor, Senhor! entrará no reino dos céus, mas aquele que faz a vontade de meu Pai, que está nos céus."** (Mateus 7:21).

Negar a Jesus é invocar outro nome no lugar do Dele ou junto ao Dele; é servir, cultuar e/ou adorar algum deus, divindade, criatura, entidade, objeto ou pessoa; é orar a outra pessoa ou a mais uma pessoa; é desobedecer sua Palavra; é negar que O conhece como Pedro fez antes de receber o batismo do Espírito Santo; é ter vergonha Dele e/ou de Sua Palavra; é ter vergonha de algum irmão em Cristo; é ter intimidade com o maligno; é comungar das coisas do mundo; é praticar idolatria; é trocar a liderança do Espírito Santo por outro tipo de liderança; é desprezar o Espírito Santo; é blasfemar; é fazer e/ou tocar as coisas tidas por imundas e abomináveis por Deus; é distorcer a Pessoa e/ou a Palavra de Jesus; é negar a divindade de Jesus; é negar que Jesus veio em carne; é não crer na eficácia do sangue de Jesus; é trocar as Escrituras Sagradas por teologia, palavras dos homens ou pela ciência (sabedoria humana); é acreditar em tradições, fábulas, lendas, mitologia, folclore, simpatia, magia, feitiços, adivinhações, sortilégios, prognósticos... Em síntese é não permanecer com Jesus e Sua Palavra.

Entretanto, **não se pode confundir anti-Cristos com O Anti-Cristo.** Todo aquele que nega Jesus ou as palavras de Jesus é um anti-Cristo, mas somente um homem pode ser O Anti-Cristo, o diabo encarnado.

"Quem é o mentiroso, senão aquele que nega que Jesus é o Cristo? **É o anticristo esse mesmo que nega o Pai e o Filho**." (I João 2:22).

"Porque já **muitos enganadores** entraram no mundo, os quais não confessam que Jesus Cristo veio em carne. **Este tal é o enganador e o anticristo**." (II João 1:7).

"Porque **surgirão falsos cristos** e falsos profetas, e farão tão grandes sinais e prodígios que, se possível fora, enganariam até os escolhidos." (Mateus [Mt] 24:24).

"Porque **muitos** há, dos quais muitas vezes vos disse, e agora também digo, chorando, que são **inimigos da cruz** de Cristo" (Filipenses [Fp] 3:18).

"Adúlteros e adúlteras, não sabeis vós que **a amizade do mundo é inimizade contra Deus**? Portanto, qualquer que quiser ser amigo do mundo constitui-se inimigo de Deus." (Tiago [Tg] 4:4).

Portanto, ser anti-Cristo é ser Anti-Palavra, pois Jesus é a Palavra Viva de Deus (Hebreus 4:12); ou seja, é ir contra as Escrituras Sagradas (Bíblia). É colocar filosofia, ciência, credos, dogmas, mitos, lendas, fábulas, gnosticismo, astrologia, misticismo, paganismo, etc. no lugar da Palavra de Deus.

"No princípio era o Verbo, e o Verbo estava com Deus, e o Verbo era Deus." (João 1:1).

"E o Verbo se fez carne, e habitou entre nós, e vimos a sua glória, como a glória do unigênito do Pai, cheio de graça e de verdade." (João 1:14).

"E estava vestido de uma veste salpicada de sangue; e o nome pelo qual se chama é a Palavra de Deus." (Apocalipse [Ap] 19:13).

O Apocalipse adverte que **o Anti-Cristo vem parecendo um cordeiro** (Apocalipse 13:11). Isso significa o Anti-Cristo personificando, falsificando, fingindo... ser ungido de Deus (Mt 24:24); pois o verdadeiro Cordeiro é Jesus (João 1:36; I Pedro 1:19 e Apocalipse 17:14 e 7:14). Portanto, **o Anti-Cristo (ser espiritual) tem que se incorporar num líder religioso que finja pregar a Cristo Jesus, mas na verdade afasta as pessoas Dele (promove a apostasia)** e persegue os verdadeiros adoradores de Jesus, taxando-os de hereges, como a Igreja Católica já fez várias vezes no passado (Santo Ofício, Inquisições e Cruzadas).

Mateus 7:15 – "Acautelai-vos, porém, dos falsos profetas, que **vêm até vós vestidos como ovelhas**, mas, interiormente, são lobos devoradores.".

Lucas 6:26 - 'Ai de vós quando todos os homens de vós disserem bem, porque assim faziam seus pais aos falsos profetas.".

II Coríntios 11:13-15 – “Porque tais falsos apóstolos são obreiros fraudulentos, transfigurando-se em apóstolos de Cristo. E não é maravilha, porque **o próprio Satanás se transfigura em anjo de luz. Não é muito, pois, que os seus ministros se transfigurem em ministros da justiça**; o fim dos quais será conforme as suas obras.”.

Em reforço a Bíblia adverte que o Anti-Cristo, apesar da aparência de Cordeiro, fala como dragão. Isso significa que está possuído por Satanás (Ap 12:9 e 20:2) e, por isso, possui a mesma personalidade dele (arrogância, prepotência, insolência, violência, assassino, ladrão, mentiroso, cruel, sanguinário, impiedoso, falso, usurpador, rico, inteligente, etc.); vez que dele recebeu poder (Ap 13:2), e, principalmente, distorce as Escrituras, como fez no princípio enganando Eva (I Tim 6:3-5; Rom 3:4; Gal 1:8; Mt 15:8-9; Jr 17:5), persegue os cristãos (Ap 12:17) e difama os santos (Ap 13:56); ou seja, fala como se representasse os santos, mas profere blasfêmias e foram eles mesmo que mataram os santos (Mt 23:29-31). Portanto, há de ser uma pessoa religiosa ou espiritual que finja pregar a Cristo Jesus, mas na Verdade afasta as pessoas Dele (apostasia) e persegue os verdadeiros adoradores de Jesus.

A Bíblia ensina que uma das premissas necessárias para a manifestação do Anti-Cristo é a ocorrência da apostasia (e não o ceticismo, o ateísmo, o paganismo, etc.); portanto, o Anti-Cristo envolve a deturpação, distorção, adulteração, perversão... do Cristianismo.

"Ninguém de maneira alguma vos engane; porque não será assim sem que antes venha a apostasia, e se manifeste o homem do pecado, o filho da perdição, O qual se opõe, e se levanta contra tudo o que se chama Deus, ou se adora; de sorte que se assentará, como Deus, no templo de Deus, querendo parecer Deus." (II Tessalonicenses 2:3-4).

“MAS o Espírito expressamente diz que nos últimos tempos apostatarão alguns da fé, dando ouvidos a espíritos enganadores, e a doutrinas de demônios; Pela hipocrisia de homens que falam mentiras, tendo cauterizada a sua própria consciência; Proibindo o casamento, e ordenando a abstinência dos alimentos que Deus criou para os fiéis, e para os que conhecem a verdade, a fim de usarem deles com ações de graças;” (I Timóteo 4:1-3).

“E TAMBÉM houve entre o povo falsos profetas, como entre vós haverá também falsos doutores, que introduzirão encobertamente heresias de perdição, e negarão o Senhor que os resgatou, trazendo sobre si mesmos repentina perdição. E muitos seguirão as suas dissoluções, pelos quais será blasfemado o caminho da verdade.” (II Pedro 2:1-2).

O verbo **“apostatar”**, considerando sua raiz semântica, está relacionado à ideia de “afastar-se de algo”. Apostasia, dentro do contexto bíblico, é o

desvio ou afastamento consciente da verdadeira fé. Consequentemente, vemos aqui uma reação em cadeia: a multiplicação crescente da iniquidade (Mateus 24:12), gera uma apostasia de grandes proporções (II Tessalonicenses 2:3), a qual, por sua vez, tornará propicia a revelação do anticristo. Podemos afirmar que o surgimento e revelação do anticristo estão intimamente ligados ao desvio da verdadeira fé por parte de muitos.

No Apocalipse consta que o Anti-Cristo usa do “vinho” (doutrina falsa, ensinamento apóstata, ensinamento demoníaco...) para entorpecer/hipnotizar as mentes dos homens (I Timóteo 4:2), para que não saibam o que estão fazendo, para onde estão indo e assim, caíam no abismo (Jeremias 51:7). Exemplos: proibição do casamento e de comer carne (I Timóteo 4:1-3); incentivar o apego às tradições dos homens no lugar das Escrituras (Colossenses 2:8); etc.

A marca da Besta é espiritual e consiste na crença (aceitação, anuência, acatamento, concordância, submissão, devoção, respeito, zelo, defesa, etc.) de uma doutrina (credo, dogma, conceito, profissão de fé, catecismo, filosofia, etc.) inescriturística (inexistente na Bíblia) ou demoníaca aceita pela maioria das pessoas. Explica-se. Já que pela fé somos salvos (Marcos 16:16, João 3:15, 11:25 e 12:46, Efésios 2:8, I Pedro 1:5, Romanos 9:30,33 e 10:11 e Gálatas 2:16), nossa fé deve estar corretamente ajustada, mirada e sintonizada (João 7:38 e Mateus 7:23), sob pena de errarmos o alvo e perdermos a vitória (sermos condenados). Simplesmente crer que Deus existe e que sua Palavra é a Verdade, até mesmo Satanás e os demônios não duvidam disso.

> "Crês, tu, na existência de um só Deus? Fazes bem! Até mesmo os demônios crêem e tremem!" (Tiago 2:19).

O diabo ao convencer as pessoas da sua versão, pregação ou interpretação manipulada das Escrituras (acrescentar, retirar ou distorcer uma única palavra, letra, til, vírgula, acento, ponto...) já as faz dignas do Inferno (Apocalipse 22:18-19), pois um pouco de fermento levada toda a massa (Gálatas 5:9).

> "Olhai, pois, que façais como vos mandou o SENHOR vosso Deus; não vos desviareis, nem para a direita nem para a esquerda." (Deuteronômio 5:32).

Muitas pessoas pensam que Deus não se importa com pequenos desvios de Sua Palavra, mas como quando vamos sintonizar uma estação de rádio, a frequência tem que estar precisa/exata para podermos ter um som limpo, claro, puro, audível e compreensível ou, como uma senha (de banco, cartão, alarme, cofre, fechadura, Internet, etc.), basta apenas um digito incorreto (diferente, a mais ou a menos) ou fora de ordem para dar erro apesar de todos os demais estarem corretíssimos.

Igualmente, uma simples e mínima alteração de nosso DNA já nos transforma em aberrações da natureza, pois, para se ter uma noção disso, a diferença do DNA humano para o DNA de um chimpanzé ou de um grão de arroz é de apenas menos de 1% (um por cento).

Um medicamento se não for ministrado na dosagem precisa poderá ser fatal, ou seja, uma gota a mais ou a menos poderá ter consequências desastrosas.

Um único pedaço faltante, solto, mal pregado, torto ou trincado dos trilhos de um trem, o faz descarrilhar por completo. Um pequeno furo na fuselagem de um avião é o suficiente para fazê-lo cair.

Um simples e pequeno buraco numa rodovia novíssima como um carpete é o suficiente para provocar desastres.

Uma simples e pequena rachadura num dique, barreira, represa ou hidroelétrica é o suficiente para causar uma calamidade.

Se o médico aplicar a injeção ou passar o bisturi um pouco a mais ou a menos do local correto pode provocar consequências desastrosas.

Se você for num caixa eletrônico para sacar determinada quantia em dinheiro e seu saldo e/ou limite de crédito for inferior a isso apenas um centavo, acaso conseguirá sacar o valor pretendido?

Uma única vez que a pessoa esquece de tomar sua medicação contínua para o coração poderá lhe causar um ataque cardíaco e matá-la, não

importando que ela durante 30 anos tomou a medicação religiosamente.

Basta um pequeno desalinhamento no cano de uma arma de fogo para que o projétil não seja disparado corretamente.

Se calçamos um sapato um número maior ou menor do que o nosso número correto, não será a mesma coisa, pois o número menor será desconfortável, apertado, nos atrapalhará a andar normalmente e, ainda, nos machucará. Já o número maior, ficará folgado, não ficará firme, ficará saindo do pé e, também, nos atrapalhará a andar normalmente.

Uma torneira de água gotejando continuamente faz um rombo enorme na conta no final do mês.

Se em apenas um ponto de numa fiação condutora de energia elétrica, houver um rompimento, desse ponto em diante não haverá mais condução de eletricidade, não importando se nos outros 500 metros anteriores e/ou posteriores não há nenhum rompimento. Assim, tem-se que encontrar em que ponto tem um rompimento para poder repará-lo para a energia voltar a fluir.

Não importa se um paraquedista já deu um milhão de saltos com sucesso, basta apenas ele esquecer o paraquedas uma vez ou este falhar uma vez só, que será o suficiente para matá-lo. Do mesmo modo, uma pessoa pode ter passado décadas com uma conduta exemplar, mas basta apenas a prática de um único crime para ser considerada criminosa e ser condenada à prisão.

Os homens podem ter suas tolerâncias, mas a lei natural não. Assim, um credor poderá não fazer questão de um centavo de uma dívida ou um motorista poderá esperar cinco minutos além do horário por um passageiro atrasado, mas a natureza não faz isso. Um predador não vai perdoar uma presa que está doente, idosa, obesa, machucada, distraída, sonolenta, dormindo, cansada, presa, fazendo suas necessidades fisiológicas, etc., mas, pelo contrário, são as presas nessas condições que o predador prefere para atacar. Um juiz humano pode relevar um atraso de quinze minutos, mas o Juiz divino não irá, pois nossas vidas não são como jogos eletrônicos (videogame), onde temos várias vidas/chances para perdermos errando até acertarmos (Hb 9:27).

Em Apocalipse, nas cartas às sete Igrejas, vemos o início, avanço e desenvolvimento da infiltração, atuação e manifestação de Satanás dentro da Igreja de Jesus Cristo até que conseguiu, lentamente, levá-la à apostasia que culminará no total desvirtuamento da Igreja de Jesus Cristo transformando-a na Igreja do Anti-Cristo.

Paulo, que pela teologia, pelos livros, pela ciência humana, pelo racionamento humano, pelas tradições, pela sabedoria deste mundo... pensava que Cristo fosse um enviado de Satanás, após conhecer Jesus face a face e ter sido instruído por Ele, passou a combater as mentiras de Satanás, mas estas já estavam muitas disseminadas, enraizadas e espalhadas, não tendo conseguido exterminá-las por completo.

Após a revelação divina dada por Jesus, Paulo pregou o verdadeiro Evangelho e nos advertiu que suas pregações não consistiam em ciências (I Tim 6:20), argumentações, filosofias (Col 2:8) ou palavras persuasivas (Col 2:4) de sabedoria (I Cor 1:17,21) humana (I Cor 2:1-5).

Aos poucos falsos convertidos foram ingressando no Cristianismo um após o outro e em algumas situações vários de uma vez só em razão de imposição dos governantes (reis, monarcas, regentes, ditadores, imperadores...). Assim, países, impérios, reinos e continentes foram tidos por cristãos sem nunca terem ouvido falar de Cristo e, pior, contra a vontade (sob o uso da força, intimidação, ameaça, violência, pressão, tortura...) e sem real conversão, pois a motivação era outra (conveniência, influência, captação de clientes, vantagens financeiras, lucro fácil, interesses escusos, etc.). Pouco tempo bastou para que surgissem falsos ministros pregando, com sutileza, pequenas distorções e desvios. Com o passar dos tempos surgiram títulos, hierarquias e organizações, ou seja, trocaram o companheirismo fraternal entre os irmãos e a simplicidade da Liderança do Espírito Santo pela instituição de castas (classes separadas = Clero x fiéis ou servos) e pela organização e liderança humanas. A cada dia que se passava o paganismo e as doutrinas demoníacas eram incorporadas, pouco a pouco, dentro do Cristianismo.

Aos poucos o Anti-Cristo foi infiltrando pensamentos, ideias, crenças, dogmas, conceitos, doutrinas... anti-bíblicas dentro do Cristianismo. Depois, uma vez que conseguiu infiltrar tais em algumas pessoas, passou a segunda fase que foi começar a infiltrar atos, rituais, manifestações atitudes... anti-bíblicas (exteriorização dos pensamentos ou atitudes demonstrativas das modernas convicções religiosas). Assim, como que hipnotizando essas pessoas durante séculos, primeiro lhes incute um pensamento (ordem, ideia, conceito, doutrina, entendimento, vontade...) e, após conseguir enraizar/encravar isso passa-se à estimulação de concretizar (realizar, fazer, exteriorizar, manifestar, praticar...) aquele pensamento induzido.

Passo a passo, degrau por degrau, martelada por martelada... o diabo foi desviando as pessoas de Jesus, como uma pessoa que amarra o tronco de uma muda de árvore para que ele fique envergado e ela não cresça ereta, mas se torne torta. Assim, devemos nos desprender dessas amarras do diabo enquanto ainda é possível a regeneração.

Como uma mulher recém-casada que é séria e fiel ao seu marido, o sedutor para corrompê-la não poderá chegar de uma vez e já manifestar suas intenções. Mas, antes, terá que primeiro se aproximar sem levantar suspeitas ou desconfiança. Terá que conquistar confiança. Se aproveitar de sua ingenuidade. Terá que conquistar sua amizade. Terá que dar provas de confiança e amizade. Terá que fazer toda uma encenação, fingimento, teatro... para que consiga não só se aproximar dela, mas para que consiga habitualmente estar próximo dela. Portanto não poderá um estranho se aproximar de uma vez dela e já ter algum tipo de intimidade. Assim, terá que ter uma desculpa para se aproximar, tal como, por exemplo, fazer uma gentileza (pegar algo que ela deixou cair) e nada mais que isso, frequentar os mesmos lugares que ela, apenas cumprimentá-la nas outras vezes que a vir, falar bem e defender o marido dela de modo que ela possa ver o ouvir ele fazendo isso, começar a sentar perto dela nos lugares, começar a conversar com ela, oferecer-lhe carona, lembrar-lhe de seus aniversários, elogiar sua aparência e vestimenta... até que ela não o mais tenha por um estranho, mas, pelo contrário, tenha simpatia por ele aí ele poderá não só manifestar suas verdadeiras intenções, como, normalmente, conseguirá realizar o que planejou.

Assim, o diabo não podia de uma vez já falar para as pessoas que Deus não tem nome, que Deus não tem sexo, que Deus ama e salvará todas as pessoas, que todas as crenças e religiões levam a Deus, que Deus quer unir todos os povos, que Deus quer que construamos um mundo melhor, que nenhuma religião está errada, que somos todos irmãos, que Pedro foi o primeiro papa, que Jesus tinha olhos verdes e era loiro, que não existe Inferno, etc., pois ninguém iria acreditar-lhe. Explica-se. Ninguém que conheceu o Messias ou conheceu quem conheceu o Messias iria acreditar que Cristo fosse gay, que abençoava a todos indiscriminadamente, que proibia o consumo de vinho, que guardava o sábado, que não comia carne na sexta-feira, etc., pois saberiam que era mentira. Assim, somente com quem não teve contato com quem O conheceu, é que Satanás podia incutir suas mentiras.

Para ser mais didático. Eu só conheço meu avô paterno por fotos antigas e pelo que me falam dele. Não tenho como saber se o que me falam é verdade ou mentira, pois eu não o conheci pessoalmente. E o que falarei dele aos meus filhos e netos? Falarei o que lembrarei do que me falaram dele. Mas, tudo o que eu ouvi dele é verdade? As pessoas que me falaram dele não se esqueceram de nada? Mesmo que essas pessoas que me falaram sobre ele tenham dito a verdade e falado tudo o que sabem, elas sabem de tudo sobre ele? Claro que não! Só falaram apenas daquilo que presenciaram.

Com o passar dos tempos, os discípulos de Cristo e as demais pessoas que O conheceram pessoalmente (quando em carne), foram deixando este mundo. E, do mesmo modo, as pessoas que O conheceram indiretamente (ou seja, souberam de Jesus por meio daqueles que O conheceram pessoalmente). Assim, foi diminuindo as pessoas que poderiam desmentir as mentiras que Satanás ia espalhando, ou seja, Satanás começou a caluniar os santos que partiram deste mundo.

Por isso a Bíblia diz que Satanás calunia e blasfema dos mortos (Santos) que não podem se defender e nem desmentir o que deles Satanás fala. Assim, por exemplo, a alegação de que os santos mortos intercedem pelos vivos e, pouco tempo depois da morte de Lutero, seus pseudos seguidores, imediatamente, distorceram os seus ensinamentos.

Quando não havia vivo mais nenhum discípulo de Cristo e nem mesmo os alunos dos discípulos, Satanás teve o caminho livre para poder disseminar suas mentiras, mas, mesmo assim, não podia fazer com que as pessoas de uma vez girassem 180º, mas grau por grau, guinada por guinada, distorcida por distorcida... é que foi fazendo as pessoas se desviarem cada vez mais do caminho que conduz à salvação. Assim, por exemplo, ainda seria cedo para Satanás dizer para algumas pessoas que Cristo nunca existiu, que foi tudo invenção (como alguns dizem que o holocausto dos Judeus por Hitler nunca existiu), pois ainda haviam os familiares, íntimos e alunos dos alunos dos discípulos de Cristo que iriam desmenti-lo. Inclusive, ainda havia muitos registros de sua existência. Assim, ele precisava antes esperar essas pessoas morrerem e precisava ir destruindo os registros, documentos e escritos que lhe atrapalhavam.

No passado Satanás cometeu o erro de ser afobado, precipitado, impaciente, apressado... em desviar rapidamente e em grande monta o povo de Deus (causar a apostasia total e repentina), mas isso o levou a ser rápido e facilmente percebido e combatido. Explica-se. Quando Moisés subiu ao monte Sinai para receber os dez mandamentos de Deus, esses poucos dias da presença de Moisés perante o povo judeu foi suficiente para o diabo causar uma tremenda depravação, luxúria e idolatria (Ex 32).

Volta e meia quando tudo parecia perdido e sem solução, Deus levantava alguém para limpar toda a imundícia e regenerar sua Igreja, mas algum tempo depois, como uma casa recém limpa, a sujeira voltou, pouco a pouco a se acumular, necessitando de uma nova faxina urgente e assim a história foi se repetindo até os dias de hoje.

Em toda a Bíblia vemos que sempre que Deus levantou algum profeta para tirar seu povo da apostasia (erro, engano, idolatria, paganismo, superstições, bruxaria, ecumenismo...) e trazê-los de volta, após a morte deste enviado, seus pseudos seguidores (leia-se agentes secretos do Maligno) trataram de rapidamente corromper tudo de novo e a história assim tem se repetido vez por vez.

Quando o ungido de Deus não está mais vivo para se defender ou desmentir seus caluniadores, seus falsos seguidores podem mentir à vontade,

pois as pessoas acreditam que tais pessoas devem estar falando a verdade.

Por outras palavras, enquanto o ungido de Deus está vivo, muitos falsos convertidos/discípulos lhe acompanham esperando o momento oportuno de lhe traírem. Explica-se. Assim que o ungido de Deus morre, esses falsos seguidores ou se auto-intitulam como os escolhidos para serem seus sucessores ou se aproveitam que ele está morto e não pode se defender, e começam a caluniá-lo, ou seja, a fazerem falsas acusações de heresias, blasfêmias, perversões, etc., numa atitude hipócrita vez que enquanto o ungido estava vivo se apresentavam publicamente como seus aliados, mas bastou ele morrer para mudarem de opinião e verem as coisas de modo diferente.

O fato é que muitas vezes essas pessoas não mentem conscientemente, mas são manipuladas pelo diabo, pois nunca se converteram de verdade, mas estavam ao lado do ungido por interesses escusos (conveniência, privilégios, medo, status, riquezas, pressão...) e quando o ungido morre, esses soldados de Satanás se manifestam e passam a desviar as pessoas novamente de Deus. Bastou Moisés se ausentar por alguns dias para todo o povo que o seguia se corromper, praticar orgias e adorar ao bezerro de ouro (Ex 32). O plano de Satanás é desviar a adoração de Deus para si. Assim, aquele que hoje é conhecido por vários nomes, personalidades e formas, tratou desde o princípio de confundir as pessoas e criar várias personalidades suas para receber adoração pelo mundo.

Mas, como **o diabo nunca se limita a um único plano, estratégia, tática, estratagema, meio, recurso, técnicas... por vez, ele usou várias armas de uma vez só**:

1) Tentou destruir todos os documentos que lhe atrapalhavam;

2) Tentou fazer as pessoas desacreditarem nesses documentos;

3) Passou a dar outras explicações, entendimentos, sentidos, significados e objetivos a tais documentos que lhe prejudicavam;

4) Passou a produzir diversos documentos com uma variedade de testes teológicas e doutrinárias para confundir as pessoas;

5) Passou a alterar tais documentos (versões falsas) para esconder ou adulterar a informação que lhe prejudicava;

6) Passou a forjar outros documentos atribuindo a autoria a algum santo para confundir;

7) Levantou falsos ungidos para guardarem tais documentos e abafarem a informação contida neles;

8) Passou a levantar falsos missionários e evangelistas para divulgarem uma versão deturpada do Cristianismo e de tais documentos.

A infiltração do mal pode ser melhor entendida **como se fosse um câncer**, ou seja, começa discretamente e imperceptivelmente como um pequeno nódulo ou carocinho, como se não fosse nada sério, preocupante ou prejudicial, mas como não nos atentamos para ele, ele vai crescendo sorrateiramente, vai enraizando e estendendo seus tentáculos (firmando suas raízes) até que quando você se dá conta de que ele existe e é maligno, ele já dominou o seu corpo e já está na iminência de matá-lo e não há mais nada que se possa fazer para salvá-lo, pois ele atingiu vários membros vitais de seu corpo.

Desse modo, pode-se fazer uma analogia de que cada vez que Deus enviou um ungido para socorrer (curar, purificar, restaurar, regenerar, limpar, corrigir...) sua igreja seria como um cirurgião oncologista removendo o câncer de um paciente, mas, volta e meia, o câncer voltava a se manifestar em outros pontos e necessitava de outra extração cirúrgica até que a quimioterapia (transformação de nossos corpos corruptíveis em incorruptíveis) elimina completamente todas as células cancerígenas malignas.

Assim, o único meio de proteger-se, é preventivamente, ou seja, tendo zelo, cautela, cuidado, atenção e realizando autoexames periódicos, a fim de constatá-lo no início para poder extirpá-lo antes de atingir todo o corpo, pois, quando o câncer já possui determinado tamanho ou já atingiu mais de um órgão, mesmo retirando-o, ele pode ter deixado fragmentos ou raízes pelo corpo, os quais continuam a se desenvolvendo e matando o corpo.

Como uma **laranja podre** dentro de um saco de laranjas novas boas, a única laranja podre estraga todas as demais como uma epidemia. Desse modo, o contato, a intimidade ou o convívio com uma única célula

adulterada (estragada, podre, defeituosa, corrompida, deficiente, anormal...) contamina todas as demais células saudáveis.

"2 Porque haverá homens amantes de si mesmos, avarentos, presunçosos, soberbos, blasfemos, desobedientes a pais e mães, ingratos, profanos,
3 Sem afeto natural, irreconciliáveis, caluniadores, incontinentes, cruéis, sem amor para com os bons,
4 Traidores, obstinados, orgulhosos, mais amigos dos deleites do que amigos de Deus,
5 Tendo aparência de piedade, mas negando a eficácia dela. **Destes afasta-te.**" (II Tim 3:2-5).

"Ao homem herege, depois de uma e outra admoestação, **evita-o**," (Tt 3:10).

Jesus comparou seu ministério como o ato de semear a boa semente, ou seja, fez uma analogia de sua igreja com o ato de plantar um pé de mostarda:

"18 Escutai vós, pois, a parábola do semeador.
19 Ouvindo alguém a palavra do reino, e não a entendendo, vem o maligno, e arrebata o que foi semeado no seu coração; este é o que foi semeado ao pé do caminho.
20 O que foi semeado em pedregais é o que ouve a palavra, e logo a recebe com alegria;
21 Mas **não tem raiz em si mesmo**, antes é de pouca duração; e, chegada a angústia e a perseguição, por causa da palavra, logo se ofende;
22 E o que foi semeado entre espinhos é o que ouve a palavra, mas os cuidados deste mundo, e a sedução das riquezas sufocam a palavra, e fica infrutífera;
23 Mas, **o que foi semeado em boa terra é o que ouve e compreende a palavra; e dá fruto**, e um produz cem, outro sessenta, e outro trinta.
24 Propôs-lhes outra parábola, dizendo: **O reino dos céus é semelhante ao homem que semeia a boa semente no seu campo**;
25 Mas, dormindo os homens, **veio o seu inimigo, e semeou joio no meio do trigo**, e retirou-se.
26 E, quando a erva cresceu e frutificou, apareceu também o joio.
27 E os servos do pai de família, indo ter com ele, disseram-lhe: Senhor, não semeaste tu, no teu campo, boa semente? Por que tem, então, joio?
28 E ele lhes disse: Um inimigo é quem fez isso. E os servos lhe disseram: Queres pois que vamos arrancá-lo?
29 Ele, porém, lhes disse: Não; para que, ao colher o joio, não arranqueis também o trigo com ele.
30 **Deixai crescer ambos juntos até à ceifa; e, por ocasião da ceifa, direi aos ceifeiros: Colhei primeiro o joio, e atai-o em molhos para o queimar; mas, o trigo, ajuntai-o no meu celeiro**.
31 Outra parábola lhes propôs, dizendo: **O reino dos céus é semelhante ao grão de mostarda que o homem, pegando nele, semeou no seu campo**;
32 **O qual é, realmente, a menor de todas as sementes; mas, crescendo, é a maior das plantas, e faz-se uma árvore, de sorte que VÊM AS AVES DO CÉU, E SE ANINHAM NOS SEUS RAMOS**.
33 Outra parábola lhes disse: **O reino dos céus é semelhante ao fermento, que uma mulher toma e introduz em três medidas de farinha, até que tudo esteja levedado**.
34 Tudo isto disse Jesus, por parábolas à multidão, e nada lhes falava sem parábolas;

35 Para que se cumprisse o que fora dito pelo profeta, que disse: Abrirei em parábolas a minha boca; Publicarei coisas ocultas desde a fundação do mundo.

36 Então, tendo despedido a multidão, foi Jesus para casa. E chegaram ao pé dele os seus discípulos, dizendo: Explica-nos a parábola do joio do campo.

37 E ele, respondendo, disse-lhes: O que semeia a boa semente, é o Filho do homem;

38 O campo é o mundo; e a boa semente são os filhos do reino; e o joio são os filhos do maligno;

39 **O inimigo, que o semeou, é o diabo; e a ceifa é o fim do mundo; e os ceifeiros são os anjos**.

40 Assim como o joio é colhido e queimado no fogo, assim será na consumação deste mundo.

41 **Mandará o Filho do homem os seus anjos, e eles colherão DO SEU REINO tudo o que causa escândalo, e os que cometem iniqüidade**.

42 E lançá-los-ão na fornalha de fogo; ali haverá pranto e ranger de dentes.

43 Então os justos resplandecerão como o sol, no reino de seu Pai. Quem tem ouvidos para ouvir, ouça." (Mt 13:18-43).

Jesus deixa claro que o Maligno não poderia destruir diretamente a plantação do Senhor, ou seja, as boas sementes plantadas germinariam (isso ele não poderia impedir), mas o Maligno semeou outras sementes junto para que estas causassem danos, transtornos, tumultos, contendas e confusões na plantação de Deus. Desta feita, ambas as sementes iriam desfrutar e disputar pelo mesmo solo, água, Sol e cuidados, crescendo juntas, misturadas, lado a lado na mesma lavoura, até o dia da colheita quando então serão distinguidas e separadas. Observe que expressamente diz que "do seu reino", ou seja, de sua igreja, é que seria feita a separação do que é joio e do que é trigo. Por outras palavras, essa separação não é feita sobre os pagãos, ímpios, ateus, etc., vez que ali não há trigo para ser separado (mas somente existe as más sementes) e **o julgamento começa pela casa de Deus** (I Pe 4:17):

"21 Nem todo o que me diz: Senhor, Senhor! entrará no reino dos céus, mas aquele que faz a vontade de meu Pai, que está nos céus.

22 Muitos me dirão naquele dia: Senhor, Senhor, não profetizamos nós em teu nome? e em teu nome não expulsamos demônios? e em teu nome não fizemos muitas maravilhas?

23 E então lhes direi abertamente: Nunca vos conheci; apartai-vos de mim, vós que praticais a iniqüidade.” (Mt 7:21-23).

Assim, **é uma utopia, ilusão, engano, mentira... pensar que na Igreja de Jesus ou na Casa de Deus somente haveria trigo**, pois o próprio Jesus afirmou que na sua Igreja, desde o seu princípio/início até a sua colheita (arrebatamento e julgamento), haveria joio (Judas Iscariotes; Ananias e Safira – Atos 5; inveja, contendas e dissensões em Corinto – I Cor 1:11, 3:3-5 e 11:18; fornicações em Corinto – I Cor 5:1; heresias em Corinto I Cor 11:19 e 15:12; II Tes 3:11; Ef 4:31; etc) misturado ao trigo. Isso não quer dizer que a Igreja de Cristo foi vencida, destruída ou que fracassou. Apenas significa que Satanás infiltrou e mantém infiltrado os seus soldados no meio da Igreja de Jesus para tentá-la, enfraquecê-la, drogá-la, adormecê-la, hipnotizá-la, entorpecê-la, atormentá-la... mas, sem poder destruí-la como Deus permitiu ao diabo atormentar (torturar) à Jó sem, contudo, matá-lo – “E disse o SENHOR a Satanás: Eis que ele está na tua mão; porém guarda a sua vida.” (Jó 2:6).

Em síntese, como nós ainda possuímos um corpo carnal corruptível, nos é impossível permanecermos na Palavra de Deus. Nossa carne continuamente luta contra o Espírito Santo de Jesus. Ambos possuem interesses, pensamentos, sensações, desejos, prazeres... opostos. Só seremos perfeitos quando formos revestidos da perfeição ao sermos transformados no novo corpo incorruptível. O lavrador plantou a semente no solo fértil com os nutrientes adequados e na quantidade correta, lhe regou com boa água, na quantidade e nos horários adequados, o sol foi na medida exata, mas isso não garante que a planta cresça e continue saudável, pois as pragas (larva, pulgão, gafanhoto, etc.) são inúmeras e seus ataques, são constantes e cada inseticida, germicida, veneno... contra as pragas também afetam a própria planta, além do que cada ataque das pragas enfraquece a planta vez que ela é frágil. Portanto, o único modo/meio da planta ficar perfeita/pura é exterminando, completa e definitivamente, todas as pragas existentes no mundo, pois, como diz o ditado popular: “De nada adianta matar uma única barata, mas, sim, tem-se que matar à todas elas.” Assim, quando mal for, total e definitivamente, erradicado não haverá mais corrupção.

Quando Cristo veio, o mundo e inclusive o povo de Deus (Judeus) estavam impregnados das mentiras de Satanás. Assim, muitos duvidaram de

Cristo, pois Ele falava coisas contrárias às suas tradições, credos, dogmas, estudos, teologia, filosofias, igrejas, denominações religiosas, guias espirituais, rabinos, crenças, rituais... E não é para menos, pois até vir o profeta João Batista preparando o caminho do Senhor (Jesus Cristo), foram 400 anos de silêncio (sem Deus ungir ninguém, sem Deus enviar um profeta, sem Deus dar uma mensagem...).

Quando o Messias estava cumprindo o seu ministério na Terra, Judas Iscariotes estava corporalmente ao seu lado, mas, na verdade, era um ungido de Satanás infiltrado (Lc 22:3 e Jo 6:70, 13:2 e 13:26-27) para tentar fazer desacreditar, atrapalhar, confundir, tumultuar... por outras palavras, era um agente secreto do inimigo infiltrado para, no momento mais propício, traí-lo.

Está bem claro na parábola do pé de mostarda que todas as aves viriam se acomodar nos ramos da árvore que representa a Igreja de Cristo, ou seja, que não seriam somente as boas aves, mas de todas as espécies:

> "Assim diz o Senhor DEUS: Também eu tomarei um broto do topo do cedro, e o plantarei; do principal dos seus renovos cortarei o mais tenro, e o plantarei sobre um monte alto e sublime. No monte alto de Israel o plantarei, e produzirá ramos, e dará fruto, e se fará um cedro excelente; e habitarão debaixo dele aves de toda plumagem, à sombra dos seus ramos habitarão." (Ez 17:22-23).

> "12 A sua folhagem era formosa, e o seu fruto abundante, e havia nela sustento para todos; debaixo dela os animais do campo achavam sombra, e as aves do céu faziam morada nos seus ramos, e toda a carne se mantinha dela.
> (...)
> 21 Cujas folhas eram formosas, e o seu fruto abundante, e em que para todos havia sustento, debaixo da qual moravam os animais do campo, e em cujos ramos habitavam as aves do céu;" (Dn 4:12,21).

Sobre a falsa igreja (joios), Deus deixa claro que o seu povo está no meio dela:

> “E clamou fortemente com grande voz, dizendo: Caiu, caiu a grande Babilônia, e se tornou morada de demônios, e covil de todo espírito imundo, e esconderijo de toda ave imunda e odiável. Porque todas as nações beberam do vinho da ira da sua prostituição, e os reis da terra se prostituíram com ela; e os mercadores da terra se enriqueceram com a abundância de suas delícias. E ouvi outra voz do céu, que dizia: Sai dela, povo meu, para que não sejas participante dos seus pecados, e para que não incorras nas suas pragas.” (Ap 18:2-4).

Numa planta cítrica, como um pé de laranja, por exemplo, podem ser enxertados ramos de outras plantas cítricas (limão, lima, tangerina, mexerica, poncã, pêra, maçã, acerola, etc.), que o pé de laranja continuará sendo um pé de laranja e não deixará de dar laranjas nos seus ramos originais (se ainda houver estes). Mas, nos ramos enxertados, apesar de correrem a mesma seiva do pé de laranja que alimenta e dá vida a todos os ramos e a planta inteira, não se produzirão laranjas, mas somente os frutos desses enxertos (limão, lima, etc.). **Assim, não é porque a semente original, as raízes, o tronco e a seiva são de um pé de laranja que seus frutos serão somente laranjas, pois os ramos manifestam (pelos seus frutos) as suas verdadeiras raízes e sementes apesar de estarem grudados em outra planta como parasitas.** Todos os ramos recebem a mesma luz do Sol, a mesma água da chuva e estão ligados a mesma raiz e tronco, mas não produzem os mesmos frutos. Ressalta-se que não é o pé de laranja que está dando outros frutos, mas são os ramos das outras plantas que estão cada um dando seus próprios frutos. Outro detalhe é que o pé de laranja continua vivo e com vigor, ou seja, não foi destruído, mas somente foi corrompido. Para que o pé de laranja cheio de enxertos de outros frutos cítricos volte a somente dar laranjas, é necessário podar todos os seus enxertos e recuperar os seus ramos originais da laranjeira. Assim, Deus prometeu regenerar sua igreja depois dos vários ataques que ela sofreu, ou seja, restabelecer os ramos que foram podados, destruídos, corrompidos e trocados:

> "O que ficou da lagarta, o gafanhoto o comeu, e o que ficou do gafanhoto, a locusta o comeu, e o que ficou da locusta, o pulgão o comeu." (Joel 1:4).

> "E restituir-vos-ei os anos que comeu o gafanhoto, a locusta, e o pulgão e a lagarta, o meu grande exército que enviei contra vós." (Joel 2:25).

Assim está claro que a aceitação e o poderio do Anti-Cristo envolvem questão doutrinária do Cristianismo que incorpora doutrinas demoníacas (sincretismo religioso, ecumenismo, o espírito da padronização e ajuntamento).

> "Deixai crescer ambos juntos até à ceifa; e, por ocasião da ceifa, direi aos ceifeiros: Colhei primeiro o joio, e atai-o em molhos para o queimar; mas, o trigo, ajuntai-o no meu celeiro." (Mateus 13:30).

No versículo I João 4:3, a Bíblia expressamente diz que: "o espírito do anticristo, do qual já ouvistes que há de vir, e eis que já está no mundo". Ainda mais, no livro de João, capítulo 12, versículo 31 Jesus disse: "Agora é o juízo deste mundo; agora será expulso o príncipe deste mundo.". De igual modo, no capítulo 16, versículo 11: "E do juízo, porque já o príncipe deste mundo está julgado.". Em Efésios 2:2 consta: "Em que noutro tempo andastes segundo o curso deste mundo, segundo o príncipe das potestades do ar, do espírito que agora opera nos filhos da desobediência.". Complementando, em I João 5:19 diz: "Sabemos que somos de Deus, e que todo o mundo está no maligno.".

Desse modo, desde a época do apóstolo João (I João 4:3) o espírito do Anti-Cristo já está agindo no mundo preparando o terreno para ele vir em forma humana séculos mais tarde. Assim, há muito tempo as pessoas estão levando a marca da Besta enquanto que o chip existe a pouco tempo. Enquanto as pessoas ficam pensando que a marca da Besta é algo futuro que ainda está por vir, já são e estão sendo marcadas há séculos e nem se dão conta.

Assim como os judeus ainda estão esperando pelo Messias/Cristo (pensando que Ele ainda está por vir), mas descobrirão que Ele já veio faz milênios (e receberão dois profetas – Moisés e Elias – ao invés de um), muitos pseudos cristãos estarão esperando Cristo voltar e descobriram que a Noiva de Cristo já foi arrebatada e eles encontrarão o Anti-Cristo em vez de Cristo.

Portanto, O Anti-Cristo veio primeiro na forma espiritual (sua forma original) e depois será incorporado numa pessoa. Por outras palavras, O Anti-Cristo não precisa de um corpo físico para estar vivo, estar consciente e para poder agir. Ainda mais, há dezenas de séculos O Anti-Cristo já está agindo; ou seja, marcando o seu gado para o abate. Por outras palavras, O Anti-Cristo não irá começar a marcar as pessoas somente depois que ele tomar uma forma humana. Quando ele fizer isso, todos os humanos já terão sido previamente marcados.

A marca da besta já é imposta desde há séculos nos seguidores de Satanás (I João 4:3). O perigo da marca da besta, é fazer das pessoas gado

(como o fazendeiro põe sua marca identificatória com ferro quente no seu gado), ou seja, o senhor coloca sua marca nos seus escravos/servos e os obriga a lhe servirem (fazerem o que ele quer ou lhe agrada).

> "Respondeu-lhes Jesus: Em verdade, em verdade vos digo que **todo aquele que comete pecado é servo do pecado**." (João 8:34).

> "Não sabeis vós que a quem vos apresentardes por servos para lhe obedecer, **sois servos daquele a quem obedeceis**, ou do pecado para a morte, ou da obediência para a justiça?
> Mas graças a Deus que, tendo sido servos do pecado, obedecestes de coração à forma de doutrina a que fostes entregues.
> E, libertados do pecado, fostes feitos servos da justiça.
> Falo como homem, pela fraqueza da vossa carne; pois que, assim como apresentastes os vossos membros para servirem à imundícia, e à maldade para maldade, assim apresentai agora os vossos membros para servirem à justiça para santificação.
> Porque, quando éreis servos do pecado, estáveis livres da justiça.
> E que fruto tínheis então das coisas de que agora vos envergonhais? Porque o fim delas é a morte.
> Mas agora, libertados do pecado, e feitos servos de Deus, tendes o vosso fruto para santificação, e por fim a vida eterna.
> Porque o salário do pecado é a morte, mas o dom gratuito de Deus é a vida eterna, por Cristo Jesus nosso Senhor." (Romanos 6:16-23).

Ressalta-se que **não se pode confundir cristos (ungidos) com O Cristo (Ungido, Messias)**. Um ungido é quem tem a unção do Espírito Santo; a qual pode ser parcial ou momentânea (Juízes [Jz] 16:20 e I Samuel 16:14). São exemplos a concessão divina de um ou alguns dons do Espírito Santo (Isaías [Is] 11:1-4, Atos 2:17, I Coríntios 12:4-12, I Coríntios 13, Romanos [Rm] 5:1-11 e 12:6-21 e Efésios [Ef] 4:1-3) ou Deus usar a boca da pessoa para falar algo (I Samuel 10:10, Mateus 10:20 e Atos [At] 3:21); nem que seja uma única frase ou vez na vida dessa pessoa (Números [Nm] 11:25). Já Ungido e Cristo são sinônimos para Messias; ou seja, Deus encarnado, porque o Espírito Santo é o próprio Deus em sua forma original. Portanto, Cristo é o Único que possui a plenitude (totalidade) e eternidade (permanente) da unção do Espírito Santo (João 4:24, I Timóteo 1:17, Colossenses 1:15, I Coríntios 3:16 e 7:40, II Coríntios 4:4 e I Tessalonicenses 4:8).

> "Não toqueis os meus ungidos, e aos meus profetas não façais mal." (I Crônicas 16:22 e Salmos 105:15).

> "Porque surgirão falsos cristos e falsos profetas, e farão tão grandes sinais e prodígios que, se possível fora, enganariam até os escolhidos." (Mateus 24:24).

"Filhinhos, é já a última hora; e, como ouvistes que vem o anticristo, também agora muitos se têm feito anticristos, por onde conhecemos que é já a última hora." (I João 2:18).

"Levantaram-se os reis da terra, E os príncipes se ajuntaram à uma, contra o Senhor e contra o seu Ungido." (Atos 4:26).

"Este achou primeiro a seu irmão Simão, e disse-lhe: Achamos o Messias (que, traduzido, é o Cristo)." (João 1:41).

Ressalta-se, também, que **não se pode confundir "vocação" com "unção"**. Unção é gênero e vocação é uma espécie de unção. Toda habilidade que o Espírito Santo proporciona é uma unção, mas nem toda unção é uma vocação. Toda manifestação de Deus numa pessoa, é unção, ressalvando que o batismo no Espírito Santo é a unção total. Há diferentes tipos de unções. Já a **vocação nasce com a pessoa** e fica com ela durante toda a sua vida **"Porque os dons e a vocação de Deus são sem arrependimento." (Romanos 11:29)**, ou seja, são irrevogáveis, mas não significa que a pessoa seja de Deus ou que tem a salvação garantida. Deus concede vocação, unção e dons tanto aos justos como aos injustos, mas o batismo do Espírito Santo Deus só dá aos salvos (eleitos).

Pelo Dicionário Aurélio, dom é dote ou qualidade natural, inata. Assim o dom é uma habilidade da pessoa. Mas pela Bíblia é vocação, ou seja, a disposição natural e espontânea que orienta uma pessoa no sentido de uma atividade, uma função ou profissão; pendor, propensão, tendência.

Um profeta é nascido profeta. Ele sempre tem o "Assim diz o Senhor". Isso nasce com ele. Jeremias era um profeta. Deus disse: "Antes mesmo de você ser formado no ventre de sua mãe eu te conheci e te santifiquei para ser um profeta e te enviei para as nações" (Jeremias 1:5). Isso é vocação.

José, quando ele nasceu, era um homem espiritual, um profeta, Deus falava com ele nos sonhos e lhe concedia a interpretação de sonhos. Isso é vocação. José, desde criança, exercia naturalmente sua vocação sem ter sido necessário antes lhe terem feito imposição de mãos, unção com azeite, ter tido um encontro com Deus ou ter tido um novo nascimento.

Não confundir "unção" com "dom". Unção é gênero e dom é uma qualidade de unção. Toda habilidade que o Espírito Santo proporciona é uma unção, mas nem toda unção é um dom. Toda vez que Deus apodera-se de alguma pessoa, é unção. Há diferentes tipos de unções e de dons. **Há unção com a qualidade de permanente (dom) e há unção com a qualidade de temporária (mera unção momentânea).** Nem toda unção é um dom (permanente). Dom é quando a unção é definitiva/irrevogável e há unções que são momentâneas/temporárias. A unção pode ser temporária e pode ser perdida/retirada. Já os dons e as vocações são permanentes/definitivas, mas não significa que a pessoa seja de Deus ou que tem a salvação garantida. Deus concede vocação, unção e dons tanto aos justos como aos injustos, mas o batismo do Espírito Santo Deus só dá aos salvos. A pessoa pode até nascer com o dom, mas não o manifesta antes de um encontro com Deus, um novo nascimento, o batismo no Espírito Santo.

Os dons do Espírito Santo versam sobre: sabedoria, ciência, fé, cura, operação de maravilhas, profecia, discernimento de espíritos, variedade de línguas e interpretação de línguas (I Coríntios 12:8-10).

Essas pessoas nascem neste mundo com algum propósito. O arrependimento não traz a vocação, ela é predestinada à essas pessoas. O que pode acontecer é que a pessoa esteja com a habilidade inerte, adormecido, atrofiado... e precise ser reavivado/reanimado. Assim, quanto a estes que estão com o dom (e não vocação) inerte, as Escrituras dizem para "procurar" (I Coríntios 12:31 e 14:1) ou "desejar" (I Coríntios 14:12) os dons para serem despertos/manifestados.

"Por cujo motivo te lembro que despertes o dom de Deus que existe em ti pela imposição das minhas mãos." (II Timóteo 1:6). Assim a pessoa já tem o dom, já nasceu com ela, mas não o estava exercendo.

Gálatas 1:15-16 declara, efetivamente, que Paulo foi dotado para pregar desde antes o seu nascimento, mas precisou ter um encontro com Jesus para despertar/manifestar essa habilidade (dom).

Moisés foi predestinado a ser o instrumento de Deus para libertar seu povo da escravidão do Egito, mas antes de despertar/manifestar esse seu

dom foi preciso ter um encontro com Deus.

Em relação a Davi, antes Deus enviou o profeta Samuel para ungir Davi com azeite e depois disso é que Deus passou a manifestar Seu Espírito em Davi.

Ministério é o exercício constante/periódico da habilidade concedida pelo Espírito Santo. Mas, qualquer pessoa pode falar línguas estranhas, profetizar... sem ter se arrependido e nem ter nascido de novo (isso tanto para dom ou unção). Assim não pode ser tida como prova do batismo do Espírito Santo tais manifestações do Espírito Santo, ainda, mais que há muito hipócritas, fingidos e farsantes.

Satanás, seus demônios e seus "ungidos" (possessos) podem imitar as manifestações do Espírito Santo (Mateus 7:21-23, 24:11,24; II Coríntios 11:13-15 e II Tessalonicenses 2:8-10).

A Bíblia relata que Deus falou com Samuel normalmente (I Samuel 3) sem ter sido necessário antes lhe terem feito imposição de mãos, unção com azeite, ter tido um encontro com Deus ou ter tido um novo nascimento e a Bíblia se refere a essa habilidade de Samuel de ministério profético (I Crônicas 11:3 e I Samuel 28:15).

Os ministérios estão descritos em Efésios 4:11-12 em grau de importância/hierarquia: "E ele mesmo deu uns para apóstolos, e outros para profetas, e outros para evangelistas, e outros para pastores e doutores, Querendo o aperfeiçoamento dos santos, para a obra do ministério, para edificação do corpo de Cristo;".

Também não se pode cometer o equívoco de confundirmos "unção" com o "batismo do (ou "no") Espírito Santo". A unção pode ser permanente (vocação) ou meramente provisória (momentânea) enquanto que o batismo do Espírito Santo é sempre eterno (não tem volta, não tem retorno, não sai, não se perde, não se tira...). "Não me lances fora da tua presença, e não retires de mim o teu Espírito Santo." (Salmos [Sl] 51:11). Essa passagem mostra que **a unção pode ser temporária; ou seja, pode ser retirada (Juízes 13:25 e 16:20)**, mas o dom e a vocação não. **Sansão** era

ungido de Deus, mas perdeu sua unção (Juízes [Jz] 16:20) e depois Deus lhe restituiu a unção (Juízes 16:28-20).

Desse modo, **não se pode confundir "o dom do Espírito Santo" com "os dons do Espírito Santo"**. O dom (singular) é a vida eterna (Romanos [Rm] 6:23); ou seja, é simplesmente o próprio Espírito Santo (batismo do Espírito Santo). **Tanto as unções como os dons (pois são uma qualidade de unção) versam sobre as mesmas habilidades**: sabedoria, ciência, fé, cura, operação de maravilhas, profecia, discernimento de espíritos, variedade de línguas e interpretação de línguas (I Coríntios [Cor] 12:8-10).

Nem devemos confundir os dons do Espírito (edificação da Igreja) com os frutos do Espírito (edificação pessoal). Os dons são serviços para serem prestados aos outros; "fruto" fala das graças ou traços característicos de uma pessoa habitada pelo Espírito Santo. Quando o Espírito de Deus toma residência num homem, Ele não somente o capacita para servir, mas também começa a cultivar a santidade da pessoa (edificação pessoal), a evidência de que é um solo profundo, o "amor, gozo, paz, longanimidade, benignidade, bondade, fidelidade, mansidão, domínio próprio" (Gálatas [Gl ou Gal] 5:22-23). Tanto o fruto como os dons são essenciais. Ambos são manifestações da habitação do Espírito. Mas os dois não são a mesma coisa.

Já os **frutos/obras da carne** são: adultério, prostituição, impureza, lascívia, idolatria, feitiçaria, inimizades, porfias, emulações, iras, pelejas, dissensões, heresias, invejas, homicídios, bebedices, glutonarias, e coisas semelhantes a estas (Gálatas 5:19-21).

As Escrituras dizem que os cristãos são como lâmpadas e epístolas vivas nesse mundo e que pelos frutos fareis distinção entre os que são de Deus e os que procedem do maligno. Não precisa de nenhuma marca física ou material para reconhecer um cristão.

Um ungido de Deus pode errar, pecar, falhar, fracassar, desviar..., mas quem é batizado no Espírito Santo não. O batismo do Espírito Santo é o poder máximo (total ou pleno) que o Espírito Santo dá; já a unção, vocação ou dom é apenas fração (parte, parcela ou porção) de poder do Espírito Santo.

As expressões **“arrebatado no espírito”** (Apocalipse 1:10 e 4:2), arrebatado ao céu (II Coríntios 12:2) ou semelhantes (I Tessalonicenses [Ts ou Tes] 4:17, Atos 10:10, 11:5 e 22:17, II Coríntios 12:4 e II Pedro [Pe] 3:17) evidenciam que a pessoa já foi batizada no Espírito Santo, pois somente quem já tem o Espírito Santo incorporado definitivamente nela pode subir aos céus ou achegar-se à presença do trono de Deus.

No Antigo Testamento (AT) consta a expressão “o Espírito do Senhor se apossou” ou “se apoderou” de fulano demonstrando que o Espírito Santo pode usar momentaneamente as pessoas como bem lhe aprouver (Juízes [Jz] 14:6,9; 15:14, I Samuel 10:6,10; 11:6, 16:13, 18:10, Salmos [Sl] 119:53). Já no Novo Testamento (NT) usa o verbo “descer” (Lucas [Lc] 1:35). Entretanto no NT esse verbo (no português) tanto pode significar um uso momentâneo como o batismo do Espírito Santo. Entretanto, um eleito (predestinado) de Deus nunca perde sua unção ou seu ministério. Em outras palavras, **Deus só usa momentaneamente os ímpios na falta de um justo para a obra.** Importante lembrar que os demônios “ungem” (possessão) as pessoas e lhes concedem habilidades parecidas com as do Espírito Santo para confundirem/enganarem, exemplo, força física (Mateus [Mt] 8:28, Marcos [Mc] 5:2-4, Lucas [Lc] 8:27-29), adivinhação (Atos [At] 16:16-18), manifestação da verdade (Marcos 1:23-26, 3:11, 5:2-7, Lucas 4:33-35), gritos e/ou grunhidos/gemidos (Marcos 1:26, 5:2-5, Lucas 4:33, Atos 8:7), etc.

Por outras palavras, **não é só O Espírito Santo que pode incorporar-se (ungir uma pessoa)**, mas os demônios (anjos rebeldes, anjos caídos, espíritos imundos, espíritos de porcos ou espíritos malignos) também podem entrar nas pessoas; a esse fenômeno se dá o nome de possessão demoníaca (Marcos 5:1-15).

> "Então ele disse: Ouve, pois, a palavra do SENHOR: Vi ao SENHOR assentado sobre o seu trono, e todo o exército do céu estava junto a ele, à sua mão direita e à sua esquerda.
>
> E disse o SENHOR: Quem induzirá Acabe, para que suba, e caia em Ramote de Gileade? E um dizia desta maneira e outro de outra.
>
> Então saiu um espírito, e se apresentou diante do SENHOR, e disse: Eu o induzirei. E o SENHOR lhe disse: Com quê?
>
> E disse ele: Eu sairei, e serei um espírito de mentira na boca de todos os seus profetas. E ele disse: Tu o induzirás, e ainda prevalecerás; sai e faze assim.

Agora, pois, eis que o SENHOR pôs o espírito de mentira na boca de todos estes teus profetas, e o SENHOR falou o mal contra ti." (I Reis 22:19-23).

"Então disse Elias ao povo: Só eu fiquei por profeta do SENHOR, e os profetas de Baal são quatrocentos e cinqüenta homens." (I Reis 18:22).

"AMADOS, não creiais a todo o espírito, mas provai se os espíritos são de Deus, porque já muitos falsos profetas se têm levantado no mundo." (I João 4:1).

"Acautelai-vos, porém, dos falsos profetas, que vêm até vós vestidos como ovelhas, mas, interiormente, são lobos devoradores." (Mateus 7:15).

"E surgirão muitos falsos profetas, e enganarão a muitos." (Mateus 24:11).

"Porque surgirão falsos cristos e falsos profetas, e farão tão grandes sinais e prodígios que, se possível fora, enganariam até os escolhidos." (Mateus 24:24).

"A esse cuja vinda é segundo a eficácia de Satanás, com todo o poder, e sinais e prodígios de mentira," (II Tessalonicenses 2:9).

"Porque são espíritos de demônios, que fazem prodígios; os quais vão ao encontro dos reis da terra e de todo o mundo, para os congregar para a batalha, naquele grande dia do Deus Todo-Poderoso." (Apocalipse 16:14).

"E, chegada a tarde, trouxeram-lhe muitos endemoninhados, e ele com a sua palavra expulsou deles os espíritos, e curou todos os que estavam enfermos;" (Mateus 8:16).

Tal como Deus unge os seus, Satanás também unge os dele e, ainda, quer ungir os de Deus. Assim como Deus sela os seus, o diabo marca os dele e quer marcar (roubar) os de Deus, como um ladrão de gado/ovelhas. Esse modo, como qualquer pessoa pode momentaneamente ter a unção do Espírito Santo (não o batismo do Espírito Santo) e não significar necessariamente que a pessoa é de Deus ou que está salva, mas que apenas está sendo usada por Deus naquele momento/circunstância; do mesmo modo, qualquer mortal/criatura pode ser momentaneamente possuído ou ungido por Satanás ou seus demônios e não significar que a pessoa é do diabo ou que irá para o Inferno, mas tão somente que naquele momento estava sob o domínio do Maligno.

Exemplificando. **Judas Iscariotes** teve a mesma unção do que os demais apóstolos para pregar, operar milagres, realizar curas, expulsar demônios... (Mateus 10, Marcos 6:7 e Lucas 8:1 e 9:1) mas não permaneceu no caminho da salvação. **Até mesmo pela boca de uma jumenta Deus já falou** (Números 22:28). **Saul** foi ungido de Deus e rei de Israel, mas não

permaneceu na unção. Seus atos acabaram se tornando incompatíveis com os de um ungido de Deus e, por isso, acabou sendo desprezado por Deus, perdeu sua unção e seu reinado (I Samuel 13:13-14 e 15:26). **Salomão**, outro ungido de Deus e rei de Israel, apesar de sua grande sabedoria concedida por Deus, acabou se apostatando, fazendo amizade com os egípcios, casando-se com a filha do faraó egípcio (I Reis 11:1) e com outras mulheres pagãs, além de ter construindo vários templos aos deuses egípcios a pedido de suas esposas (I Reis 11:1-4,7,27) depois de ter construído o templo de Deus (tanto é assim que Salomão é o herói dos maçons) e foi também desprezado por Deus (I Reis 11:9-11,29-30). **Balaão** era um mercenário (Deuteronômio 23:4), mas mesmo assim também pregou a Palavra de Deus (Números 23:5,16), mesmo não querendo fazê-lo (Josué 24:9-10, Deuteronômio 23:4-5 e Neemias 13:2). **Caifás** era um hipócrita, mercenário e assassino, mas mesmo assim profetizou sobre o significado da morte de Cristo (João 11:49-51), como **Saul que, também apesar de não ser profeta, profetizou** (I Samuel 10:10-11). **Pedro** foi dominado por Satanás várias vezes (Mateus 16:22-23 e 26:69-75), mas depois teve o batismo do Espírito Santo e onde sua sombra tocava expulsava os demônios, realizava milagres, realizava curas... (Atos 5:15). Igualmente **Paulo** que já foi blasfemador, assassino e perseguidor dos Cristãos (Atos 22), depois do batismo do Espírito Santo (Atos 13:9), até suas vestes expulsava os demônios, realizava milagres, realizava curas... (Atos 19:11-12).

Vejamos Mateus 7:13-23:

"Entrai pela porta estreita; porque larga é a porta, e espaçoso o caminho que conduz à perdição, e muitos são os que entram por ela;

E porque estreita é a porta, e apertado o caminho que leva à vida, e poucos há que a encontrem.

Acautelai-vos, porém, dos falsos profetas, que **vêm até vós vestidos como ovelhas, mas, interiormente, são lobos devoradores**.

Por seus frutos os conhecereis. Porventura colhem-se uvas dos espinheiros, ou figos dos abrolhos?

Assim, **toda a árvore boa produz bons frutos, e toda a árvore má produz frutos maus**.

Não pode a árvore boa dar maus frutos; nem a árvore má dar frutos bons.

Toda a árvore que não dá bom fruto corta-se e lança-se no fogo.

Portanto, pelos seus frutos os conhecereis.

Nem todo o que me diz: Senhor, Senhor! Entrará no reino dos céus, mas aquele que faz a vontade de meu Pai, que está nos céus.

Muitos me dirão naquele dia: Senhor, Senhor, não profetizamos nós em teu nome? E em teu nome não expulsamos demônios? E em teu nome não fizemos muitas maravilhas?

E então lhes direi abertamente: Nunca vos conheci; apartai-vos de mim, vós que praticais a iniqüidade."

Vejamos o que a Bíblia fala sobre marcas ou sinais. Na Bíblia há vários sinais que Deus deu ao seu povo ou que colocou em seu povo, ora para serventia aos homens, ora para ser usado pelos anjos e demônios.

Em Romanos 4:11 vemos como "sinal" e "selo" são sinônimos indiscutíveis:

"E recebeu o sinal da circuncisão, selo da justiça da fé, quando estava na incircuncisão, para que fosse pai de todos os que creem, estando eles também na incircuncisão; a fim de que também a justiça lhes seja imputada;".

Pelo **Dicionário Houaiss**:

"**Marca**" - desenho, inscrição, nome, número, selo, símbolo, carimbo etc. que se coloca sobre um artigo para distingui-lo de outros, ou como indicação de propriedade, qualidade, categoria, origem; sinal ou qualquer coisa para avivar a lembrança a respeito de algo, ou que serve para reconhecer ou encontrar uma outra coisa; traço distintivo por que se reconhece alguém ou algo; estilo ou maneira pessoal.

"**Sinal**" – gesto para comunicar algo a alguém; impressão deixada por alguém ou algo; marca, traço; quantia ou objeto dado por um dos contratantes ao outro, para garantir o cumprimento de um contrato; arras, penhor; assinatura ou rubrica; manifestação clara de alguma coisa; mostra, demonstração; breve descrição de uma pessoa.

"**Selo**" - grande cunho sobre o qual são gravados em côncavo a figura, a assinatura, as armas ou a marca simbólica de um Estado, um rei, uma comunidade ou um particular, e que se aplica sobre atos ou objetos a fim de autenticá-los, fechá-los inviolavelmente ou marcar uma propriedade; chancela, sinete; pequeno sinal que se põe ou se apõe às coisas para assinalá-las, identificá-las ou torná-las invioláveis; carimbo; sinal particular; distintivo, marca; sinete que servia para imprimir na argila, antes de cozida, uma assinatura ou marca de fábrica.

"**Sinete**" - utensílio com assinatura, monograma ou divisa gravada em alto ou baixo-relevo e que se usa para imprimir em lacre, cera, papel etc.

"**Assinatura**" - nome ou marca firmada na parte inferior de um escrito, designando autoria ou aprovação de seu conteúdo; contrato pelo qual uma pessoa adquire o direito de receber determinada mercadoria ou usufruir de algum serviço; marca, desenho ou modelo próprio de alguém; entre ourives, gravadores, ebanistas etc., marca ou nome do autor.

"**Emblema**" - distintivo ou insígnia de instituição, sociedade, associação etc., utilizada no traje ou em objetos a elas relativos.

"**Logotipo**" - símbolo que serve à identificação de uma empresa, instituição, produto, marca etc., e que consiste ger. na estilização de uma letra ou na combinação de grupo de letras com design característico, fixo e peculiar.

Percebe-se, assim, que a marca, selo, sinal... transmite uma mensagem/informação. Desse modo, há um objetivo a ser alcançado; qual seja, que os destinatários consigam compreender o sinal. Assim, por exemplo, temos a sinalização de trânsito que possui desenhos que nos passam informações resumidas e facilmente assimiladas/compreendidas. Portanto, não é concebível imaginarmos uma placa de trânsito com o desenho de um tomate, pois a única ideia de que vamos ter será de que deve haver uma feira, mercado, mercearia... nas proximidades.

Outra constatação é que um chip não se enquadra na definição de sinal ou marca.

No princípio Deus usou o **arco-íris** como um **sinal aos homens** da Sua Aliança com seu povo (Gênesis 9:11-13):

"E eu convosco estabeleço a minha aliança, que **não será mais destruída toda a carne pelas águas do dilúvio**, e que não haverá mais dilúvio, para destruir a terra.
E disse Deus: Este é o sinal da aliança que ponho entre mim e vós, e entre toda a alma vivente, que está convosco, por gerações eternas.
O meu arco tenho posto nas nuvens; este será por sinal da aliança entre mim e a terra.".

Depois Deus usou a **circuncisão** com sinal identificador aos homens para distinguir seu povo (Gênesis 17:11):

"E circuncidareis a carne do vosso prepúcio; e isto será por sinal da aliança entre mim e vós.".

"E o SENHOR teu Deus circuncidará o teu coração, e o coração de tua descendência, para amares ao SENHOR teu Deus com todo o coração, e com toda a tua alma, para que vivas." (Deuteronômio 30:6).

Outro sinal identificador para os homens era/foi o povo de Deus **guardar o Sábado** (Êxodo 31:13):

"Tu, pois, fala aos filhos de Israel, dizendo: Certamente guardareis meus sábados; porquanto isso é um sinal entre mim e vós nas vossas gerações; para que saibais que eu sou o SENHOR, que vos santifica."

Os adventistas do sétimo dia, equivocados, acreditam que o selo de Deus seria a guarda do Sábado (palavra que significa descanso), quando, na

verdade, é o batismo com o Espírito Santo. Assim, portanto não é uma marca física/material. Ainda mais, Jesus aboliu a guarda do sábado (Mateus 12:1-8), pois Ele cumpriu toda a Lei por nós (Mateus 5:17, Lucas 16:16, Romanos 10:4, Gálatas 2:16 e 5:18) e nos concedeu a Graça (Romanos 6:14). O próprio Jesus é o novo Sábado (descanso – Gênesis 2:3, Êxodo 31:15, Levítico 16:31 e 23:32 e Mateus 11:29).

Outro erro dos adventistas é dizer que a marca da Besta seria guardar o Domingo (ou seja, não guardar o Sábado), quando, na realidade é uma marca espiritual; ou seja, a crença no dogma universal de como é Deus. Em outras palavras, é crer como os pagãos e a Cristandade (Cristãos apóstatas) como é a pessoa de Deus. E essa concepção universal de como é a pessoa de Deus é a pilastra (coluna mestra) que permitirá a unificação de todas as crenças, credos, dogmas, religiões, igrejas, filosofias... na religião mundial (Ecumenismo) do Anti-Cristo.

Já, em relação a um **sinal identificador para os anjos celestiais e para os demônios**, Deus usou o **sangue de cordeiro** para identificar os seus (Êxodo 12:7,13):

> "7 E tomarão do sangue, e pô-lo-ão em ambas as ombreiras, e na verga da porta, nas casas em que o comerem.
> (...)
> 13 E aquele sangue vos será por sinal nas casas em que estiverdes; vendo eu sangue, passarei por cima de vós, e não haverá entre vós praga de mortandade, quando eu ferir a terra do Egito."

E, recorde, no Novo Testamento reza que o sangue de Jesus Cristo está continuamente cobrindo e protegendo os Seus (João 6:56, Hebreus 9:12); exceto, claro, para aqueles que desistem, desviam, abandonam, renunciam...

Posteriormente o sinal identificador para os humanos passou a ser a **manifestação do Espírito Santo** (Êxodo 3:12):

> "E disse: Certamente eu serei contigo; e isto te será por sinal de que eu te enviei: Quando houveres tirado este povo do Egito, servireis a Deus neste monte.".

Em Isaías 66:19 vemos a expressão "E porei entre eles um sinal" mostrando que o sinal identificador no povo de Deus é feito pelo próprio Deus neles.

“E a glória do Deus de Israel se levantou de sobre o querubim, sobre o qual estava, indo até a entrada da casa; e clamou ao homem vestido de linho, que tinha o tinteiro de escrivão à sua cintura.

E disse-lhe o SENHOR: Passa pelo meio da cidade, pelo meio de Jerusalém, e **marca com um sinal as testas dos homens** que suspiram e que gemem por causa de todas as abominações que se cometem no meio dela.

E aos outros disse ele, ouvindo eu: Passai pela cidade após ele, e feri; não poupe o vosso olho, nem vos compadeçais.

Matai velhos, jovens, virgens, meninos e mulheres, até exterminá-los; **mas a todo o homem que tiver o sinal não vos chegueis**; e começai pelo meu santuário. E começaram pelos homens mais velhos que estavam diante da casa.” (Ezequiel 9:3-6).

"E vi outro anjo subir do lado do sol nascente, e que tinha o selo do Deus vivo; e clamou com grande voz aos quatro anjos, a quem fora dado o poder de danificar a terra e o mar,

Dizendo: Não danifiqueis a terra, nem o mar, nem as árvores, até que hajamos assinalado nas suas testas os servos do nosso Deus." (Apocalipse 7:2-3).

"E da fumaça vieram gafanhotos sobre a terra; e foi-lhes dado poder, como o poder que têm os escorpiões da terra.

E foi-lhes dito que não fizessem dano à erva da terra, nem a verdura alguma, nem a árvore alguma, mas somente aos homens que não têm nas suas testas o sinal de Deus." (Apocalipse 9:3-4).

Como se trata de uma questão espiritual, a marca igualmente tem que ser espiritual. Do mesmo modo, em sendo algo que envolve religiosidade e crença, a marca tem que estar relacionada a isso. Portanto, como a Besta tem que ser uma pessoa religiosa, sua marca, igualmente, tem que possuir esta característica. Assim, por exemplo, quando vemos o logotipo da Coca-Cola, logo lembramos do dito refrigerante. Entretanto, quando qualquer pessoa vê um chip iria lembrar do Anti-Cristo se nunca tivesse ouvido ou lido tal teoria apocalíptica? Nunca! A identificação, correlação, ligação... da marca com seu dono tem que ser algo natural e nunca forçado (sem nenhuma correlação, ligação ou vínculo).

Exemplificando. Os judeus utilizam o **tefilin** ou filactério; ou seja, duas caixinhas quadradas pretas de couro, uma no meio da testa e outra no braço esquerdo, na altura do coração, ambas presas (amarradas) através de tiras de couro de animal kasher (animal permitido como alimento pelo Antigo Testamento: Levítico 11 e Deuteronômio 14), dentro das quais contêm um pergaminho com os quatro trechos da Torá (Antigo Testamento) em que se baseia o uso dos mesmos (Deuteronômio [Dt] 6:8 e 11:18 e Êxodo [Ex] 13:9,16). Entretanto, tal prática consiste num simbolismo de que a Palavra

(Lei) de Deus deve estar na mente (Jeremias 31:33, Josué 1:8, Salmos 1:2 e 119:15, Isaías 26:3, Marcos 12:30 e Lucas 10:27), no coração (Deuteronômio 4:29,39 6:6, 10:16 e 30:6,10, I Reis 2:4, Isaías 8:6, Jeremias 31:33, Romanos [Rm] 2:29 e II Coríntios 1:22 e 3:33) e ser vivida ou praticada (Êxodo 35:1 e Deuteronômio 6:5, 10:12, 11:13, 17:19, 26:16, 28:58, 29:9, 29:29, 30:2,10, 31:12 e 32:46). Uma ressalva, a cultura antiga não possuía a definição de mente e, em razão disso, muitas vezes utilizava a palavra coração querendo se referir à mente (Gênesis 6:5 e Salmos 19:14 e 49:3). Desse modo, todas essas práticas, rituais e cerimônias prescritas no Antigo Testamento não passam de sombras do que havia de vir (Hebreus 8:5 e 10:1 e Colossenses 2:17). E, como sombras, de forma semelhante à uma parábola não possuem exatidão precisa ou total coincidência, mas apenas similitude ou referência simbólica ao que se queria expressar.

A **testa e a mão** simbolizam as duas atitudes individuais essenciais do Cristianismo para a salvação. A testa (ou fronte) é um símbolo para o que tem lugar nas nossas mentes (decisões, consciência, crenças, dogmas, credos, ideologias, pensamentos, filosofias, personalidade, conceitos, ideias, etc.). A fronte indica a inteligência, porque a mente é a sede da razão humana.

Já a mão representa aquilo que fazemos, as nossas ações ou atos. Diante disso, a testa representa a fé e a mão se refere às obras.

> "Assim também a fé, se não tiver as obras, é morta em si mesma." (Tiago 2:17).
>
> "Porque, assim como o corpo sem o espírito está morto, assim também a fé sem obras é morta." (Tiago 2:26).

Por outras palavras, o Cristianismo exige que a pessoa tenha a fé sintonizada corretamente e que não se limite à teoria, mas que viva de acordo, exteriorize, pratique, transpareça aos outros, resplandeça sua luz, pregue o Evangelho, etc.

A marca na testa descrita em Ezequiel 9:4 é espiritual ou física?

> "E disse-lhe o SENHOR: Passa pelo meio da cidade, pelo meio de Jerusalém, e marca com um sinal as testas dos homens que suspiram e que gemem por causa de todas as abominações que se cometem no meio dela." (Ezequiel 9:4).

A marca na **“mão”**, portanto, simboliza os atos que demonstram a crença e a obediência às doutrinas demoníacas do Anti-Cristo. Representa aquilo que fazemos, as nossas ações. Exemplo, o ditado/expressão “pôr mãos à obra”. Alguns irão mentalmente aceitar as palavras do Anti-Cristo e outros apenas lhe obedecem por comodismo, ser moda, por seguir a maioria, por ignorância, conveniência, interesses ou por receio de serem castigados. Em **Êxodo 13:9,16** vemos a expressão **"E te será por sinal sobre tua mão"** sem sentido literal, mas apenas simbólico de atitude. Assim, a mão exprime a atividade humana, porque é com as suas mãos que o homem opera e trabalha. Do mesmo modo, na Bíblia vemos as expressões **“mão de Deus”** (II Crônicas 30:12 e Eclesiastes 2:24) e **“dedo de Deus”** (Êxodo 8:19 e Lucas 11:20) significando ações, atos, obras, atitudes, feitos, realizações, atividades... de Deus.

Primeiro a coisa é estabelecida espiritualmente. Você recebe aquilo lá dentro de você, em seu raciocínio, em sua memória, em sua consciência, em sua imaginação, em seu afeto, em seu coração, enfim, em seu espírito. Antes de a Eva "comer" o fruto, ela se conscientizou, raciocinou, memorizou, imaginou e tomou aquilo em seu afeto (veja espiritualmente) e concluiu que aquilo era a verdade, para depois tomar uma atitude natural que foi a de comer o fruto. Quando Jesus morreu no calvário diz a Bíblia que aquilo já tinha acontecido desde a fundação do mundo (Apocalipse 13:8). Ali no calvário estava acontecendo apenas o lado natural daquilo que já tinha acontecido espiritualmente.

Portanto, tudo começa por dentro (interior) como uma fruta que vai apodrecendo de dentro para fora e quando a podridão atinge o exterior (se torna nitidamente visível) é porque o interior está repleto de podridão, está totalmente contaminado/estragado (Mateus 23:27). Quando nosso interior já está repleto de podridão, passamos a agir de acordo com a vontade dos demônios que deixamos nos dominarem ao aceitarmos suas palavras, pois “todo aquele que comete pecado é servo do pecado” (João 8:34).

Em síntese, a marca sobre a fronte e sobre a mão é a expressão de total dependência daquele que é significado por este sinal.

Do mesmo modo, no Novo Testamento, consta que pelos frutos (Mateus 7:20) distinguimos os que são de Deus ("epístolas vivas lidas por todos" – II Coríntios 3:2-3) dos que são ungidos de Satanás (falsos cristos e falsos profetas) que, apesar dos falsos prodígios (sinais, milagres, visões, fenômenos sobrenaturais... – Mateus 24:24, II Tessalonicenses 2:9 e Apocalipse 13:11-15) para seduzir, não conseguem permanecer na Palavra.

"QUANDO profeta ou sonhador de sonhos se levantar no meio de ti, e te der um sinal ou prodígio,

E suceder o tal sinal ou prodígio, de que te houver falado, dizendo: Vamos após outros deuses, que não conheceste, e sirvamo-los;

Não ouvirás as palavras daquele profeta ou sonhador de sonhos; porquanto o SENHOR vosso Deus vos prova, para saber se amais o SENHOR vosso Deus com todo o vosso coração, e com toda a vossa alma." (Deuteronômio 13:1-3).

Esses falsos Cristãos (soldados de Satanás) podem fingir sobre muitas coisas e durante muito tempo, mas eles não conseguem fingir o tempo todo, sobre tudo e a todos. Inclusive Deus revela aos seus quem são hipócritas (I Coríntios 12:10, Hebreus 4:12-13 e Atos 5:1-11). Desse modo, é perfeitamente possível identificá-los, seja por suas obras, seja pelas suas pregações (I Coríntios 12:3).

"Propôs-lhes outra parábola, dizendo: O reino dos céus é semelhante ao homem que semeia a boa semente no seu campo;

Mas, dormindo os homens, veio o seu inimigo, e semeou joio no meio do trigo, e retirou-se.

E, quando a erva cresceu e frutificou, apareceu também o joio.

E os servos do pai de família, indo ter com ele, disseram-lhe: Senhor, não semeaste tu, no teu campo, boa semente? Por que tem, então, joio?

E ele lhes disse: Um inimigo é quem fez isso. E os servos lhe disseram: Queres pois que vamos arrancá-lo?

Ele, porém, lhes disse: Não; para que, ao colher o joio, não arranqueis também o trigo com ele.

Deixai crescer ambos juntos até à ceifa; e, por ocasião da ceifa, direi aos ceifeiros: Colhei primeiro o joio, e atai-o em molhos para o queimar; mas, o trigo, ajuntai-o no meu celeiro." (Mateus 13:24-30).

"Porque faz que o seu sol se levante sobre maus e bons, e a chuva desça sobre justos e injustos." (Mateus 5:45).

"E há de ser que, depois derramarei o meu Espírito sobre toda a carne, e vossos filhos e vossas filhas profetizarão, os vossos velhos terão sonhos, os vossos jovens terão visões." (Joel 2:28).

Os falsos Cristãos não permanecem na Palavra de Deus e a síntese dos principais pontos do Plano de Deus é:

- Amar Deus sobre todas as coisas;
- Somente a Deus prestar culto e orações;
- Somente invocar o nome de Jesus em oração, culto e rituais (Rm 10:13, Jo 14:14 e Fp 2:10-11);
- Amar o próximo como a ti mesmo;
- Não servir as riquezas desse mundo;
- As bençãos, milagres e Salvação são presentes (Graça) diretos de Deus, não são recompensa, paga ou ato de comércio;
- Somente o sacrifício de Jesus expia nossos pecados e é o suficiente;
- Somente Jesus nos perdoa e diretamente mediante nosso arrependimento sincero (nada mais que isso);
- Somente Jesus é nosso Único e Direto Mediador e não há coadjuvantes (santos, profetas, padres, denominações, igreja...);
- A Bíblia, por ser a Palavra de Deus, é a autoridade máxima de nossa fé e Deus não é imperfeito ou contraditório para falar contra Si mesmo;
- Deus é sempre o mesmo (é imutável) e age sempre da mesma forma, pois é Perfeito (e não precisa evoluir, modernizar ou acompanhar o progresso, ciência, sociedade...);
- Seja sempre a Deus e Sua Palavra a Verdade e tudo o mais é mentira;
- Somente por Revelação Divina se conhece a Verdade e se tem entendimento das Escrituras;
- Os Cristãos estão submissos à liderança do Espírito Santo e não de homens, denominações ou teologias;
- Tudo o que passa/acresce ou diminui da Palavra de Deus é obra do Maligno (não se usa o ditado que "o que abunda, não prejudica").

Infra algumas características dos cristãos e pastores sinceros. Não basta ter uma ou outra característica, mas deve apresentar várias delas (não precisa ser todas) e não pode apresentar nenhuma das evidências dos falsos (exceto, claro, se já tiver ocorrido a regeneração).

- Alimentam e protegem as ovelhas (Jr 3:15 e 23:4, Ez 34:23, João 21:17, At 20:28 e I Pe 5:2);
- Amam, exaltam, glorificam e honram à Jesus (João 14:6 e 16:13-14, At 2:11,36 e 10:44-46, II Cor 8:23, Fp 1:20, Lc 9:26);
- Amor sincero - não fingido (Gal 5:22, II Cor 6:6, I Tim 6:11, I Cor 13, Rom 12:9 e 5:5);
- Benignidade (Gal 5:22, Col 3:12, Rm 11:22, II Cor 6:6);
- Bondade (Gal 5:22, II Cor 6:6, Rom 15:14, Ef 5:9, II Ts 1:11);
- Ciência divina (Sl 119:66, Jr 3:15, Rm 11:33, I Cor 8:11, II Cor 6:6 e 8:7, Fp 1:9, II Pe 1:5);
- Colocam a Palavra de Deus em primeiro lugar (II Tim 3:16, Jo 7:38 e 15:7);
- Conduzem as ovelhas à santificação (At 26:18, I Cor 6:18, II Cor 6:16-18);
- Constância (I Tim 6:14);
- Defendem as Escrituras e a fé que foi dada aos santos (Jo 15:7, Fip 1:16 e Jd 3);
- Fazem de coração a obra de Deus (I Pe 5:2);

- Fé (Gal 5:22);
- Fraternidade (Rm 12:10, I Ts 4:9, Hb 13:1, I Pe 2:17, II Pe 1:7);
- Gozo (Gal 5:22);
- Incentivam, estimulam e priorizam a leitura de toda a Bíblia e não apenas de fragmentos dela (II Tim 3:16);
- Julgam/analisam todas as coisas e reteêm o que é bom (I Tes 5:21);
- Levam a salvação aos perdidos (I Cor 9:19-22);
- Longanimidade (Gal 5:22, II Cor 6:6, Ef 4:2, Col 1:11 e 3:12, Rm 2:4, II Tim 3:10 e 4:2);
- Mansidão (Gal 5:22, I Tim 6:11, Ef 4:2, Mt 11:29, Col 3:12);
- Não buscam glórias humanas (I Tes 2:6);
- Não confiam em homens (Mt 10:17, Rom 3:4, Jer 17:5, Sl 118:8);
- Não exigem ser custeados (I Tes 2:7, II Tes 3:8, Mt 10:8);
- Não falam difícil, mas usam linguajar simples (I Cor 2:1,4-5);
- Não há escândalos em suas vidas – são irrepreensíveis (II Cor 6:3, Tt 1:7, I Tim 3:2);
- Não possuem malícia (Sl 34:21, Jó 15:35, Mt 22:18, At 13:10, Rm 1:29, I Cor 5:8 e 14:20, Ef 4:31);
- Não pregam para agradar aos homens (I Tes 2:4-5);
- Não priorizam os negócios deste mundo (II Tim 2:4);
- Não são astutos – são ingênuos (II Cor 4:2);
- Não são dados à bebida alcóolica (I Tim 3:3, Rom 14:21);
- Não são famosos, populares ou influentes;
- Não são precipitados/afobados (I Tim 5:22);
- Não se apegam a dinheiro ou a riquezas materiais (I Tim 6:9-10, Sl 37:16, At 3:6, Mt 16:26);
- Paciência (II Cor 6:4, II Tim 2:24, II Pe 1:6);
- Paz (Gal 5:22);
- Piedade (I Tim 4:7 e 6:11, II Pe 1:6);
- Possuem consciência limpa/tranqüila (Rom 13:5, I Cor 10:25, II Cor 1:12, I Tim 1:5,19, 3:9, 4:2, II Tim 1:3, Hb 10:22 e 13:18);
- Pregam sobre Jesus e Sua Palavra e condenam o pecado e a apostasia (Mt 23 e Lc 3:18-20) desafiando a santidade aparente, superficial, hipócrita, fingida, forçada e oca das pessoas;
- Pregam em conformidade com as Escrituras (Is 8:20);
- Repudiam, fogem, condenam... as diversões pecaminosas e os prazeres ímpios sem odiar os que estão em pecado;
- São a minoria (Dt 7:7, Lc 12:32, Mt 7:13);
- São caridosos (II Pe 1:7, Dt 10:11);
- São exemplo para o rebanho (I Tim 4:12 e I Pe 5:3);
- São justos (I Tim 6:11, Mt 1:19, 3:15, 5:6,20, 13:43, 25:37,46, Gal 3:11, Tt 1:8, Tg 5:16);
- São odiados (Mt 10:22);
- São perseguidos (Mt 5:11-12, João 16:2-3);
- São pessoas humildes (II Cor 10:1, Ef 4:2, Fp 2:3, Mt 11:29, Mt 18:4, Atos 20:19, Col 3:12, I Pe 5:5);
- São prudentes (Mt 7:24, 10:16, 24:45 e 25:1-13);
- São servos (Mt 20:26, Lc 22:26);
- São simples (Mt 10:16, II Cor 1:12 e 11:3, Col 3:22);

- Sofrem aflições e tribulações (II Cor 6:4-5, II Tim 1:7 e 4:5, Sl 34:19, Ap 2:9 e 21:4) pelo nome de Jesus (Ap 2:3);
- Sofrem privações (II Cor 6:4);
- Temperança (Gal 5:22, II Pe 1:6);
- Virtude (Lc 6:19, 8:46 e 9:1, At 1:8, 3:12, 8:10 e 10:38, Rm 15:13 e 15:19 e II Pe 1:5).

Assim suas características (personalidade, comportamento, modo/estilo de vida) se identificam com a própria vida de Cristo, dos apóstolos, dos santos e dos profetas (I Cor 4:16 e 11:1, Ef 5:1, Fp 3:7, I Ts 1:6, II Ts 3:9, Hb 6:12 e 13:7); pois eles "são epístolas vivas lidas por todos" (II Cor 3:2).

Assim, como se marca gado para identificar o seu dono, assim a Besta marca os seus com a sua marca e Deus marca os deles com o seu selo (batismo do Espírito Santo). Por se tratar de questão espiritual ou religiosa, a marca também tem que ser espiritual ou religiosa e não uma marca física ou material.

Ezequiel 9:2-6 – "2 E eis que vinham seis homens a caminho da porta superior, que olha para o norte, e cada um com a sua arma destruidora na mão, e entre eles um homem vestido de linho, com um tinteiro de escrivão à sua cintura; e entraram, e se puseram junto ao altar de bronze.
3 E a glória do Deus de Israel se levantou de sobre o querubim, sobre o qual estava, indo até a entrada da casa; e clamou ao homem vestido de linho, que tinha o tinteiro de escrivão à sua cintura.
4 E **disse-lhe o SENHOR**: Passa pelo meio da cidade, pelo meio de Jerusalém, e **marca com um sinal as testas dos homens** que suspiram e que gemem por causa de todas as abominações que se cometem no meio dela.
5 E aos outros disse ele, ouvindo eu: Passai pela cidade após ele, e feri; não poupe o vosso olho, nem vos compadeçais.
6 Matai velhos, jovens, virgens, meninos e mulheres, até exterminá-los; mas **a todo o homem que tiver o sinal não vos chegueis**; e começai pelo meu santuário. E começaram pelos homens mais velhos que estavam diante da casa."

Na Bíblia de Jerusalém (católica), em Ezequiel 9:4, consta a expressão: "com uma cruz" no lugar de "com um sinal" porque na Vulgata, consta a expressão: "com um tav" e no alfabeto hebraico antigo, esta letra ("tav" ou "tau") tinha a forma semelhante a de cruz.

Portanto, o Selo (Marca) de Deus é o batismo do Espírito Santo:

"Resguarda o testemunho, **sela a lei no coração dos meus discípulos**." (Isaías 8:16).

"Mas o que nos confirma convosco em Cristo, e **o que nos ungiu, é Deus**,

O qual também **nos SELOU e deu o PENHOR do Espírito** em nossos corações." (II Coríntios 1:21-22).

"Em quem também vós estais, depois que ouvistes a palavra da verdade, o evangelho da vossa salvação; e, tendo nele também crido, **fostes SELADOS com o Espírito Santo** da promessa.
O qual é o penhor da nossa herança, para redenção da possessão adquirida, para louvor da sua glória." (Efésios [Ef] 1:13-14).

"E não entristeçais o **Espírito Santo de Deus, no qual estais SELADOS para o dia da redenção**." (Efésios 4:30).

Pelo **Dicionário Houaiss:**

"**Penhor**" significa ato ou palavra que assegura o cumprimento de um compromisso, obrigação, promessa etc.; garantia, segurança, prova; empenho ou entrega de coisa móvel ou imóvel como garantia de obrigação assumida.

"**Selado**" - que se tornou efetivo; confirmado, validado; que se concluiu; terminado; bem fechado; cerrado, lacrado.

Percebe-se, assim, que a pessoa que foi batizada com o Espirito Santo está com sua salvação garantida e não há mais nenhuma possibilidade de abandonar Jesus.

Somente Deus é Eterno (I Timóteo [Tim] 6:16). Assim, para que algo ou alguém possa ter eternidade, é necessário estar revestido do Espírito Santo (Hebreus [Hb] 9:14, Romanos [Rm ou Rom] 6:23 e I Coríntios [Cor] 15:53-54). Portanto, somente o selo de Deus (batismo do Espírito Santo) é que possui o caráter/qualidade de imutável, imodificável, inquebrável, indestrutível... (pois Deus além de Eterno, é Perfeito) enquanto que a marca da Besta pode ser retirada, quebrada, anulada, desfeita... a qualquer tempo, pois o diabo é criatura e não Criador.

Todos nós temos marcas no mundo físico e espiritual. As marcas são aquilo pelo que somos conhecidos.

Deus tem dado uma marca espiritual aos que são seus e o diabo está tentando pôr a sua marca em todos. Não se trata de uma questão burocrática, de uma questão religiosa ou denominacional; mas sim o meio pelo qual seremos conhecidos em todo o Universo por anjos e demônios.

"E alguns dos exorcistas judeus ambulantes tentavam invocar o nome do Senhor Jesus sobre os que tinham espíritos malignos, dizendo: Esconjuro-vos por Jesus a quem Paulo prega.

E os que faziam isto eram sete filhos de Ceva, judeu, principal dos sacerdotes.

Respondendo, porém, o espírito maligno, disse: Conheço a Jesus, e bem sei quem é Paulo; mas vós quem sois?

E, saltando neles o homem que tinha o espírito maligno, e assenhoreando-se de todos, pôde mais do que eles; de tal maneira que, nus e feridos, fugiram daquela casa." (Atos 19:13-16).

A marca de Deus é semelhante a crença católica da marca indelével impressa pelo Espírito Santo quando, alguém que é batizado na Igreja Católica quando criança, é Crismado (ato de confirmação posterior). Para os católicos a confirmação feita pela Crisma imprime uma marca espiritual indelével; qual seja, o caráter/personalidade de Jesus, transformando-os em templos do Espírito Santo para habilitar/capacitar as pessoas a serem testemunhas de Cristo e colaboradoras de seu Reino:

"1304 Como o Batismo, do qual é consumação, a Confirmação é dada uma só vez, pois imprime na alma uma marca espiritual indelével, o "caráter", que é o sinal de que Jesus Cristo assinalou um cristão com o selo de seu Espírito, revestindo-o da força do alto para ser sua testemunha." (Catecismo da Igreja Católica).

Mas, essa "confirmação" não se encontra na Bíblia porque é uma tradição de homens. **A marca espiritual de Deus se recebe apenas com o batismo do Espírito Santo, mediante a santificação (II Pedro 1:1-8, Hebreus 11:32-40, Atos 7:44-47, Mateus 5:48, Efésios 4:11-15, Is 6:1-10 e Apocalipse 22:11) após a verdadeira conversão (o Novo Nascimento e proceder em Cristo) e não necessariamente num simples batismo nas águas ou em outro ritual litúrgico qualquer.**

Como o batismo do Espírito Santo produz separação dos santos do mundo. É a marca espiritual que traz consequências no mundo físico (Lucas 24:49 e Efésios 1:13 e 4:31). Uma pessoa batizada com o Espírito Santo possui a personalidade e a mente de Cristo, pois o Espírito Santo fez morada em seu coração, assim, é notória a comparação da pessoa com o ministério de Cristo e dos apóstolos.

"Os quais mostram a obra da lei escrita em seus corações, testificando juntamente a sua consciência, e os seus pensamentos, quer acusando-os, quer defendendo-os;" (Romanos 2:15).

"Porque, quem conheceu a mente do SENHOR, para que possa instruí-lo? Mas nós temos a mente de Cristo." (I Coríntios 2:16).

"Vós sois a nossa carta, escrita em nossos corações, conhecida e lida por todos os homens.
Porque já é manifesto que vós sois a carta de Cristo, ministrada por nós, e escrita, não com tinta, mas com o Espírito do Deus vivo, não em tábuas de pedra, mas nas tábuas de carne do coração." (II Coríntios 3:2-3).

"Sede meus imitadores, como também eu sou de Cristo." (I Coríntios 11:1).

"Guarda o bom depósito pelo Espírito Santo que habita em nós" (II Timóteo 1:14).

"Porque os que são segundo a carne inclinam-se para as coisas da carne; mas os que são segundo o Espírito para as coisas do Espírito." (Romanos 8:5).

"Vós, porém, não estais na carne, mas no Espírito, se é que o Espírito de Deus habita em vós. Mas, se alguém não tem o Espírito de Cristo, esse tal não é dele." (Romanos 8:9).

"E Moisés edificou um altar, ao qual chamou: O SENHOR É MINHA BANDEIRA." (Êxodo 17:15).

"Portanto, vos quero fazer compreender que ninguém que fala pelo Espírito de Deus diz: Jesus é anátema, e ninguém pode dizer que Jesus é o SENHOR, senão pelo Espírito Santo." (I Coríntios 12:3).

Assim como a marca de Deus é espiritual, a marca da Besta também é espiritual. Vez que a marca da Besta é diabólica e como o diabo é um ser espiritual, a sua marca só pode ser também espiritual. Como a marca de Deus transforma a mentalidade e atitude das pessoas, a marca da Besta também o faz. Como os filhos de Deus possuem a mente do Pai, os filhos das trevas possuem os pensamentos do pai deles (João 8:43-44 e 13:2, Marcos 8:33).

Portanto, a marca da Besta não é um chip e nenhum tipo de marca física ou material. Ambos os lados (Deus x Satanás) são pessoas espirituais e suas marcas também são espirituais. O selo de Deus é o batismo no Espírito Santo e a marca da Besta é a possessão demoníaca. Pelos frutos se identifica qual é qual (Mateus 7:16). Os demônios reconhecem de longe a presença do Espírito Santo (Atos 19:11-17 e Lucas 8:27-28) e não precisam de um crachá para isso. A pessoa pensa (cabeça) e age (mãos) de acordo com o espírito que está nela. No AT (Antigo Testamento) Deus falava sobre ter sua Palavra na cabeça e no coração; mas não era cabeça ou coração literais (não era para ter colado/prendido/amarrado as Escrituras impressas em cima do coração ou da cabeça; era para ter na mente/memória e no desejo do coração). Todos os demônios, crenças pagãs, seitas, heresias, rituais satânicos incutem uma ideia em comum (Trindade em oposição ao Deus

único dos judeus) para levar todos ao ecumenismo e permitir a unificação de todas as crenças debaixo de um grande líder mundial.

- http://igrejacibernetica.blogspot.com.br/2005/11/quem-deus-trindade-o-que-plato-tem-ver.html;

- http://igrejacibernetica.blogspot.com.br/2014/06/ecumenismo-ou-religioes-unidas-e-obra.html.

Tanto é assim que a Bíblia diz que "pelos frutos" e não por nenhuma marca física, material, mecânica, pintada, desenhada, eletrônica... é que são identificados e diferenciados o trigo do joio, sobre os quais (ambos – justos e injustos) Deus envia sua chuva (Espírito Santo) concedendo dons, unções, bênçãos, milagres...

É importante reconhecermos as atitudes e os atributos da personalidade de Lúcifer para podermos identificá-lo por de trás de seus inúmeros disfarces, máscaras, aparências angelicais, formas inocentes, corpos humanos e supostas doutrinas bíblicas. Por outras palavras, uma vez conhecendo a pessoa do manipulador ou ventrículo, conseguimos reconhecê-lo por de trás dos fantoches, marionetes e corpos humanos.

- Ele é uma pessoa real e com livre arbítrio;
- Possui intelecto. É inteligente e astuto/sagaz (Gn 3:1, Ez 28:12 e II Cor 11:3): a) Ele foi tentar o próprio Senhor Jesus (Lucas 4:1-12); b) Ele conseguiu permissão de Deus para tentar Jó (Jó 1:6-12); c) A astúcia na tentação de Eva: "você vai se transformar como DEUS" (Gênesis 3:1-7); d) Possui o hábito de dialogar, argumentar, filosofar, usar da lógica e do raciocínio para convencer as pessoas;
- Tem emoções (Ap 12:17): a) orgulho (Isaias 14:12-17); b) ira (Apocalipse 12:17); c) antipatia (Jó 1:9-11); etc.;
- Tem vontade (II Tim 2:26): a) de mandar (Lucas 4:3,9); b) volitude (ato que se determina a vontade). Em sua queda ele demonstra isso: "Eu subirei, Eu dominarei, Eu exaltarei, Eu assentarei..." (Isaias 14:12-14); c) vontade maquiavélica de ser adorado (Mateus 4:9); etc;
- É uma pessoa consciente, lúcida, capaz e moralmente responsável (Mt 25:41);
- Ele é homicida e tem prazer na morte (Jo 8:44 e Hb 2:14);
- Ele é mentiroso e pai da mentira (Jo 8:44 e Gn 3:1-7);
- Ele é um pecador desde o princípio e contumaz e para ele não há perdão (I Jo 3:8);
- Ele é acusador (Ap 12:10 e Jó 1:6-11);
- Ele é adversário de Deus e dos Cristãos (I Pe 5:8);
- É o tentador (Mt 4:11);
- Destruidor (Apoliom – Ap 9:11): seu interior é cheio de violência (Is 14:20 e Ez 28:16);

- Poderoso: dono de grande poder (Is 14:1-2);
- Encarcerador: aprisiona, nos programa, nos coloca numa rotina, não nos permite pensar... (Is 14:17 e II Tim 2:26);
- Opressor (At 10:38);
- Causador dos males (I Jo 3:8 e Ez 28:16);
- Injusto (I Jo 3:10);
- Sedutor: usa da sedução para nos afastar de Deus (Mt 13:22 e Ap 20:10);
- Soberba: querer exaltar-se e colocar-se no lugar de Deus. (Is 14:13-14);
- Enganador (I Tim 4:1, II Jo 1:7 e Ap 12:9 e 20:10);
- Manipulador = ele tenta levar-nos a pensar que ele e/ou Deus não existe(m) (Ap 20:10);
- Cruel (Atos 20:29 e II Tim 3:3);
- Violento (Gn 6:11, Sl 18:48, Ez 45:9, Mc 9:20);
- Feroz (I Pe 5:8);
- Sádico – sente prazer no sofrimento, desgraça e morte alheias;
- Malicioso (Jó 15:35, Sl 34:21, PV 14:32, Jr 9:3, Mt 22:18, At 13:10, Rm 1:28-29, Ef 4:31, Col 3:8);
- Inescrupuloso, Dissimulado. Vaidoso. Exibicionista. Arrogante. Atrevido. Impiedoso. Trapaceiro. Oportunista. Teimoso. Rebelde. Insubmisso. Invejoso. Ingrato. Insatisfeito. Ganancioso...

Um dos atributos de Satanás é a sutileza. Como um mestre dos disfarces, ele se disfarça tão bem que, frequentemente, a pessoa que está sendo tentada nem se dá conta de seu envolvimento, da cilada, da tentação.... pois, ninguém tropeça em montanha, mas, sim, tropeçamos em coisas pequenas, aparentemente simples, irrelevantes, insignificantes e inofensivas. São os detalhes/minúcias que fazem a diferença para podermos distinguir o original e verdadeiro do falsificado.

Recordemos que a razão de existência do falso é justamente a existência do verdadeiro, ou seja, o falso não pode existir se não existe o verdadeiro, pois o falso é a perversão do verdadeiro. Ainda mais, a Bíblia nos adverte que essas imitações seriam quase idênticas as originais, ao ponto que poderiam até mesmo enganar os escolhidos se não fosse a revelação divina do Espírito Santo (Mt 24:24). Assim, por exemplo, não é porque determinado produto “Made in China” ou “Made in Paraguay” seja idêntico ao original que isso o tornaria um original, pois apesar de aparentemente serem a mesma coisa, os falsificados não foram feitos do mesmo modo, não foram feitos no mesmo lugar, com os mesmos materiais, com a mesma qualidade, pelo mesmo fabricante, não tiveram os mesmos cuidados, não respeitaram a lei, não recolheram os tributos pertinentes, não possuem a mesma garantia, não possuem a mesma assistência técnica, não possuem

Nota Fiscal, não recebem a proteção do Código de Defesa do Consumidor, etc.

Não podemos achar que Imosec (remédio para diarreia) e Ivomec (antiparasitário de uso animal) são a mesma coisa, servem para a mesma coisa ou que dá na mesma. Não é porque as coisas são parecidas ou semelhantes que significam que são a mesma coisa. Até mesmo irmãos gêmeos univitelinos não são exatamente idênticos. Os pais sabem distinguir seus filhos gêmeos "idênticos" por meros detalhes sutis, discretos, suaves... que passam desapercebidos aqueles que não estão familiarizados com eles. Assim devemos ter intimidade com a Palavra de Deus para que saibamos discernir entre o certo e o errado e o verdadeiro e o falso.

Assim a finalidade do falso é prejudicar o original, ou seja, fazer as pessoas preferirem o falsificado por ser mais fácil, rápido, simples, barato, popular, etc., para que o original seja esquecido, ignorado, desprezado e deixado de lado.

Já o verdadeiro pode muito bem existir sozinho, pois não depende do falso para existir, vez que existe por si próprio, ou seja, o verdadeiro é verdadeiro pelas suas próprias natureza, essência e existência.

Satanás não se manifesta para você em todo o seu horror, dizendo: "Eu sou o diabo. Eu estou aqui para lhe atrair a uma armadilha para que eu possa destruí-lo". Pelo contrário, ele se esconde nas sombras e atrás de máscaras e disfarces. Nós nem percebemos que ele está lá nos bastidores, puxando as cordas e manipulando as situações. Às vezes, ele age como se desejasse o nosso bem. Lembre-se de Eva, no Jardim do Éden. Satanás sugeriu a ela que Deus era egoísta e que estava guardando algo que seria bom para ela. Ele usou a mesma tática quando tentou a Jesus. Como um pescador experiente, que sabe exatamente qual isca usar. Satanás conhece suas áreas de fraqueza (pai da psicologia e de todas as ciências) e, assim, as usa. Ele pode aparecer como um anjo de luz (II Cor 11:14), uma donzela em apuros, a solução para os seus problemas financeiros, a resposta para a insatisfação com a sua própria aparência...

> "O que receio, e quero evitar, é que assim como a serpente enganou Eva com astúcia, a mente de vocês seja corrompida e se desvie da sua sincera e pura devoção a Cristo." (II Coríntios 11:3).

Em Gênesis notamos a sutileza e sabedoria de Satanás, que contou uma mentira tão bem contada a Adão e Eva que fez ela parecer uma verdade. Pregou que o homem seria como Deus (soberba). Em Mateus percebemos que ao tentar o Senhor Jesus ele usava passagens bíblicas distorcendo-as (o que hoje ainda faz por ser o **pai da Teologia e o primeiro intérprete e pregador da Palavra de Deus, só que distorcida**). Assim, o diabo usa até a própria Palavra de Deus para nos destruir. Ele usa de todos os meios possíveis para atingir o seu fim, até as coisas santas de Deus. Em Jó fica claro a intenção dele de nos acusar perante Deus e de procurar a nossa destruição.

Na sedução de Eva (Gn 3), Lúcifer utilizou-se das seguintes estratégias:

1) Usou um disfarce para não ser reconhecido. Ele não se apresentou na sua forma atual e real, mas usou o corpo de uma criatura aparentemente inocente e insuspeita, na qual ele estava escondido para poder se aproximar e receber a atenção de Eva sem levantar suspeitas, receio ou desconfiança;

2) Mesclou a verdade com a mentira. O que Satanás falou para Eva não foi totalmente mentira. Realmente os olhos de Eva se abriram para aquilo que estavam cegados (nudez e sexo) e adquiriu conhecimento (deixou de ser ingênua), pois se ele somente falasse a mentira não conseguiria enganá-la. Como, por exemplo, ninguém acreditaria numa cédula de onze reais, pois tal não existe;

3) Se aproveitou da curiosidade. Satanás instigou a curiosidade de Eva para que ela quisesse conhecer e experimentar para saber como é, pois o diabo costuma dizer que você não pode falar mal do que não conhece. Satanás fez, assim, que Eva não achasse suficiente a Palavra de Deus de que tal coisa era errada e levava à morte. Ela quis provar aquilo para poder tirar suas próprias conclusões e ter certeza de que realmente era como Deus disse. Não lhe foi suficiente o que Deus lhe disse, ela queria provas e queria saber o porquê das coisas;

4) Escondeu a verdade. O diabo não falou expressamente seus planos e o que aconteceria. Ele pulou a parte desagradável e ruim. Ele falou somente a parte sedutora como um traficante de drogas que enfatiza o lado bom dos psicotrópicos e esconde os seus efeitos nefastos para convencer a pessoa a experimentar. Por outras palavras, o diabo não disse à Eva que ela nunca morreria (mas que não morreria naquele momento) por fazer aquilo e nem disse que Deus não iria ficar irado com aquilo;

5) Sutileza. O diabo usou a sua principal tática, qual seja, fazer a pessoa desobedecer a Deus sem se dar conta. Não importa quais sejam as razões, motivos, objetivos, circunstâncias... a pessoa tem que ficar sempre somente com o que Deus disse apesar de tudo o mais falar o contrário. Deus disse que é assim, é assim e pronto. Não há o que se discutir, criticar, questionar, debater, confabular, filosofar, especular... Basta o que Deus disse. A Palavra de Deus é o

suficiente. Deus disse para não fazer aquilo, mas Eva deu ouvidos (obedeceu) a Lúcifer ao invés de obedecer a Deus e fez o que Deus ordenou que não fizesse. Eva deveria ter recitado a Palavra de Deus em sua defesa como Cristo fez em sua defesa ao ser tentado pelo Maligno;

6) Dúvida ou incerteza. O diabo fez Eva duvidar do que Deus disse. Deus quer que creiam plenamente e somente Nele e no que Ele diz. Basta a pessoa duvidar de um til, jota, vírgula, artigo, palavra ou frase do que Deus disse que o diabo já conseguiu seu intento. A dúvida é o contrário da fé. O diabo é o pai do "se", "talvez" e "será?". Quando Satanás tentou Cristo, ele nem falou a verdade e nem falou a mentira, ou seja, ela falou a verdade distorcida. Costuma usar de frases de quem não acredita, mas também não desacredita. Fala como um verdadeiro filósofo (pois é o pai da Filosofia) e demonstra que conhece as Escrituras de cor, o que prova que Satanás também prega a Bíblia, só que distorcendo o seu sentido, significado, objetivo, razão, finalidade...

7) Sedução da lógica e do raciocínio/razoamento humanos. O diabo usou raciocínio/razoamento humanos para convencer Eva de que o que ele dizia fazia sentido e era a coisa mais lógica, racional, inteligente, sensata, razoável, plausível... a ser feita;

8) Convicção em negar a Palavra de Deus. O diabo afirma com convicção, como se não tivesse a menor sombra de dúvida, como se fosse certeza absoluta, como já tivesse sido completa e definitivamente provado, como se fosse algo inquestionável, indubitável, irrefutável... que a Bíblia está errada;

9) Egocentrismo/egoísmo. O diabo fez Eva colocar seus próprios interesses, proveitos, desejos, prazeres, satisfações, necessidades... acima de Deus. Fez Eva pensar e se preocupar mais em si ou consigo mesma do que com Deus e o próximo. O verdadeiro Cristão é altruísta, ou seja, não pensa em si próprio, mas primeiramente em Deus sobre todas as coisas e se dedica ao próximo como a si mesmo, ou seja, faz ao próximo o que esperaria que fizessem por si e não faz ao próximo o que não queria que fizessem consigo;

10) Sedução do poder. O diabo disse a Eva que "sereis iguais a Deus" despertando-lhe o desejo pelo poder e autoridade à qualquer preço/meio e de qualquer modo/forma, ou seja, de se igualar a Deus e deixar de ser apenas uma de suas criaturas. Por outras Palavras, lhe instigou à rebelião, pois quem não se conforma em ser apenas um filho, servo, criado, súdito... mas quer ser como seu Senhor ou tomar o lugar de seu Senhor, constitui-se num rebelde, vez que não reconhece e não se sujeita à autoridade do seu Senhor;

11) Sedução pela independência. Satanás incutiu a ideia de que Eva poderia ser independente de Deus, ou seja, de se livrar, não depender, não precisar... de Deus. Por outras palavras, que poderia ser autossuficiente, vez que teria os mesmos conhecimentos e poderes de Deus. Desse modo, Satanás instigou Eva a praticar a rebelião, insubordinação, insubmissão... Satanás pregou uma vida alternativa a dada por Deus consistente na liberdade de Deus, na igualdade a Deus e na fraternidade entre os rebeldes;

12) Concessões. O diabo costuma nos conduzir a fazermos concessões ou acordos para evitarmos conflitos, atritos, desentendimentos, confrontos, ataques... com o que nos torna apóstatas.

Outra das principais mentiras de Satanás, que ele usou contra Eva e tentou usar contra Jesus, é de que Deus não dará coisas boas a seus

filhos ou que a obediência a Deus jamais trará felicidade. Todavia, a Bíblia diz que Deus sente prazer em que se obedeça a sua Palavra. Para, Deus, obedecer é melhor que sacrificar. Quando obedecemos agradamos a Deus e com certeza sentimos um censo de realização que nos proporciona o sentimento de contentamento. A prosperidade vem pela obediência, da mesma forma que a rejeição vem pela desobediência. (I Sam 15:1-31).

Satanás, o inimigo de nossa alma, é muito astuto e um perito em armar-nos ciladas e **lança mão de qualquer coisa e de tudo que está ao seu dispor para nos afastar de Cristo**. Satanás não economiza munição e nem soldados, mas usa de todo o seu arsenal disponível para nos destruir.

A principal atividade de Satanás, com o auxílio de seus demônios, é opor-se e esconder a obra de Deus (Mateus 13:39; Marcos 4:15; II Coríntios 11:14,15; II Tessalonicenses 2:9,10; Apocalipse 2:10 e 3:9), mediante diversas estratégias (Gênesis 3:1-7, Mateus 4:1-11 e Jó 1:1-22).

Satanás e seus demônios realizam **tentações personalizadas**, ou seja, por nos conhecerem bem de tanto nos observarem e estudarem antes, sabem exatamente quais são nossas fraquezas, vulnerabilidades, insatisfações, problemas, dificuldades, desejos... e, assim, acabam por nos oferecerem justamente aquilo que com maior probabilidade iremos aceitar por causa de nossa personalidade, situação, circunstâncias, ambiente, contatos, trabalho, íntimos... que eles conhecem em razão de tanto nos observarem.

São inúmeras as atitudes de Satanás para nos afastar de Jesus e nos destruir, assim, infra, elencamos apenas algumas das mais comuns para darem uma noção de como ele age.

O diabo procura mostrar aos outros que ele não existe; pois se ele existir; sua contrapartida (a saber, Deus) também existirá. E é evidente que ele, como estando perdido, vai procurar levar junto com ele o maior número de pessoas que puder; por isso, ele se esconde do homem, pois se aparecer explicitamente a qualquer ser vivo, este apegar-se-á a Jesus para fugir ao mal.

É perfeita a analogia bíblica entre luz (Deus) e trevas (diabo). Quem está na luz enxerga o que acontece ao seu redor, enquanto que quem não está na luz não enxerga nada, e por isso não sabe que está no mal. Por isso, o diabo é tão difícil de ser provado, vez que **o maior truque do diabo é convencer o mundo de que ele não existe**.

A cada dia que passa, o número de pessoas que acreditam na existência de Satanás vem diminuindo cada vez mais. Entre os mais intelectuais, Satanás não passa de um mito. Até mesmo pessoas que professam ser religiosas não acreditam na existência do diabo. Mas Satanás não se importa com a descrença das pessoas, pois ao ignorá-lo, elas estão também ignorando os seus muitos enganos que levarão tais pessoas a perderem a vida eterna que Cristo gratuitamente deseja conceder-nos. Imagine que você dissesse que não acredita que sua casa possa ser roubada. Então você deixa a porta aberta o tempo todo, não se importa que saibam o que você possui em casa, etc. Estaria você por esta atitude deixando sua casa mais segura? Se você não acreditasse na existência de ladrões, você estaria livre de ser assaltado por eles? O mesmo ocorre com aqueles que ignoram a existência de Satanás. As pessoas não se preocupam em fechar as portas de sua alma a Satanás, e ele entra e faz o que quiser com a vida delas.

Assim, como qualquer ladrão, também o diabo quer passar despercebido para que suas ações funestas não sejam impedidas e ele não seja combatido. Muitos simploriamente dizem: “Deus existe, mas o diabo é fruto da imaginação dos homens”. Quem assim fala acaba por chamar Jesus de mentiroso, louco ou equivocado, pois Jesus deu nome ao oponente e o descreveu.

Trata-se de um ato de extrema ignorância julgar-se mais inteligente, esperto, sábio, astuto, culto, experiente, forte... do que Satanás, pois ele nos é muito superior em força, forma, inteligência, experiência, poder e habilidades. Somente Jesus é capaz de não só detê-lo e vencê-lo, mas também de destruí-lo completamente e desfazer todas as suas obras maléficas.

Então, devemos temer a Satanás? Não, pois ele já foi vencido por Cristo e pode ser vencido por nós também se estivermos em harmonia com Jesus,

mas não devemos provocá-lo, zombar dele, ignorá-lo e nem achar que ele é um inimigo fácil de ser vencido. Nunca devemos buscar um confronto com ele, como fazem várias igrejas pentecostais que convidam Satanás para vir as suas igrejas a fim de ser derrotado por homens que se dizem preparados. Só por esta atitude da parte destes homens, já se pode ver que eles estão sem Cristo. Jesus disse que “muitos” quando Ele voltar lhe dirão que expulsaram demônios em Seu nome e Ele dirá que nunca conheceu tais homens. No original em grego está escrito: apartai-vos de mim vós que não têm lei, ou seja, que não guardam os meus mandamentos. (Mt 7:22-23).

A principal arma de Satanás é a mentira, pois ele é o pai da mentira (João 8:44). Ele mente desde o jardim do Éden e mentirá até a sua morte. Ele é o mestre do engano. E sempre está em ação. Ele é teimoso, persistente e nunca descansa. No entanto, poucos são os que vigiam para não serem enganados por ele. O apóstolo Pedro diz: “Sede sóbrios, vigiai, porque o diabo, vosso adversário, anda em derredor, bramando como leão, buscando a quem possa tragar.” (I Pedro 5: 8).

O diabo é um psicólogo milenar (aliás, pai da psicologia, pois estuda os nossos pensamentos, comportamentos, desejos, reações... a milênios) que trabalha incansavelmente para nos fazer acreditar nas suas mentiras. Eis a razão por que o apóstolo Paulo disse: "A palavra de Cristo habite em vós abundantemente, em toda a sabedoria, ensinando-vos e admoestando-vos uns aos outros, com salmos, hinos e cânticos espirituais, cantando ao Senhor com graça em vosso coração". (Col 3:16) Lembre-se, Satanás sempre tentará ganhar a batalha em nossa mente, fazendo com que prevalece em nós as suas mentiras. Não foi por acaso que Paulo, o apóstolo que nesta batalha espiritual deveríamos tomar toda a armadura de Deus, inclusive o "capacete da salvação" (Ef 6:13,17), que é a proteção para nossa mente.

As mentiras de Satanás são mais efetivas quando ele consegue misturá-las com a verdade ou com as Escrituras. Sérios erros são cometidos em relação a Satanás porque as pessoas pensam que ele é uma criatura feia, terrível e sacrílega, que os homens naturalmente só teriam a odiar. Isso não é verdade, porque, embora sua natureza seja como a de um leão que brama a procura de quem possa devorar, sua aparência é como a de um lindo anjo de luz. É também muito religioso e, como quer o lugar de

Deus, incentiva a religiosidade/espiritualidade, mas desvia a adoração para si. **Seu truque básico é tentar fazer os homens virem a Deus pelas obras (mérito) e não por Cristo (misericórdia). Os homens, ao fazerem isso, na verdade, não veem a Deus, mas a Satanás.**

A criatividade e imaginação de Satanás são imensas, desse modo suas mentiras são inúmeras, sendo humanamente impossível enumerá-las ou prever todas. Precisamos parar de darmos ouvidos às palavras do diabo e começarmos a crer nas Palavras de Jesus. Assim, nossa única atitude defensiva (além de confiarmos plenamente em Jesus e Sua Palavra), é conhecermos as Escrituras, pois **quanto melhor se conhece a Palavra de Deus (e não a dos homens e suas Teologias e interpretações), mais fácil é detectar as mentiras de Satanás, rejeitar suas ofertas e escapar de suas ciladas.**

Infra, apenas **algumas das mentiras do diabo** para servir de exemplo de sua astúcia:

1) “Todos são filhos de Deus” (cf. João 1:12.13): mentira, a pior de todas, a Bíblia diz que os únicos que são filhos de Deus são aqueles que crêem no Senhor Jesus. Quem são os filhos do diabo? (Leia Efésios 2:1-3, 12; II Timóteo 3:2-7). Todo aquele que comete o pecado do diabo, a saber, a soberba, procede dele (do diabo). Todo aquele que exalta a si não pode ser de Deus. Todo homem alheio de Deus, é filho do diabo, e isto, o fazem sem nenhuma intenção, porque ele não tem entendimento das coisas de Deus.

2) “O diabo não existe” (cf. I Pedro 5:8): Deus, que não pode mentir, diz que ele existe.

3) "Seja bom, faça o seu melhor, e tudo sairá bem" (cf. I João 5:12). Para sermos salvos a Bíblia diz que devemos aceitar a obra de Jesus em nossas vidas. A Bíblia também diz que somos salvos pela fé e não pelas obras que fizemos (cf. Efésios 2:8-10). Obras boas não salvam ninguém, o ÚNICO QUE SALVA É JESUS. Leia II Tim 3:2-7. Muitos homens aprendem muitas coisas (e podem até, humanamente, ser muito sábios), mas não podem chegar ao conhecimento da verdade bíblica (Jesus), porque estão em trevas (espiritualmente) e precisam ser levados à Luz; portanto "conhecereis a Verdade [Jesus] e a Verdade vos libertará" (Jo 8:32). "Se, pois, o Filho vos libertar, verdadeiramente sereis livres" (Jo 8:36). Jesus pode nos libertar de toda opressão demoníaca, basta crermos Nele.

4) "Deus é bonzinho, não preciso me preocupar" (cf. Salmo 145:17): metade da verdade é mentira; Deus é bom (disso não duvidemos), mas Deus é amor (Deus pode deixar de te amar? Deus se alegra em te ver errante?), só que Deus também é santo (Deus pode habitar junto com o pecado sendo santo?), Deus também é justo (e em todos seus caminhos, pode ele colocar em seu Reino alguém que não está limpo -a saber, quem não aceitou o sacrifício de Jesus na cruz-? Pode Deus sendo justo deixar de punir o pecado? Pense! Leia Ezequiel 18:32.

5) "Jesus foi um grande homem, e um exemplo de vida" (João 1:1,14) MENTIRA, Jesus foi muito mais que um homem, Jesus foi homem-Deus (100% homem [corpo Ungido] e 100% Deus [Espírito Santo]). Muito mais que um exemplo de vida, Jesus é a própria vida (João 14:6), Jesus traz a vida (I Coríntios 15:45).

6) “O homem é basicamente bom”. Cada pessoa é um pecador por nascimento e por escolha. "Como está escrito: não há justo, nem sequer um." "Pois todos pecaram e carecem da glória de Deus." (Romanos 6:10,23).

7) "O bom Deus faz vistas grossas quanto aos nossos pecados.” O castigo pelo pecado é a separação eterna aos nossos pecados de Deus, "Porque o salário do pecado é a morte, mas o dom gratuito de Deus é a vida eterna em Cristo Jesus nosso Senhor." (Romanos 6:23).

8) “Se nós tentarmos fazer o que é certo, certamente Deus nos deixará entrar no céu.” Nenhum homem pode alcançar a perfeição que Deus requer para entrar no céu. "Porque pela graça sois salvos, mediante a fé; e isto não vem de vós, é dom de Deus; não de obras, para que ninguém se glorie." (Efésios 2:8-9).

9) “O sofrimento que passamos aqui na terra é o único julgamento de Deus quanto ao pecado.” Deus demonstrou seu amor por nós enviando Seu Filho para pagar o castigo eterno do nosso pecado. "Porque Deus amou ao mundo de tal maneira deu o seu Filho unigênito, para que todo aquele que nele crê não pereça, mas tenha a vida eterna." (João 3:16).

10) “Nós precisamos ter fé em nós mesmos.” Precisamos crer somente no Senhor Jesus Cristo como Salvador pessoal para sermos salvos. "Se com a tua boca confessares a Jesus como Senhor, e em teu coração creres que Deus O ressuscitou dentre os mortos, serás salvo." (Romanos 10:9).

11) “Eu sempre fui crente.” Somente quando colocamos nossa fé em Cristo é que nos tornamos um cristão genuíno. "Por isso quem crê no Filho tem a vida eterna; o que, todavia, se mantém rebelde contra o Filho não verá a vida, mas sobre ele permanece a ira de Deus." (João 3:36).

12) “Não podemos realmente ter certeza do céu.” Podemos saber agora que temos a vida eterna. "Estas coisas vos escrevi a fim de saberdes que tendes a vida eterna, a vós outros que credes em o nome do Filho de Deus” (I João 5:13).

13) Ele ensina ou faz com que o homem sinta que é imortal. Está foi a primeira mentira que ele contou aos seres humanos (Gn 3:4). Quase todas as pessoas no mundo inteiro acreditam que são imortais, ou seja, quando o corpo morrer, elas continuarão a viver uma outra vida onde o corpo não será mais necessário. Mas a Bíblia diz que só Deus é imortal (I Timóteo 6:16).

14) Satanás joga tão baixo que ele chega ao ponto de aparecer algumas vezes, como na forma de uma pessoa que já morreu. E ele faz essa imitação tão perfeita que muitas pessoas caem no engano dele (espiritismo, médiuns, supostas aparições dos santos mortos, etc). “Quando, pois, vos disserem: Consultai os que têm espíritos familiares e os adivinhos, que chilreiam e murmuram: Porventura não consultará o povo a seu Deus? A favor dos vivos consultar-se-á aos mortos?” (Isaías 8:19).

15) Ele tenta nos convencer de que é preciso ser um pastor ou missionário para pregar o Evangelho. E nosso erro é aceitar essa mentira e desenvolver uma atitude de "patinho feio" no reino de Deus, se julgando incapaz ou até não responsável pelo evangelismo.

Medo, receio, timidez ou vergonha. Se o Diabo conseguir deixá-lo "morrendo de medo" antes de você começar, então você nem sequer começará e nunca realizará o que Deus quer que faça. Por isso o Diabo pega todo o seu arsenal e recorre a todos os seus truques sujos para tentar evitar que você comece a servir a Deus, porque ele calcula que se conseguir evitar que você comece, então você nunca servirá a Deus.

Orgulho. Quando nos permitimos pensar que somos melhores que os outros, somos os mais capazes, os mais preparados, quando achamos que o que os outros fazem não se compara ao que fazemos, isso tanto no meio secular, quanto dentro da própria igreja, se constituí pecado (Pv 21:4).

Paixões (sentimento ou emoção levados a um alto grau de intensidade, sobrepondo-se à lucidez e à razão). Quando nos deixamos levar pelas paixões, sejam elas quais forem, acabamos abrindo uma grande brecha para o inimigo das nossas almas ocupar um espaço em nossas vidas. Como vemos na definição, a paixão nos impede de ver as coisas de forma lúcida, bloqueia a nossa razão, e isso muitas vezes nos leva a cometer atos (ou pecados) que nos impedem de nos apresentarmos diante de Deus. Ou ainda, quando nos permitimos dar muito mais atenção a outras coisas que não as do Reino de Deus, isso também acaba produzindo bloqueios em nossas vidas (Mateus 6:33 "Mas, buscai primeiro o reino de Deus, e a sua justiça, e todas estas coisas vos serão acrescentadas"). E é desejo de Deus que estejamos sempre conscientes ("Rogo-vos, pois, irmãos, pela compaixão de Deus, que apresenteis os vossos corpos em sacrifício vivo, santo e agradável a Deus, que é o vosso culto racional" - Romanos 12:1), quando nos apresentamos diante de Deus devemos sempre estar bem conscientes de quem é o Senhor e o que desejamos na sua presença.

Mágoa, rancor ou ressentimento. Esse sentimento é uma grande cadeia que é usada para nos impedir de fluir na presença de Deus. E a mágoa sempre vem acompanhada daquela falsa certeza de que nós é que estamos certos e o outro é quem errou conosco, e por isso é o outro que tem de vir se acertar conosco e não nós com ele. Na verdade, para Deus quem magoou ou deixou de magoar não faz a mínima diferença, o que Ele quer é que nos concertemos para poder estar diante Dele. (Mt 5:23-24).

Pesares. Quantas vezes por causa do grau da dificuldade que estamos enfrentando, acabamos por fim nos considerando os “seres mais sofredores da face da Terra”. João 16:33 - “Tenho-vos dito isto, para que em mim tenhais paz; no mundo tereis aflições, mas tende bom ânimo, eu venci o mundo”, o próprio Jesus está dizendo aos seus discípulos que: quem está no mundo, está sujeito as dificuldades deste mundo, más quem está em Jesus já venceu essas dificuldades, porque o próprio Jesus já venceu o mundo, portanto mesmo que as dificuldades apareçam, se estou em Jesus não devo me sentir o maior sofredor da face da Terra porque com Jesus já venci o mundo.

Endurecimento dos corações, o que acaba nos impedindo de nos apresentarmos diante de Deus. Para que não continuemos afastados de Deus precisamos quebrantar o coração. E como eu quebranto o meu coração? Arrependendo-me do meu pecado e perdoando aquele que me tem ofendido. Mesmo que eu peque o Senhor nunca vai me abandonar ou quebrar a sua aliança comigo. Ele sempre vai esperar que eu reconheça que errei, me arrependa e peça-Lhe perdão e é isso que é ter um coração quebrantado, é quando eu reconheço que é apenas de Jesus que vem o meu socorro, o alívio para minha alma e o perdão dos meus pecados. Ezequiel 36:26 - “E dar-vos-ei um coração novo, e porei dentro de vós um espírito novo; e tirarei da vossa carne o coração de pedra, e vos darei um coração de carne”.

Satanás usa até líderes da igreja para colocar nos ombros dos fieis fardos pesados de carregar. Satanás não se importa nem um pouco com a espiritualidade, religiosidade, trabalhos da igreja, leitura ou pregação da Bíblia... desde isso mantenha as pessoas ocupadas, distraídas, cegadas, equivocadas, longe da Verdade e afastadas de Jesus, apesar de tanto falarem Dele.

Fazendo uma leitura atenta de Êxodo 5:15-20 descobrimos que os capatazes do povo de Deus eram israelitas também, isto significa que eram seus próprios irmãos que exigiam do povo hebreu a produção da cota diária de tijolos para o Faraó do Egito.

Vivemos continuamente sob pressão e correndo contra o tempo. Não temos tempo suficiente para fazermos tudo o que devemos, necessitamos ou queremos. Em tudo nesse mundo há a questão do trabalho (esforço físico e estudos), necessários para nosso sustento, necessidades básicas e fornecimento de recursos e materiais para outras atividades. O trabalho nos ocupa, consome tempo e suga nossas forças, causando-nos cansaço e necessidade de descansarmos. Por isso temos sentimento de culpa sempre que não estamos correndo de um lado para outro fazendo alguma coisa produtiva. Quantas vezes agimos exatamente como Marta (preocupada, ocupada e agitada no serviço de casa), sem nunca termos tempo para sentar-nos aos pés de Jesus como sua irmã Maria fez. E o que ela (Marta) estava fazendo (preparando de coração uma excelente, nutritiva e deliciosa refeição para Jesus) era perfeitamente legítimo. Mas o Senhor Jesus afirmou que Maria escolhera a boa parte (Lc 10:39-42). Muitos ditos cristãos estão precisando aprender a resistir à tentação de se entregar a certas atividades que apenas drenam suas forças espirituais e não produzem os frutos almejados por Deus. Alguns pensam que quanto mais movimento, obra ou barulho fizer, mais realizarão para Deus. Entretanto, isso não é vida, mas mera atividade ou ocupação. Nesse empenho de realizar a obra do Senhor, muitas vezes, perdemos o Senhor da obra e ainda por cima deixamos nosso povo esgotado. Muitas dessas atividades que ocupam tanto de nosso tempo são inúteis e outras simplesmente ridículas. Mas aqueles que gostam de ver todo mundo atuando, irão retrucar: “Isso é bom para promover a comunhão entre os irmãos.” Mas o fato é que a maior parte das atividades existentes nas igrejas em geral não contribui em nada para realizar a verdadeira obra de Cristo na Terra. Na maioria dos lugares é praticamente impossível conseguir que alguém assista a uma reunião onde a única coisa a acontecer é a comunhão com Deus. O próprio fundador da Igreja, ou seja, Cristo, condenou e criticou duramente os líderes que colocam fardos tão pesados que nem eles mesmos conseguiam carregar: “Atam fardos pesados e difíceis de carregar e os põem sobre os ombros dos homens; entretanto, eles mesmos nem com o dedo querem movê-los.” (Mt 23:4).

Assim, o diabo faz dos líderes sem nenhuma visão espiritual, capatazes do povo de Deus, para que coloquem tarefas e mais tarefas. Portanto, o diabo ordena encher os ombros dos crentes com programas e programações, um sem fim de trabalhos e afazeres, que parecem ser de dedicação ao

Senhor, mas na realidade não passam de atividades para passar o tempo e transformar a igreja num clube social, local de fazer e encontrar amigos, troca de fofocas, captar clientela, conseguir emprego, realizar vendas, fazer terapia, ponto de encontro para sair para a balada...

Satanás nos faz desviarmos a atenção, ou seja, nos tira a concentração das coisas de Deus. Qualquer coisa que controla a sua atenção domina sobre a sua vida. "Tão-somente sê forte e mui corajoso para teres o cuidado de fazer segundo toda a lei que meu servo Moisés te ordenou; dela não te desvies, nem para a direita nem para a esquerda, para que sejas bem-sucedido por onde quer que andares" (Js 1:7). Não desviar nem para direita nem para a esquerda é o mesmo que manter o foco. Não podemos olhar para os lados e nem tampouco para trás. Isaías 43:18 diz: "Não vos lembreis das coisas passadas, nem considereis as antigas. Eis que faço coisas novas, que está saindo à luz; porventura, não o percebeis?" Tire o seu foco do passado, coloque-o no presente. Tire o seu foco da morte, ponha-o na vida. Ponha a sua atenção nas coisas positivas e não nas negativas. O seu foco determina a sua atitude. Estamos sempre focando aquilo que pensamos que não temos ou não somos, mas Deus sempre toma o que consideramos insignificante e faz disso uma solução. **Precisamos aprender a reconhecer, valorizar e sermos gratos por tudo aquilo que Deus nos faz, concede e dá**.

E **a lista prossegue imensamente**, desse modo, enumeramos apenas mais algumas abaixo.

- Matar, roubar e destruir (Jo 10:10).
- Semeia a semente do mal (Mt 13.38-39).
- Cega as mentes (entendimento) dos homens para a Bíblia (At 26:18, 2 Cor 4:4 e II Tim 2:26).
- Escurece o entendimento (Ef 4:18).
- Tira a Palavra que é semeada (Mc 4:15).
- Arrebata a Palavra plantada nos corações e mentes (Lc 8:12).
- Desvia as pessoas do Evangelho (II Co 11:3; I Ts 3:5).
- Obstrui os servos de Deus em seus ministérios (I Ts 2:18).
- Cria falsos líderes para perverterem a verdade do Evangelho (Mt 13:38-39, II Co 11:4,14, Gálatas 1:8 e II Pe 2:1-19).
- Disfarçar-se de anjo de luz (II Coríntios 11:14).
- Disfarçar-se de um dos santos (Gálatas 1:8).
- Anda ao derredor como leão rugindo (I Pe 5:7-9).
- Transforma-se num falso Cristo (anti-Cristo).

- Imita as manifestações do Espírito Santo, ou seja, realiza falsos sinais, prodígios, maravilhas e milagres (Mt 7:21-23, 24:11,24; II Cor 11:13-15; II Ts 2:8-10).
- Engana as nações (Ap 20:3).
- Governa as nações através de seus enviados (Dn 10:13).
- Ele se prepara para a "BATALHA DO ARMAGEDOM" (Ap 16:13-14).
- Usa homens para se opor à obra de Deus (Ap 2:13 e Jo 7:30).
- Promove lutas e dissensões entre os que crêem (Ef 6:10-18 e I Cor 1:10).
- Acusa e planta dúvidas (Gn 3:1-5 e Ap 12:10).
- Por causa do orgulho, leva a mentir (At 5:3).
- Influencia na área do sexo, levando ao pecado (I Co 7:5 e Gl 5:19).
- Leva os homens a ficarem ocupados com este mundo (I Jo 2:15-17 e 5:19).
- Desperta o orgulho das questões espirituais (I Tim 3:6).
- Cria facções na Igreja, nos lares e comunidades (Tg 3:14-16).
- Corrompe, cauteriza e aprisiona as mentes (II Cor 10:4-5).
- Faz esfriar o amor entre os irmãos, tornando-os egoístas (Mt 24:12-14).
- Põe obstáculos aos Cristãos (1 Ts 2:18).
- Causa cansaço e desânimo para a obra de Deus (II Cor 4:8,16 e Ap 3:9).
- Causa doenças/enfermidades físicas e mentais (Jó 2:7, Mc 5:1-15, 9:17-18 e Lc 11:14) e todo o tipo de males (Mc 7:26).
- Tenta o crente a mentir (I Tess 2:18).
- Usa demônios para tentar derrotar os servos de Deus (Ef 6:11-12).
- Tenta o crente a imoralidade (I Cor 7:5).
- Tenta as pessoas à desobediência a Deus (Gn 3:4-5).
- Calunia os santos (Jó 1:9-11).
- Semeia o joio entre o crente (Mt 13:38-39).
- Levanta perseguições entre os crentes.
- Os demônios tentam subverter os propósitos de Deus (Dn 10:10-14 e Ap 16:13-16).
- Os demônios tentam estender a autoridade de Satanás, cumprindo sua vontade (Ef 6:11-12).
- Demônios podem causar doenças.
- Demônios podem possuir animais (Mc 5:13).
- Demônios podem possuir homens (Mt 4:24).
- Os demônios se opõem ao nosso crescimento espiritual (Ef 6:12).
- Demônios disseminam doutrinas falsas (I Tim 4:1).
- Satanás tem uma hierarquia bem organizada de demônios (Ef 6:11-12).
- Satanás pode influenciar em nossas decisões, palavras e gestos (como no caso de Pedro; Jesus lhe disse: "arreda-te Satanás"); ou pode possuir a uma vida e sobre ela ter controle (como em Lucas 9:37-43).
- Faz falsas promessas (Gn 3:5).
- Faz mau uso das Escrituras (Mt 4:6).
- Possui planos astutos (II Cor 2:11).
- Manipulador = ele tenta levar-nos a pensar que ele e/ou Deus não existe(m) (Ap 20:10).
- Usa das ciências e tecnologia para fazerem os homens desacreditarem na Bíblia e em Deus.
- Tenta convencer os homens de que ele não existe.
- Tenta esconder ou desacreditar as informações a seu respeito.
- Tenta convencer que Deus não existe.
- Desvia a adoração a Deus para si.

- Tira a Palavra de Deus do seu contexto.
- Altera o sentido ou significado da Palavra de Deus.
- Acresce, exclui ou altera partes da Palavra de Deus.
- Muda os costumes e o significado/sentido das palavras para confundir.
- Usa a luxúria para afastar as pessoas de Deus (Os 4:12).
- Usa as riquezas para afastar as pessoas de Deus (Mt 13:22).
- Tenta convencer de que a Bíblia foi inventada, manipulada, é ficção, é mentira, é fraude, é incompleta, foi modificada pelos homens, servia apenas para as pessoas daquela época e contexto ou de que somente os teólogos sabem interpretá-la corretamente.
- Tira ou deprecia o valor do que é precioso para Deus.
- Nos faz depender de motivações externas, mas não temos que andar por vistas e nem por circunstâncias (Fl 4:12-13).
- Nos faz buscarmos aceitação e aprovação, mas nossa aprovação vem dos céus (I Ts 2:3-4).
- Nos desperta o interesse pelo retorno financeiro, mas nosso empenho deve ser o Reino de Deus e Sua justiça, as demais coisas, Deus acrescentará (Pv 30:8 e Mt 6:24).
- Nos faz valorizamos o exterior mais do que a presença interior de Deus, o que é o primeiro passo para a luxúria (Ap 18:7-9).
- Faz-nos conformamos com as coisas deste século, com o que perdemos a identidade de Santos (Rm 12:2 e II Co 4:4).
- Nos tira a iniciativa em buscarmos a Deus, que é sinal que o Espírito de Deus está prestes a apagar em nós (I Ts 5:19).
- Rouba a simplicidade dos que são de Cristo (II Cor 11:3).
- Faz pensar que a Palavra de Deus é Mentira. Ele articula as coisas de tal maneira para que a verdade pareça mentira e a mentira pareça verdade, pois é o pai da Filosofia.
- Coloca mais fardos e pesos sobre os ombros das pessoas.
- Provoca o desânimo.
- Faz as ficarem dando voltas e mais voltas sem saírem do lugar.
- Usa das emoções e lágrimas para comover, sensibilizar e enganar.
- Usa da aparência de piedade para conquistar a confiança e credibilidade.
- Modula a voz para impressionar.
- Cria cenários fantásticos (verdadeiros shows hollywoodianos) para impressionar.
- Usa de músicas que parecem coral de anjos para comover.
- Nos incute o medo, o receio, a timidez, a insegurança, a dúvida, a incerteza, a vergonha das coisas de Deus...

Ressalta-se que os demônios podem ser usados por Deus na realização de Seus propósitos (I Sam 16:14 e II Cor 12:7).

Abaixo, algumas das evidências dos falsos cristãos, pastores, profetas, ungidos, etc.:

- Agem conforme sua ganância (Tito 1:11 e Jeremias 6:13);
- Andam segundo suas próprias cobiças e concupiscências (II Timóteo 4:3);
- Aparentam ser bonzinhos (Mateus 7:15);

- Chamam a manifestação do Espírito Santo de obra do Maligno (Mateus 10:25, 12:24, Marcos 3:22 e Lucas 11:15);
- Dão ouvidos à espíritos malignos e pregam doutrinas dos demônios (I Timóteo 4:2);
- De suas pregações não se aprende quase nada (muitas palavras e muito tempo, mas pouco conteúdo);
- Desviam as ovelhas de Deus e de Sua Palavra (Jeremias 50:6, Deuteronômio 13:1-5 e Miquéias 3:5);
- Devoram e/ou tosquiam o rebanho em vez de alimentá-lo (Ezequiel 34:2-3 e Zacarias 11:17);
- Dialogam com outros espíritos;
- Dispersam o rebanho (Jeremias 23:2);
- Dizem que a Bíblia é machista, preconceituosa e discriminatória;
- Dizem que a Bíblia foi escrita por homens;
- Dizem que são/somos filhos do dono/senhor do mundo (Mateus 4:5-7, 16:26, Lucas 16:8, João 8:23, 14:30, 16:11, 17:16, 18:26, I Coríntios 2:8 e I João 5:19);
- Enrolam a língua para simular que estão orando em línguas (Atos 2:4-8 e I Coríntios 12:30, 13:1, 14:8-9,27-28);
- Ensinam doutrinas dos homens (Mateus 15:9, Levítico 20:23 e Isaías 8:20);
- Ensinam e agem de forma diversa dos apóstolos (Gálatas 1:8, I Timóteo 6:3, II Coríntios 11:4 e Isaías 8:20);
- Estão em companhia de doutores, mestres, sábios, eruditos, especialistas, etc. (II Timóteo 4:3 e Jeremias 50:35-36);
- Estipulam metas, datas, prazos, resultados, quantidades, etc.;
- Excomungam as sãs doutrinas e as pessoas que os condenam, denunciam, expõem, etc. (Mateus 5:11-12, 10:22,25, 12:24, Marcos 3:22 e João 16:2-3);
- Extrapolam o sentido da Liberdade que há em Cristo dizendo que é proibido proibir (I Coríntios 6:12);
- Falam de si próprios (Ezequiel 13:3);
- Falam na primeira pessoa (“eu”) (João 5:43);
- Falam para orarmos pelo país, pelas nações e pelo mundo (João 17:9, Tiago 4:4 e I João 5:19);
- Falsos pastores andam juntos com falsos profetas (Jeremias 5:31);
- Fazem comércio das coisas de Deus (Mateus 27:12-13, Isaías 23:18, Ezequiel 27:15 e 28:18);
- Fazem de Jesus um escravo, servo, empregado, etc. (Mateus 6:10, 7:21, 12:50 e 26:42);
- Fazem do púlpito um circo ou palco de teatro;
- Fazem exigências e cobranças a Jesus (Mateus 6:10, 7:21, 12:50 e 26:42);
- Fazem falsos sinais e prodígios (Mateus 24:24);
- Gostam de belos trajes/vestimentas (Ezequiel 28:13, Mateus 11:7-9, II Reis 1:7-8 e Mateus 3:4);
- Gostam de holofotes e plateia (Mateus 6:1,5, 23:5 e Lucas 14:10);
- Gostam de poderes terrenos;
- Gostam de ritualismo e cerimônias (Isaías 1:11-16);
- Insaciáveis e amantes do prazer (Isaías 56:10-12 e II Timóteo 3:4);
- Interpretam um versículo isoladamente fora do contexto dos demais (Mateus 4:3-11, Isaías 28:13, Josué 1:7 e II Reis 17:13);
- Mandam-nos profetizar (repetir uma frase afirmativa de algo que irá supostamente acontecer como tivesse sido Deus quem falou/ordenou) isso e aquilo, mas a

Bíblia diz para não ficarmos brincando de sermos profetas (Deuteronômio 13:1-5 e 18:20-22);

- Não admoestam/reprendem os que estão em erro (Ezequiel 3:17-18);
- Não denunciam o pecado (Jeremias 23:9-18);
- Não possuem a Bíblia como única autoridade inerrante, máxima e suficiente (II Timóteo 3:16-17);
- Negam a autossuficiência do Sacrifício de Jesus – pregam indulgências, simpatias, novenas, flagelos, obras expiatórias, correntes, etc. (Marcos 8:37);
- Negam Jesus (II Pedro 2:1, Tito 1:16, Mateus 10:33, II Timóteo 2:12 e Jeremias 2:8);
- Negam o Senhorio de Jesus (II Pedro 2:1);
- Negam que a Bíblia é a Palavra de Deus;
- Negam que a Bíblia é Perfeita, sem erros e sem falhas;
- O discurso preferido dos impostores é sobre paz, prosperidade e segurança para os que estão em pecado (Jeremias 15:15, 20:1-6, 26:8-11, Amós 5:10, Mateus 23:29-36 e Atos 7:51-53);
- Os seguidores dos falsos normalmente não seguem toda a Palavra de Deus;
- Os seguidores priorizam mais as experiências religiosas e as manifestações sobrenaturais do que o teor da Bíblia;
- Possuem cargos/ministérios hereditários;
- Possuem companheirismo com seus rivais para juntos combaterem a Verdade como os escribas, saduceus, fariseus, herodianos... fizeram com Jesus e os seus discípulos (Marcos 3:6, 11:18, 14:1,55 e Lucas 19:47);
- Possuem dogmas, credos, conceitos, filosofias, doutrinas, práticas... inquestionáveis (todos devem crer sem duvidar, indagar ou criticar, mesmo não tendo expresso e claro suporte bíblico);
- Pregam a guarda do Sábado, do Domingo ou de outro dia “santo” (Mateus 12:8,11-12, Marcos 2:27, Lucas 13:15, João 5:16-17, Colossenses 2:16 e II Timóteo 4:2);
- Pregam a liderança do Espírito Santo (João 16:13, Atos 10:19-20, 13:2, 16:6, Romanos 8:14) mas é notória a liderança e organização humanas (Mateus 15:8-9, Jeremias 17:5, II Timóteo 4:3-4, Colossenses 2:8 e Mateus 21:23);
- Pregam a prosperidade financeira;
- Pregam a união entre todas as denominações/igrejas da Cristandade (e não a harmonia em Cristo e Sua Palavra);
- Pregam contra a piedade (I Timóteo 3:5 e 6:3);
- Pregam contra a santidade ao Senhor, dizendo que Deus não olha nossa aparência ou comportamento, mas que Ele só vê nosso coração;
- Pregam mensagens atraentes e agradáveis segundo o raciocínio carnal/humano – agradam e seduzem os homens;
- Pregam o caminho largo e fácil (Lucas 13:24 e Mateus 7:13);
- Pregam obediência à Lei – negam a Graça (Romanos 3:20, Gálatas 2:16, 5:1,18,22 e Efésios 2:8);
- Pregam o ecumenismo, que todos adoram o mesmo Deus e que todos somos filhos de Deus;
- Pregam que a marca da Besta será um microchip ou um código de barras;
- Pregam que a religião do Anti-Cristo ainda (futuro) vai surgir, sendo que já existe;
- Pregam que Deus é um Deus de Amor e, por isso, não vai mandar ninguém ao Inferno;

- Priorizam a realização das curas e outros milagres (exageram, só ficam nisso, não evolui da fase dos 70 discípulos de Jesus) durante as pregações para impressionar, cativar e seduzir os leigos e incautos;
- Proíbem a leitura, acesso, posse... de passagens bíblicas, liturgias, livros, estudos... que os desmascaram, denunciam, expõem, etc. (I Tessalonicenses 5:21);
- Proíbem determinados alimentos (I Timóteo 4:3, Atos 10:10-15 e 11:5-9 e I Coríntios 10:25-27);
- Resistem à Verdade (II Timóteo 3:8, Gálatas 4:16, João 8:43-44,47 e Jó 5:17);
- Retiram algum atributo, poder, título, autoridade, capacidade, propriedade... de Jesus;
- São amigos do mundo (Tiago 4:4, I João 2:15, Amós 3:3, Êxodo 34:12 e Jeremias 23:28);
- São arrogantes (II Timóteo 3:2);
- São atrevidos (II Timóteo 3:4);
- São aproveitadores (exploram as pessoas);
- São avarentos (II Pedro 2:2, II Timóteo 3:2, I Coríntios 6:10, Efésios 5:5 e Romanos 1:29);
- São barulhentos. Gostam de gritaria, fanfarra e algazarra (I Reis 18:28);
- São corruptos (Miquéias 3:11, Êxodo 23:8);
- São desonestos (I Coríntios 6:10 e Mateus 15:19);
- São egoístas (II Timóteo 3:2);
- São eloquentes pregadores, mas nem eles sabem o que dizem (I Timóteo 1:5-7 e I Coríntios 4:20);
- São em maior número (Êxodo 23:2, Mateus 7:13 e I Reis 18:19-22);
- São estudados na sabedoria humana (João 3:9-10, I Coríntios 1:18,21,27 e 3:19, Mateus 11:25, Lucas 21:14-15 e Colossenses 2:8);
- São exclusivistas – apontam para denominações, grupos, entidades, congregações, etc. (Lucas 9:49-50 e Marcos 9:38-40);
- São exibicionistas - gostam de fazer demonstrações de sinais para impressionar (Mateus 12:38-39 e 16:4, Marcos 8:12 e João 10:40-41);
- São famosos, influentes e respeitados (Lucas 6:26 e 19:47 e Isaías 9:15);
- São hipócritas/falsos - não creem e, muito menos, vivem o que pregam (I Timóteo 4:2, Apocalipse 21:8, Jeremias 6:13, I Pedro 2:1, I Coríntios 5:8 e Mateus 22:18 e 23:27-28);
- São homicidas – assassinos (João 8:44, Atos 7:52, I João 3:15 e Apocalipse 21:8 e 22:15);
- São idolatrados e/ou são idólatras – eles e/ou seus fiéis possuem ídolos (I Coríntios 6:9, Efésios 5:5 e Apocalipse 22:15);
- São imediatistas (Mateus 6:25-26);
- São invejosos/ciumentos (Gálatas 5:21,26, I Coríntios 3:3, I Pedro 2:1, Tito 3:3, Romanos 1:29 e Marcos 15:10);
- São irreverentes (II Timóteo 3:2);
- São libertinos/promíscuos (II Pedro 2:2, Gálatas 5:16,19, II Coríntios 12:21, Apocalipse 21:8, Mateus 15:19 e Tito 3:3);
- São materialistas (Mateus 6:19-21,24, 13:2 e 16:26, Marcos 10:23-24, Hebreus 11:26, Colossenses 3:1 e Apocalipse 3:17);
- São mentirosos (Apocalipse 21:8 e 22:15, Jeremias 14:14, Ezequiel 22:28, Zacarias 13:3 e João 8:43-44);
- São mercenários e abandonam as ovelhas (João 10:12);

- São os principais pregadores (Mateus 20:18, 27:12,20, Marcos 11:18, Lucas 19:47, 23:10 e João 12:10);
- São ou defendem quem são efeminados ou sodomitas (I Coríntios 6:9);
- São perversos (II Tessalonicenses 3:2 e II Timóteo 2:18);
- São preguiçosos (Isaías 56:10 e Malaquias 1:13);
- São usurpadores;
- São vaidosos, orgulhosos, soberbos, etc. (II Coríntios 11:12-13, Deuteronômio 18:22 e Tiago 4:6);
- São violentos/agressivos;
- Se apegam à Teologia (Mateus 15:9, 16:11-12,23, João 3:10, 7:38, I Coríntios 2:4-5 e Provérbios 3:5) ao invés da Bíblia e da Revelação Divina (Isaías 48:17 e João 6:45, 14:26 e 7:15);
- Se entregam às fábulas, mitos, estórias, lendas, folclore, tradições, etc. (II Timóteo 4:4, Apocalipse 21:8, Levítico 20:23, Mateus 15:2-3, II Pedro 1:16 e Colossenses 2:8);
- Se entregam aos desejos da carne e de suas concupiscências (Efésios 2:3, I Pedro 4:2, Romanos 7:5 e 8:1 e Gênesis 39:7-20);
- Se ocupam mais com seus próprios desejos do que com a glória e honra de Deus (Lucas 22:42);
- Seus seguidores possuem mais lealdade à pessoa do líder do que à Bíblia (João 5:43);
- Simulam/fingem a prática da caridade para atrair os leigos e incautos para o seu meio (Mateus 6:1-4);
- Suas obras os denunciam (Tito 1:16 e Mateus 7:16);
- Tem aparência de piedade, mas negam a eficácia dela (II Timóteo 3:5, Mateus 7:15 e 23:28);
- Violam a Palavra de Deus e ensinam os outros a violarem (Mateus 5:19, I Timóteo 6:3 e Ezequiel 22:26);
- Vivem de excessos/extravagâncias (Oséias 5:1-2, Gálatas 5:21, Romanos 14:17 e Isaías 56:11-12).

A marca da besta é a cauterização, impregnação, induzimento, hipnose... da mente das pessoas com as doutrinas demoníacas que servem de base para o Ecumenismo (igreja mundial do Anti-Cristo). Desse modo, os falsos ministros ecumenistas conduzem as pessoas ao Inferno com suas pregações (Mateus 23:15), por isso as Escrituras nos ordenam: “Sai dela [Babilônia e suas filhas protestantes], povo meu, para que não sejas participante dos seus pecados, e para que não incorras nas suas pragas.” (Apocalipse 18:4). Essa advertência (Jeremias 51:6,45) não é só sobre a grande meretriz escarlate (Apocalipse 17:1-2), mas também sobre suas filhas evangélicas (Isaías 47:1-3 e Zacarias 2:7), pois a meretriz é a “mãe das abominações” (Apocalipse 17:5) e, se é mãe, é porque teve filhas e “tal mãe, tal filha” (Ezequiel 16:44; Isaías 47:1-3; Zacarias 2:7; Ezequiel 23 e 16:53,55), vez que possuem o mesmo “DNA” espiritual (marca espiritual mental), que é a crença na trindade e a realização do batismo trinitário, o qual é diverso do

batismo pregado e realizado pelos apóstolos (Atos 19:1-6, 2:38, 8:12, 10:43,48, 22:16 com Romanos 6;3-4, I Coríntios 6:11 e Gálatas 3:27).

O profeta Amós perguntou: **"Andarão dois juntos, se não estiverem de acordo?" (Amós 3:3).** Refiro-me a tentativa ecumênica de unir evangélicos e católicos numa só igreja. A proposta ecumênica dos católicos é de mão única. Estes estão interessados que os evangélicos, por exemplo, aceitem o Papa como cabeça da igreja e muito mais. A meta do ecumenismo é a união de todas as igrejas em uma só Igreja Mundial. É impossível aceitar essa proposta sem abrir mão daquilo que é básico em nossa fé. Sabemos, pelas Escrituras, que o Anticristo virá sobre as asas do ecumenismo se colocando como líder religioso mundial que trará a falsa paz mundial.

"**Não vos prendais a um jugo desigual com os infiéis.** Pois que sociedade tem a justiça com injustiça? E que comunhão tem a luz com as trevas? E **que concórdia há entre Cristo e Belial?** Ou que parte o fiel com o infiel? E que consenso tem o templo de Deus com os ídolos? Pois vós sois santuário do Deus vivente, como Deus disse: Neles habitarei, e entre eles andarei, e eu serei o seu Deus e eles serão o meu povo. Pelo que saí do meio deles, apartai-vos, diz o Senhor. Não toqueis nada impuro, e eu vos receberei. Eu serei para vós Pai, e vós sereis para mim filhos e filhas, diz o Senhor Todo-poderoso". (I Coríntios 6:14-17).

DÚVIDAS, INFORMAÇÕES E ATUALIZAÇÕES

Infra alguns sites onde se pode conseguir maiores informações e atualizações:

- http://www.bitcoin.org/;
- https://bitcoin.org/pt_BR/;
- https://bitcoin.org/pt_BR/imprensa;
- http://institutobitcoin.org/;
- http://bitpedia.com.br/;
- http://www.bitcoin.com.br;
- http://www.bitkoins.com.br/;
- http://bitcoinnews.com.br/;
- https://www.mercadobitcoin.com.br/;
- http://www.facebook.com/mbitcoin;
- https://twitter.com/mercadobitcoin;
- http://pt.wikihow.com/Minerar-Bitcoins;
- http://www.bitcoinbrasil.com.br;
- https://www.bitcoinbrasil.com.br/comunidade;
- http://bitcoin-brasil.com/comunidade/;
- https://bitcoinforum.com/portuguese/;
- https://bitcoin.org/pt_BR/comunidade;
- https://bitcointalk.org/;
- https://bitco.in/forum/;
- https://forum.bitcoin.com/;
- http://bitcoinfoundation.org/forum/;
- https://en.bitcoin.it/wiki/Forums;

- https://www.reddit.com/r/bitcoin;
- http://www.reddit.com/r/oBitcoin;
- http://www.reddit.com/r/BrasilBitcoin;
- https://en.bitcoin.it/wiki/Main_Page;
- https://www.ybitcoin.com/;
- https://bitcoinmagazine.com/;
- http://pt.slideshare.net/frpaiva1/manual-bitcoinfernando;
- http://www.mises.org.br/files/literature/MisesBrasil_BITCOIN_BROCHURA.pdf.

GLOSSÁRIO

Utilize os seguintes links para facilitar a navegação: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

.onion. Veja Onion.

420, 4:20 ou 4/20. É um código usado, principalmente nos Estados Unidos, para se referir à *cannabis* (maconha). A data de 20 de abril é o "Weed Day" (Dia da Erva), "Pot Day" (Dia da Maconha) ou dia internacional de protestos pela liberação da maconha. Existem várias teorias para explicar a origem desse código.

4/20. Na *deep web* também significa venda especial e limitada.

51% attack. Ver Ataque de 51%.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

Adware. É um tipo de *software* (programa de computador), gratuito como o *freeware*; porém, para trazer rendimentos ao seu criador, geralmente possuem *banners* (propagandas) em suas janelas. A maioria possui a versão paga que é sem anúncios. Alguns programas *adware*, violam a privacidade e coletam dados do computador do usuário. Programas como Ad-Aware verificam a existência de adwares no computador.

AdWords (palavras de anúncio). É o principal serviço de publicidade (propaganda) do Google (https://www.google.com.br/adwords/) e que utiliza o sistema de *Cost Per Click Advertising* (Publicidade por Custo por Clique). Os anúncios do AdWords são exibidos juntamente com os resultados de pesquisa no Google. Veja Busca orgânica, Pay-per-click (PPP) e Link patrocinado.

Altcoin. Nome dado às moedas criptográficas alternativas à bitcoin. Exemplos: Litecoin, Dogecoin, Dash, etc. Saiba mais em Altcoins e Criptomoeda. Confira o capítulo "INTRODUÇÃO ÀS ALTCOINS".

Altura do bloco. Ver Bloco altura.

Alvo (*target*). Um número de 256 bits que coloca um limite para o *hash*. Os blocos válidos devem ter o *hash* inferior a este limite. Quanto mais baixo for o alvo (limite), maior será a dificuldade (*difficulty*) de encontrar um *hash* válido. O máximo (mais fácil) de destino é 0x00000000FFFF0000000000000000000000000000000000000000000000000000. No Bitcoin, a dificuldade e o alvo são ajustados a cada 2016 blocos para manter o intervalo entre os blocos perto de 10 (dez) minutos. Veja, ainda, Bloco e Dificuldade (*difficulty*) no texto principal e Dificuldade e *Nonce* no glossário.

AML. Sigla de *Anti-Money Laundering* (antilavagem de dinheiro), são técnicas usadas para barrar a lavagem de dinheiro (processo onde rendimentos ilícitos passam a aparentar origem lícita). Infra uma lista exemplificativa de circunstâncias suspeitas, que dependerá do fundo, detalhes das transações e outros fatos e circunstâncias: 1) clientes cuja verificação de identidade parece difícil ou clientes que parecem não quererem cooperar; 2) aumento substancial na atividade sem qualquer causa aparente; 3) grande número de contas que têm parâmetros comuns: sócios, diretores, promotores, endereço, e-mail, números de telefone, apresentadores ou signatários autorizados; 4) transações sem justificação econômica ou comercial aparente; 5) atividade súbita em contas inativas; 6) origem dos fundos são duvidosos ou há inconsistência no padrão de pagamento; 7) depósitos à vista incomuns e grandes feitos por um indivíduo ou empresa; 8) transferência de investimento contínua a terceiros, aparentemente não relacionados; 9) várias transações de valor um pouco abaixo daquele que existe obrigação de apresentação de relatórios; 10) operações incomuns por empresas de fachada, bancos *offshores*, serviços financeiros e empresas que se declaram do ramo de importação e exportação de itens de pequeno porte; 11) serviços de gestão de ativos para clientes onde a origem dos fundos não é clara ou não coincide com a aparente atividade ou negócios dos clientes; 12) clientes em jurisdições de alto risco, introduzidos por bancos ou afiliados ou baseados em jurisdições de alto risco; clientes que transferem grandes somas de dinheiro para ou a partir de locais no exterior com instruções para pagamento em dinheiro; 13) compras

feitas por conta própria transferido para um terceiro por meio de operações de mercado off; etc. Saiba mais nos capítulos "ABRIR UMA CONTA BANCÁRIA NO EXTERIOR (*OFFSHORE*)" e "DO ASPECTO CRIMINAL NO BRASIL".

Analógico (*analog*). O que não é digital. A palavra grega *analogos* significa comparação. O computador analógico utiliza propriedades físicas (fenômenos elétricos, ópticos, mecânicos ou hidráulicos), são normalmente criados para uma finalidade específica (normalmente calcular alguma coisa) e trabalham com sinais elétricos de infinitos valores de tensão e corrente. O computador digital, por sua vez, é multifuncional, trabalha com apenas dois níveis de sinais elétricos (alto e baixo) e armazena e processa dados exclusivamente sob a forma de números zeros e uns (usa a eletricidade para criar o código binário). As grandezas analógicas variam de forma contínua ao passo que as digitais variam de forma discreta. A tecnologia analógica é o processo de receber um sinal de áudio ou vídeo e traduzi-lo em pulsos eletrônicos. Já a tecnologia digital, por outro lado, converte esse mesmo sinal em um formato binário, no qual os dados de áudio e de vídeo são convertidos em uma série de números zeros e uns. O sinal (frequência) analógico é contínuo, varia em função do tempo e é representado por uma curva, tal como o rastro de uma cobra. Já o sinal digital possui valores discretos (descontínuos) no tempo e em amplitude, sendo representado por um histograma. Veja Digital.

Anexar (*attach*). Juntar. Agregar. Colocar junto de. Unir uma coisa à outra, estabelecendo uma relação de dependência. Ver *Attach*.

Antimalware. Ferramenta (software ou aplicativo) que procura detectar e anular (inutilizar) ou remover (apagar ou desinstalar) os códigos (algoritmos) maliciosos (nocivos ou prejudiciais) de um computador. Os programas antivírus, antispyware, *antirootkit* e antitrojan são exemplos de ferramentas antimalware. Confira *Malware*.

Antivírus. Programa de computador (software ou aplicativo) utilizado para descontaminar um computador ou rede (intranet) que estiver infectada com vírus, worm e códigos maliciosos; bem como fornecer proteção contra

novas contaminações e infestações. Esses programas precisam ser atualizados periodicamente para garantir sua eficácia.

API - *Application Programming Interface* (interface de programação de aplicativos). Conjunto de instruções, rotinas e padrões de programação que permite a construção ou o acesso de aplicativos e a sua utilização de maneira não evidente ao usuário. Trata-se de uma interface que funciona em segundo plano ("por trás de tudo"). Através das APIs os aplicativos conversam uns com os outros sem conhecimento ou intervenção dos usuários; por exemplo, numa loja *on line*, a API da loja se comunica com a da instituição financeira para verificar os dados do cartão de crédito. Ainda mais do que isso, é também como um convênio, parceria ou compartilhamento de recursos entre diferentes softwares, sistemas, plataformas ou sites; ou seja, uma integração ou trabalho em conjunto. Ou, ainda, é como uma terceirização de serviços (trabalho externo). Assim, por exemplos, o Windows permite que os softwares utilizem do relógio do sistema e o Google Maps permite que outros sites utilizem seu sistema de mapas dentro de suas páginas. Em síntese, a principal função de uma API é permitir que outros softwares ou sistemas se associem ou interajam com o respectivo serviço, recurso ou funcionalidade. Por outras palavras, a API determina como um programador pode realizar uma tarefa específica através de uma biblioteca. Em alguns casos uma API pode documentar alguns detalhes de como deve ser a implementação para garantir que alguns objetivos sejam alcançados. É como sexo sem compromisso; vez que os usuários não pretendem envolver-se em detalhes da implementação do software, mas apenas usar seus serviços. Pode-se comparar a API como um garçom que intermedia a ligação entre o cliente e a cozinha do restaurante, onde o cardápio seria a documentação da API. Mas se assemelha mais a um diplomata, que além de simplesmente traduzir e repassar pedidos, ainda informa as regras, formalidades e costumes e, inclusive, um diplomata negocia com outro diplomata. Em resumo, a API é a maneira como um código se relaciona com uma biblioteca e este procedimento consta de sua documentação (conjunto de regras para realizar uma tarefa). Apesar do SDK - *Software Development Kit* (kit de desenvolvimento de software) ser um conjunto de ferramentas de desenvolvimento e códigos pré-gravados que podem ser usados pelos desenvolvedores para criar aplicativos, não se confunde com a API. Um SDK fornece um conjunto de ferramentas, classes

auxiliares (como um código adicional que simplifica o acesso de uma API), de ligações linguísticas específicas e código exemplificativo para ajudar os desenvolvedores a utilizar a API. Em geral, pode-se ter uma única API expondo um conjunto de funcionalidades e ter vários SDKs para acessar a API. SDK pode incluir hardware especial de desenvolvimento e ferramentas empacotadas (embutidas) como compiladores, ferramentas de criação de mídia como codecs, software de modelagem 3D, depuradores, etc. Ainda mais, o SDK é a linguagem de programação do sistema operacional Android. As APIs mais utilizadas são: a) DLL – *Dynamic-link library*: executáveis compiladas em ambientes como .Net e Delphi; b) *Plugins*: exemplos são os usos de captcha, envio de e-mail e *feed*, anti-spam, otimizador de SEO, analisador de estatísticas, etc.; c) Frameworks compartilhados: exemplos JQuery e Bootstrap; e, d) WebAPI (ou Internet API): São APIs utilizadas em soluções web, podendo ser *client-side* (dado do cliente) ou *server-side* (lado do servidor); ou seja, executadas no *front* (frente) ou no *back-end* (no final ou por trás) de uma aplicação web.

Árvore de Merkle (*Merkle tree*), árvore de dispersão ou árvore de *hash*. Trata-se de uma estrutura de dados que contém uma árvore de informações resumidas sobre um pedaço maior de dados e que organiza uma lista de itens de dados em uma árvore de seus *hashes* (como no Git, Mercurial ou ZFS). As árvores de Merkle são árvores binárias dos *hashes*. Em dita árvore binária, as folhas (dados pareados ou transações de um único bloco) são separações de blocos de dados em um arquivo ou conjunto de arquivos. Os nós localizados mais acima na árvore são as dispersões de seus respectivos filhos. No sistema Bitcoin a árvore Merkle é usada para organizar as transações dentro de um bloco (cabeçalho do bloco contém apenas um *hash* de uma árvore). Saiba mais em Árvore de Merkle no teor do e-book.

ASCII. Tabela de símbolos, usada para gerar e armazenar os símbolos que não podem ser inseridos via teclado. Saiba mais em ASCII.

ASIC. Sigla de *Application Specific Integrated Circuit* (Circuito Integrado de Aplicação Especifica), é um chip criado especificamente para realizar uma tarefa. No caso do Bitcoin, os ASICs foram criados para

processar o *hash* SHA-256 e, assim, minerar bitcoins. Saiba mais em ASIC definição, hardware e Mineração.

ASICMiner. Um fabricante chinês de hardware de mineração de criptomoedas. Saiba mais no capítulo "EQUIPAMENTOS DE MINERAÇÃO".

Assemble to order. Significa que só é fabricado por encomenda.

Assinatura (*signature*). A criptografia de assinatura é um mecanismo matemático que permite a alguém provar a propriedade ou titularidade. Quando o software Bitcoin assina uma transação com a chave privada (*private key*), toda a rede pode ver que a assinatura coincide com as bitcoins que foram gastas. Confira o capítulo "CERTIFICADOS DIGITAIS". Veja, ainda, os verbetes: Chave criptográfica (*cryptographic key*), Autoridade certificadora e Certificado digital.

Atalho (*shortcut*). Um ícone que pode ser colocado na tela inicial do computador para facilitar o acesso a um programa ou arquivo. Assim, em vez de procurar diretamente o programa ou arquivo em diretórios e pastas, basta clicar duas vezes no seu ícone para abri-lo. Os atalhos não precisam ter o mesmo nome do arquivo, pode-se dar a ele qualquer apelido e associá-lo ao arquivo em questão. Em inglês, *shortcut* (cortar caminho). Ver Ícone e Link.

Ataque (*attack*). Em informática consiste nas ações praticadas por softwares (autônomo previamente programado ou remotamente controlado por um *hacker*) com a intenção primária de acessar ou conectar-se a um sistema, rede ou computador sem autorização (leia-se invadir) visando intenções ilícitas, maldosas ou danosas. As consequências do ataque são variadas. Pode ser para infectar com algum malware ou para componentes de hardware, de software e/ou de dados. Também pode ser uma ação preparatória para outra maior; ou seja, alterar a configuração ou o funcionamento da vítima ou alvo (sistema, rede ou computador), deixando-a vulnerável, para possibilitar outros tipos de ataques e ações futuras. Muitas vezes as invasões visam acessar dados pessoais, sigilosas, íntimas e bancárias dos usuários. Por fim a invasão pode ser do tipo *snooping*

(bisbilhotando); ou seja, sem fins lucrativos, apenas para bisbilhotar as informações alheias.

Ataque de 51% (*51% attack*). Também conhecido como ataque de >50% ou *Double Spent Attack* (ataque do gasto em dobro). Um atacante pode fazer um pagamento, esperar até que o comerciante aceita um certo número de confirmações e fornece o produto ou serviço e, em seguida, começa a minerar uma cadeia paralela de blocos de partida com um bloco antes da operação. Esta *blockchain* (cadeia de blocos) paralela, em seguida, inclui uma outra operação que gasta as mesmas saídas (unidades da criptomoeda) em algum outro endereço (pagamento ou credor). Quando a cadeia paralela se torna mais difícil, ela é considerada uma cadeia principal por todos os nós e a transação original torna-se inválida. Desse modo, é cancelado o primeiro pagamento com as mesmas unidades da criptomoeda. Tendo mais da metade do total de *hashrate* da rede, é possível ultrapassar qualquer cadeia; daí o nome mais preciso desse ataque como sendo "mais de 50%" (e não 51%). Entretanto, até mesmo 40% de *hashrate* permite fazer um gasto duplo, mas a possibilidade de êxito é menor do que 100% e diminuem exponencialmente conforme o número de confirmações de que a contraparte requer. Este ataque é considerado teórico em razão de que o custo para possuir mais de 50% de *hashrate* não compensa o gasto duplo. Outra variante desse ataque é afetar a rede pela mineração de blocos vazios, censurando todas as transações. Um ataque pode ser mitigado pela lista negra (*blacklist*) de blocos que a maioria dos mineiros honestos considerem anormal; também pode ser atenuado pelo uso de checkpoints que impedem a reorganização após determinado bloco. Em condições normais, os mineiros e piscinas de mineração não censuraram blocos. Confira o capítulo "QUEM CONTROLA OU ESTÁ POR TRÁS DO BITCOIN?" e o verbete *Double Spend* (gasto duplo). Veja Mineração.

ATM. Sigla de *Automated Teller Machine* (caixa eletrônico). No caso da bitcoin, as vezes são chamados de BTM - *Bitcoin Automatic Teller Machine* (máquina de caixa automática Bitcoin) e permite que os usuários façam compra e venda de bitcoins, usando dinheiro físico ou cartões bancários. A CoinDesk possui um mapa com ATMs espalhados pelo mundo e a lista de fabricantes (http://www.coindesk.com/bitcoin-atm-map/).

***Attach* (anexar)**. Muitas pessoas, indevidamente, usam a expressão "atachar" no lugar de "anexar" para se referir a um documento que está sendo anexado a outro. Apesar de que no inglês existe a palavra *annex* (anexo), que como a nossa "anexar", deriva do latim *annexus*, que significa "colocar junto". Mas o pessoal da informática resolveu emprestar *attach* (anexar) do francês *attacher* (laço).

Attachment ("arquivo atachado"). Envio de um arquivo associado a uma mensagem. Os serviços de correio eletrônico (e-mail) costumam permitir que qualquer arquivo seja enviado junto com uma mensagem; a qual, ao chegar no destinatário, permite abrir e salvar no computador o arquivo anexo.

Auto Id. Abreviatura de "Automatic Identification"; ou seja, identificação automática.

Autoridade certificadora. Entidade responsável por emitir e gerenciar certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: computador, pessoas física e jurídica (empresa, departamento de uma instituição, instituição, etc.). Veja Assinatura e Certificado digital.

A, **B**, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

B2B (*Business to Business*). Significa comércio eletrônico entre empresas ou simplesmente atacado on-line.

B2C (*Business to Consumer*). Significa comércio eletrônico para o consumidor final.

Backbone (o osso de trás). São os fios e os cabos que conduzem os dados dentro de um comutador e para seus periféricos. É a espinha dorsal de um sistema. Veja *Hardware*.

Backdoor. Tipo de código malicioso. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de

serviços criados ou modificados para esse fim. Normalmente esse programa é colocado de forma a não a ser notado. Veja, ainda, *Backdoor*. Veja *Cracker* e *Malware*.

***Blacklist* (lista negra)**. Lista de e-mails, domínios e/ou endereços IP, reconhecidamente fontes de *spam*, malware e/ou *scams*. Recurso utilizado, tanto em servidores como em programas leitores de e-mails para bloquear as mensagens suspeitas de serem *spam*.

Back Office. Módulo gerencial que permite a completa administração da Loja Virtual, do cadastro do cliente, ao *workflow* (fluxo de trabalho) de vendas e controle de estoque. Normalmente, é utilizado um sistema ERP - *Enterprise Resource Planning* (Planejamento de Recursos Empresariais), melhor detalhado à frente.

***Backup* (cópia de segurança)**. O idioma inglês possui muitas palavras que são a junção de outras resultando numa terceira com um sentido totalmente diferente. Isoladamente, as palavras *back*, significa "para trás" e *up*, "para cima"; mas juntas, formam uma nova palavra, com vários significados: engatar a ré, apoiar, recuar, ajudar e até cantar (*backup* vocal, aquele corinho de fundo). Mas, em informática, *backup* significa salvar uma cópia do trabalho.

***Banner* (bandeira)**. Trata-se de pequena publicidade disponível num site contendo um link para a página do anunciante. Por outras palavras, é similar a um anúncio numa publicação impressa (jornal, revista, etc.) com a grande diferença de remeter (direcionar) o curioso (interessado ou potencial cliente) diretamente para o site do anunciante. Em síntese, é simplesmente um tipo especial de link. O nome *banner* advém da propaganda tradicional em forma de bandeira, geralmente pendurada em postes, fachadas ou paredes, exposta na via pública, em pavilhões de exposições, pontos de venda, etc. Veja *Pop-up*.

Barramento (*bus*). Conjunto de linhas (trilhas, fios, caminhos, condutores, percurso, trajeto, etc.) de comunicação (condutor elétrico ou fibra óptica) que permite a interligação entre dispositivos de um sistema de computação (CPU, memória, disco rígido, etc.) ou entre vários sistemas de

computação. Por outras palavras, são os caminhos por onde a informação (dados) e comandos (instruções) circulam e, assim, são utilizados para interligar os diferentes componentes da placa-mãe, permitir o uso de placas de expansão e é o meio por onde transitam as instruções e dados, interna (dentro) e externamente (fora), do processador. Desse modo, por exemplos, o barramento é responsável pela comunicação das diversas interfaces e periféricos ligados à placa-mãe; bem como é o meio utilizado pelo processador para o envio e recebimento de sinais para outros componentes do sistema computacional. Popularmente se confunde barramento com os conectores (local de encaixe dos periféricos). Poder-se-ia fazer uma analogia com as veias e artérias do sistema circulatório sanguíneo dos seres humanos, onde o corpo seria o equivalente da placa-mãe e o coração representaria o processador. Mas a melhor representação seria com o sistema nervoso do corpo humano; ou seja, por onde transitam os dados (informações dos sensores e membros) até o cérebro e as respectivas instruções (ordens ou comandos) aos mesmos pelo cérebro.

Base58. A codificação legível compacta para dados binários, inventada por Satoshi Nakamoto, para tornar os endereços mais *user-friendly* (amigo do usuário), consiste em caracteres alfanuméricos, mas não permite caracteres que possuem a mesma aparência em algumas fontes e podem ser usados para criar endereços de procura visualmente idênticos; tais como, por exemplos, "0", "O", "I", "L". Porém, "o" e "1" são permitidos. Veja Chave pública (*public key*).

Base58Check. Uma variante de codificação Base58 que acrescenta primeiros 4 bytes de Hash256 dos dados codificados antes da conversão de Base58. É usado em endereços para detectar erros de digitação.

Bearish. Tendência em um mercado quando, pela predominância da demanda, o preço dos papéis, moedas ou ativos sofre baixa. O termo em inglês vem de "bear" (urso). Um urso ataca, joga no chão, sufoca e estraçalha suas vítimas (presas) com suas patas na direção do solo; ou seja, com movimentos de cima para baixo; daí a origem do termo que faz uma analogia com um gráfico no qual o preço das ações é cadente. Veja *Bear market* e *Bullish*.

Bear market. Significa que o mercado está em baixa; ou seja, que as ações estão em queda. Dessa expressão adveio o termo "bearish" para designar os pessimistas como mercado de ações (bolsa de valores).

Biblioteca (lib – *library*). É um repositório (conjunto ou acervo) de funções pré-escritas por outros programadores para serem reaproveitadas ou recicladas por outros programadores ou desenvolvedores em seus respectivos softwares. São como componentes pré-moldados ou pré-prontos para serem usados em outros projetos; exemplo, arquivo DLL. Uma biblioteca também é um arquivo executável com um conjunto de funções para executar diversas tarefas. Arquivos ".dll" ou ".so" são arquivos de biblioteca para ligação dinâmica na aplicação. Já arquivos ".lib" ou ".a" são arquivos de biblioteca para ligação estática na aplicação. Uma biblioteca também pode ser de strings, expressões regulares, coleções de dados, manipulação de arquivos, acesso a um banco de dados, manipulação de imagens, etc. Exemplos de bibliotecas: OpenGL, OpenCV e OpenAL. Se uma biblioteca é ou se torna muito complexa ela vira uma *framework*.

Bifurcação. Veja *Fork*.

***Big data* (megadados)**. Refere-se a conjuntos de dados muito grandes ou complexos, que os aplicativos de processamento de dados tradicionais ainda não conseguem lidar.

Binary code. Ver Código binário.

BIOS (*Basic Input Output System*). Trata-se do Sistema Básico de Entrada e Saída existente nos dispositivos computacionais, com a função de configuração e armazenamento das características de hardwares necessárias para inicializar e executar o sistema operacional. Pode-se fazer uma analogia com o motor de arranque ou de partida dos automóveis. Veja Boot.

BIP - *Bitcoin Improvement Proposals* (Propostas de Melhoria Bitcoin). Tal como o nome indica, trata-se de sugestões de introdução de recursos, correções de erros ou informações na rede Bitcoin. A BIP1 descreve o que é a BIP (https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki).

Confira uma lista de BIP em https://github.com/bitcoin/bips e https://wiki.bitcoin.com/w/Bitcoin_Improvement_Proposals. Veja: RFC.

Bit. Forma reduzida de *binary digit* (dígito binário), é a menor unidade de informação tratada pelo computador; em grupos de oito, formam os *bytes* (*Binary Term*), que são a forma mais conhecida de representação de todos os tipos de informação no computador.

bitcoin. Iniciando com letra minúscula, representa a unidade monetária (moeda) do protocolo Bitcoin. Saiba mais no capítulo "BITCOIN". Veja Satoshi e XBT.

Bitcoin. Iniciando com letra maiúscula, representa o protocolo (rede) criado por Satoshi Nakamoto. Saiba mais no capítulo "BITCOIN".

Bitcoin Address (Endereço Bitcoin). Um endereço Bitcoin é semelhante a um endereço físico ou de e-mail. É a única informação necessária que um credor (recebedor) precisa fornecer ao pagador para poder receber um pagamento em Bitcoin ou altcoin. Tipicamente os endereços Bitcoin possuem 34 caracteres entre letras e números. Veja Chave pública. Saiba mais no capítulo "COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?".

Bitcoind. Implementação original do Bitcoin com uma interface de linha de comando, que se tornou uma parte do projeto BitcoinQT (atualmente Bitcoin Core). Ver, também, BitcoinQT no glossário e Bitcoin Core no teor do e-book.

Bitcoinfog. Serviço de lavagem (*wash*) de rastros da bitcoin para dificultar seu rastreamento. Desse modo, este site apaga todos os vestígios das unidades da moeda. Os fundos transferidos para a névoa (nevoeiro) se misturam com os fundos de outros usuários e, quando solicitado, os fundos são pagos em várias transações randomizadas para anonimizar ainda mais a fonte do dinheiro. O site http: //fogcore5n3ov3tui.onion é acessível pelo Tor, navegador da *Deep Web*. Porém existem acusações de que seria um site fraudulento (*scam*). Saiba mais em https://bitcointalk.org/index.php?topic=50037.0. Veja Tumbler.

Bitcoinj. A biblioteca (lib – *library*) bitcoinj é uma implementação Java do protocolo Bitcoin, que permite manter uma carteira (enviar e receber transações) sem a necessidade de uma cópia local do Bitcoin Core. O Bitcoinj (https://github.com/bitcoinj/bitcoinj e https://bitcoinj.github.io/) inclui os serviços SPV - *Simple Payment Verification* (simples verificação de pagamento) e de operações de curva elíptica. Bitcore (https://bitcore.io/) é outra biblioteca em JavaScript (JS).

Bitcoin-ruby. Uma biblioteca de utilitários Bitcoin em Ruby utilizada na produção em Coinbase.com.

Bitcoin Core. Novo nome de BitcoinQT desde o lançamento da versão 0.9 em 19 de março de 2014. Não confundir com CoreBitcoin, uma implementação Objective-C publicada em agosto de 2013. Veja também Bitcore, uma implementação JavaScript para Node.js por Bitpay. Ver, também, BitcoinQT no glossário e Bitcoin Core no teor do e-book.

BitcoinQT. Implementação Bitcoin com base no código original por Satoshi Nakamoto. Inclui uma interface gráfica para Windows, OS X e Linux (usando QT) e uma linha de comando executável bitcoind que é normalmente usado em servidores. É considerada uma implementação de referência, uma vez que é o mais utilizado nó completo de implementação, especialmente entre os mineiros. Outras implementações devem ser compatíveis com ele para evitar ser bifurcada. BitcoinQT usa OpenSSL para as suas operações ECDSA - *Elliptic Curve Digital Signature Algorithm* (Algoritmo de Assinatura Digital de Curvas Elípticas) que tem suas próprias peculiaridades, que se tornaram uma parte do padrão (por exemplo, chaves públicas não-canonicamente codificadas são aceitas pelo OpenSSL sem um erro, para que outras implementações devem fazer o mesmo). Veja verbete acima e Bitcoin Core no teor do e-book.

Bitcoin-ruby. Uma biblioteca de linguagem ruby para interagir com o protocolo Bitcoin (https://github.com/lian/bitcoin-ruby).

Bitcore. Um kit de ferramentas Bitcoin por Bitpay escrito em JavaScript (https://bitcore.io/bitcoin). É mais completa do que Bitcoinj.

***Backdoor* (porta dos fundos)**. São falhas de segurança no sistema operacional ou em aplicativos, que permitem que usuários acessem as informações dos computadores sem que sejam detectados por firewalls ou antivírus.

***Black market* (mercado negro)**. Aquele que atua à margem da lei e das vistas do Estado. É a parte da economia ativa (compra e venda de mercadorias e/ou serviços) que envolve transações ilegais (criminosas); tais como, por exemplos, vendas de drogas ilícitas, de armas de uso restrito ou proibido, de órgãos humanos, etc. Também configura o comércio de bens ou produtos muito escassos ou muito procurados a preços exorbitantes. Ainda se incluem nele as atividades clandestinas, irregulares ou informais; ou seja, onde não há autorização governamental (exemplos, alvará ou licença de funcionamento, habilitação legal para o exercício da atividade, etc.), não estão preenchidas as formalidades legais (exemplos: vistorias, laudos, equipamentos obrigatórios, etc.) e/ou não se recolhem tributos (taxas, impostos, etc.). O câmbio paralelo (o realizado fora dos meios oficiais) é uma prática do mercado negro. Desse modo, as mercadorias (bens ou serviços) podem ser por si próprias ilegais, ser fruto de crime (roubo, furto, sequestro, etc.) ou ser comercializada de modo a fraudar ou evitar tributos, pagamentos ou exigências estatais. Portanto, é chamado de "economia negra" por ser realizado fora da lei ou à margem da lei e, assim, são conduzidas as atividades na obscuridade (fora da vista da lei ou do Estado). Veja Grams, Tor e *Deep Web*.

Black Market Reloaded (Mercado Negro Recarregado). Também conhecido como BMR, o mais antigo mercado negro desde que Silk Road foi fechado.

***Block* (Bloco)**. Uma estrutura de dados que consiste em um cabeçalho de bloco e uma árvore de Merkle de transações. Cada bloco (exceto o bloco gênesis) faz referência a um bloco anterior, formando assim uma árvore chamada *blockchain*. Bloco pode ser pensada como um grupo de transações com um *timestamp* (carimbo de data e hora) e um trabalho de prova anexado. Um bloco inclui todas as informações de transação (comprador, vendedor, valor, etc.) para todas as transações Bitcoin ao longo de um

determinado período de tempo (cerca de 10 minutos). A *Blockchain* é uma combinação de todos os blocos criados. Veja Cadeia principal.

***Blockchain* (cadeia de blocos)**. A *Blockchain* é um registro público das transações Bitcoin em ordem cronológica. A *Blockchain* é compartilhada entre todos os usuários da rede (ou protocolo) Bitcoin. Ela é utilizada para verificar a permanência de transações Bitcoin afim de evitar gastos duplos. A *Blockchain* é como um livro de contabilidade que armazena as informações de cada transação Bitcoin. Ela inclui informações sobre o comprador e o vendedor e o valor transferido em cada transação. Como um livro razão de contabilidade, a informação deve ser dividida em páginas, onde um certo número de operações deve caber em uma página. Isto é muito semelhante ao Bitcoin, onde a contabilidade é dividida em vários blocos diferentes. Não confundir com o site Blockchain.info ou outro site *Block Explorer*. Saiba mais no capítulo "*BLOCKCHAIN*". Veja, ainda, os verbetes *Block* (Bloco) e Cadeia principal.

Blockchain.info (https://blockchain.info/). Empresa que oferece serviço de carteira e explorador de blocos, erroneamente confundida com a cadeia de blocos do Bitcoin.

Block Explorer. Um *block explorer* (explorador de blocos) ou *blockchain browser* (navegador *blockchain*), é um site ou programa de computador que permite visualizar e navegar pela *Blockchain* do Bitcoin ou de altcoins (outras criptomoedas). Os *blocks explorers* mostram, de forma amigável e legível ao ser humano, todas as transações, endereços, blocos e outras informações da *blockchain*. Exemplos: https://www.blockchain.info ou https://www.blocktrail.com/BTC.

Block header. Ver Cabeçalho de bloco.

Bloco altura (*block height*). A tradução mais precisa seria "altura do bloco". Trata-se de um número sequencial de um bloco na *blockchain*. Altura 0 (zero) refere-se ao bloco gênesis (primeiro). Vários blocos podem compartilhar a mesma altura, mas apenas um deles pertence à cadeia principal.

Bloco cabeçalho. Ver Cabeçalho de bloco.

Bloco gênesis (*genesis block*). O primeiro bloco na *Blockchain* com conteúdos codificados e uma referência *all-zero* (tudo zero, sem nada ou nenhuma) a um bloco anterior. O bloco gênesis do Bitcoin, minerado por Satoshi Nakamoto, foi lançado em 03 de janeiro de 2009 com uma citação de jornal em sua coinbase: "The Times 03 / Jan / 2009 Chancellor na beira do segundo resgate para os bancos" (manchete do jornal The Times, do dia 3 de janeiro de 2009 sobre a inflação constante da oferta de moeda pelos governos e bancos), como uma prova de que não há nenhum bloco secretamente pré-minado. Veja Mineração.

Bloqueio de tempo (*lock time ou locktime*). Um campo de 32 bits em uma transação que significa tanto a altura de um bloco em que a operação se torna válida ou um timestamp UNIX. Zero significa que a transação é válida em qualquer bloco. Um número menor do que 500000000 é interpretado como um número de bloco; caso contrário, será um *timestamp*.

Bluebugging. Tipo de invasão através de falhas de segurança em dispositivos Bluetooth.

Bluetooth. Padrão para tecnologia de comunicação de dados e voz, baseado em radiofrequência e destinado à conexão de dispositivos em curtas distâncias, permitindo a formação de redes pessoais sem fio. Muito comum em aparelhos celulares.

Bot. Tipo de código malicioso (*malware*). Programa que, além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor (*hacker*), permitindo-lhe o controle remoto do dispositivo infectado. O processo de infecção e propagação do bot é similar ao do *worm*; ou seja, o bot é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em dispositivos computacionais. Não confundir bot com boot. Veja Computador zumbi.

Botnet. Rede formada por computadores infectados com bots. Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de *spam*, etc.

Boot. É o processo de inicialização (*booting*) de um computador ou dispositivo eletrônico, que começa ao apertar o botão ligar. Após apertar o botão ligar, é ativado o chip da BIOS (*Basic Input Output System* ou Sistema Básico de Entrada e Saída), que irá ligar os demais componentes do aparelho (computador, impressora, videogame, etc.), fazer um diagnóstico (inventário [lista de presença] e teste de funcionamento) dos componentes existentes e, por fim, iniciar o sistema operacional e deixá-lo pronto para o uso. O boot, portanto, só é finalizado (completado) quando o sistema operacional pode ser utilizado pelo usuário. O BIOS consiste numa memória ROM (com teor gravado de fábrica e que somente pode ser lido e executado; não podendo, em regra, ser alterado pelo usuário). O programa gravado em uma memória ROM é chamado de *firmware* e o fabricante pode disponibilizar atualizações do *firmware*. Não confundir boot com bot.

BPS (bits por segundo). É uma medida de velocidade de transmissão de dados utilizada para avaliar a velocidade de conexão à Internet. Veja Latência.

BTC - Abreviação da unidade monetária da bitcoin. Veja Satoshi e XBT.

***Browser* (navegador)**. É o programa usado para navegar pela Internet (acessar sites ou páginas). Veja Navegador.

***Budget* (orçamento)**. Documento onde se definem claramente os ganhos e as perdas de uma empresa ou pessoa física.

***Buffer* (retentor ou amortecedor)**. Memória intermediária auxiliar, que facilita as tarefas, pois alivia o processador. É uma região de memória física utilizada para armazenar temporariamente os dados enquanto eles estão sendo movidos de um lugar para outro. Por dedução lógica, é uma quantidade ou parte de memória de uma mídia mais rápida, usada para armazenar parte dos dados de uma mídia mais lenta. Desse modo, é usado para otimizar a leitura ou a gravação no caso de mídias de alta latência ou baixa velocidade. Ver cache.

***Bug* (inseto ou besouro)**. Apelido dado a uma falha no sistema, quase sempre como consequência de um erro de programação. Costumeiramente designa um erro escondido num programa ou um erro de programação. O apelido surgiu em 1945, quando uma mariposa, entrou num computador Mark II, na Universidade Harvard, e travou todo o sistema. No relatório do incidente, constou a expressão "Havia um bug no sistema". *Bug* é similar a *Tilt*. Veja, ainda, *lag* no verbete latência.

Bull market. Significa que o mercado está em uma tendência de alta, com os preços das ações subindo. Dessa expressão surgiu o adjetivo “bullish” para designar aqueles que estão otimistas com o mercado.

Bullish. Tendência em um mercado quando, pela predominância da demanda, o preço dos papéis sofre alta. O termo em inglês vem de "bull" (touro). Um touro ataca com movimentos de baixo para cima, erguendo seu rival no ar; ilustração similar a um gráfico cujos preços dos papéis são ascendentes. Veja *Bull market* e *Bearish*.

Busca orgânica (*organic search*). São os resultados naturais de um mecanismo de busca (pesquisa); ou seja, aqueles não-pagos (patrocinados ou propaganda). Veja AdWords e Link patrocinado.

Buyers. Compradores no mercado negro (*black market*).

BYOD. Abreviação de *bring your own device* (traga seu próprio aparelho). É a prática de permitir que funcionários usem computadores pessoais no trabalho.

A, B, **C**, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

Cabeçalho de bloco (*block header*). Uma estrutura de dados de 80 bytes contendo os dados do respectivo bloco; que incluem o número de versão do bloco, *hash* de uma raiz ou árvore de Merkle de transações, *timestamp*, dificuldade e *nonce*.

Cache. Cache é um dispositivo de acesso rápido, interno a um sistema, que serve de intermediário entre um operador de um processo e o dispositivo de armazenamento ao qual esse operador acede. A vantagem principal na utilização de um cache consiste em evitar o acesso ao dispositivo de armazenamento (que pode ser demorado), armazenando os dados em meios de acesso mais rápidos. Assim, a memória cache é um dispositivo de memória colocado entre a CPU (processador) e a memória principal (RAM), com o intuito de aumentar o desempenho do sistema. É uma pequena quantidade de memória localizada perto do processador pelo fato de a memória RAM (temporária) normalmente não acompanhar a velocidade do processador; a memória RAM (*Random Access Memory* ou Memória de Acesso Randômico) por ser lenta, faz o processador ter que esperar os dados serem liberados por ela. Um cache é um bloco de memória para o armazenamento temporário de dados que possuem uma grande probabilidade de serem utilizados novamente. **Cache e buffer não se confundem**. Ambas são memórias temporárias, mas uma é destinada ao processamento (cache) e outra para transferência (buffer). Buffer é uma região de armazenamento de memória física usada para armazenar dados temporariamente enquanto eles estão sendo movidos de um lugar para outro. Buffer é uma memória temporária para evitar erros ou a perda de dados durante a gravação ou transferência de dados. O buffer serve como uma espécie de controlador, que ordena em fila os dados a serem processados pelo processador e funciona como uma memória super-rápida. Já cache é uma memória auxiliar em processadores para aumentar a velocidade, pois os dados ficam mais facilmente acessíveis ao processador do que a demora que seria ele ir buscar a informação na memória RAM. Enquanto que cache implica que os dados vão ser reutilizado múltiplas vezes, o buffer somente o transfere (usa) uma única vez e, normalmente, os dados são drenados (migram para o destino estabelecido sem deixar cópia) ou descartados (deletados) após a operação. Um cache é acessado como se estivesse acessando diretamente os dados na sua fonte original ou direta (não há intermediação). Enquanto o buffer trabalha com a integridade (todos) dos dados envolvidos, o cache pode trabalhar com todos, alguns ou nenhum dos dados envolvidos. Veja Buffer e Memória.

***Cache* de motor de pesquisa**. Funcionalidade de um motor de busca que permite ao utilizador visualizar uma página mesmo que esta já não esteja

mais disponível no seu site de origem. Trata-se de um *back-up* (cópia de segurança arquivada) que facilita a recuperação de informações recentemente ou frequentemente acessadas. Exemplo: http://cachedview.com/index.php?lang=pt.

Cadeia de blocos. Veja *Blockchain*, *Block* (Bloco) e Cadeia principal.

Cadeia principal (*main chain*). A cadeia principal consiste na maior série de blocos desde o primeiro bloco minerado, o bloco gênese, até o último bloco minerado, o bloco atual. Portanto, a cadeia principal é a relação de blocos válidos ou constantes da *Blockchain* (cadeia de blocos). A adesão à *Blockchain* é definida pela seleção do bloco que tiver a maior prova de trabalho (maior dificuldade). Desse modo, ao ser selecionado, o bloco passa a fazer parte da cadeia principal. Entretanto, durante um certo período, esse bloco recém adicionado à *Blockchain* corre o risco de ser excluído da cadeia principal; como, por exemplo, não conseguir dar continuidade à corrente. Quando a cadeia paralela possuir maior grau de dificuldade, ela é considerada uma cadeia principal por todos os nós e a transação originalmente válida, torna-se inválida. Quando dois blocos se encontram ao mesmo tempo, os mineiros trabalham sobre o primeiro bloco que receberem e exibem a cadeia mais longa de blocos logo que o bloco seguinte é encontrado. Às vezes, o bloco novo estende uma corrente (sequência) paralela à corrente principal. Nesse caso, o nodo (nó ou cliente) irá anexar o bloco novo à corrente secundária que ele estendeu e, então, irá comparar a dificuldade da corrente secundária com a dificuldade da corrente principal. Se a corrente secundária possuir uma dificuldade acumulada maior do que a da corrente principal, o nodo irá convergir novamente para a corrente secundária; ou seja, ele irá selecionar a corrente secundária como sua nova corrente principal, fazendo com que a corrente principal anterior se torne uma corrente secundária. Se o nodo for um minerador, ele irá construir um bloco ao estender essa corrente nova, por ser a mais longa. As transações são enviadas para os demais participantes da rede e ficam em uma fila esperando processamento, que é a agregação dessa transação específica com outras formando um bloco que precisa ser resolvido. Ao resolver esse bloco, o minerador envia o bloco para os demais participantes da rede para conferência da solução, e se estiver tudo certo, o bloco é acrescentado ao encadeamento de blocos (*blockchain*). As transações na rede Bitcoin

somente são consideradas confirmadas quando pertencentes à uma cadeia principal; que é aquela com a maior dificuldade cumulativa de todos os blocos. Transações não confirmadas não fazem parte da *Blockchain*. Se um bloco não faz parte da cadeia principal, significa que há uma cadeia mais longa de blocos que não inclui ele. Estes são chamados de blocos órfãos ou cadeias inválidas. Portanto, blocos órfãos são aqueles que existem fora da cadeia principal. Se um bloco está na cadeia principal, o seu pai automaticamente também está na cadeia principal. Se um bloco válido é recebido e nenhum pai (bloco anterior) é encontrado nas correntes existentes, o bloco é considerado um órfão. O bloco órfão, portanto, é um bloco válido que já não faz parte da cadeia principal. Geralmente acontece isso quando dois ou mais blocos da mesma altura (posição) são produzidos ao mesmo tempo. Quando um deles se torna uma parte da cadeia principal, o outro é considerado órfão. Órfãos também podem surgir quando a *Blockchain* é bifurcada devido a um ataque de 51% ou um *bug*. Os nós da rede armazenam todos os blocos (válidos e órfãos) e recalculam a dificuldade quando recebem um novo bloco. Se o bloco recém-chegado é preterido por algum bloco anterior para estender a cadeia principal, esse procedimento é denominado de reorganização. Se alguns clientes (nodos) discordam sobre qual corrente é a principal (duas partes diferentes da rede ver diferentes correntes principais), um *fork* (cisão ou bifurcação) acontece. Há duas formas principais de se realizar um duplo gasto: reverter uma transação não confirmada, fazendo outra que tem uma maior chance de ser incluída em um bloco (só funciona com os comerciantes que aceitam transações de confirmação de zero) ou pela mineração a cadeia paralela, com uma segunda transação, ultrapassar a cadeia principal onde a primeira transação tinha sido incluída. Veja Mineração.

Caixa eletrônico. Ver ATM.

Captcha (*Completely Automated Public Turing test to tell Computers and Humans Apart*). É um teste para diferenciar se o acesso a uma página está a ser feito por uma pessoa ou por uma máquina. São normalmente aquelas letras com formato estranho que se pede que sejam reescritas numa caixa de texto antes de inserir um formulário. É usada como ferramenta anti-*spam*. Saiba mais em *Captcha* no teor do e-book.

Carding. Prática de roubo e venda de informações de cartão de crédito.

Carteira (*wallet*). Uma carteira Bitcoin é o equivalente a uma carteira física na rede Bitcoin. A carteira contém a *private key* (chave privada) que permite "enviar" (transferir a titularidade, domínio ou propriedade) os bitcoins. Trata-se, portanto, de uma aplicação, software ou serviço web que ajuda a manter as chaves privadas guardadas e protegidas para futuras operações de assinatura. A *wallet* não mantém bitcoins ou altcoins (as unidades das moedas só existem nas *blockchains*). Armazenar bitcoins ou altcoins, portanto, significa armazenar as chaves privadas. Veja: Chave pública. Confira o capítulo "COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?".

Carteira determinística (*deterministic wallet*). Um termo genérico para maneiras diferentes de gerar uma sequência de chaves privadas e/ou chaves públicas. Ao contrário do velho estilo das carteiras Bitcoin, que geram novos endereços Bitcoin e chaves privadas aleatoriamente; em uma carteira determinística (não aleatória) todos os dados são gerados utilizando um algoritmo específico a partir de uma única semente. Uma carteira determinística, portanto, é um sistema de derivação de chaves a partir de um único ponto de partida conhecido como uma semente. A semente permite que um usuário faça um *backup* e, assim, possa restaurar uma carteira sem necessidade de qualquer outra informação e, em alguns casos, permite a criação de endereços públicos sem o conhecimento da chave privada. Certos tipos de carteira determinística, para maior segurança e comodidade, permitem a separação completa da criação de chave pública e privada. A forma mais simples de uma carteira determinística é baseada no *hashing* de uma cadeia secreta concatenado com um número chave. Para cada número de *hash* resultante é utilizado como uma chave privada (a chave pública é derivada a partir dela). O esquema mais complexo usa a curva elíptica aritmética para derivar sequências de chaves públicas e privadas separadamente, o que permite gerar novos endereços para cada pedido de pagamento sem armazenar chaves privadas em um servidor web. Em suma, uma carteira determinística é qualquer sistema que usa uma senha ou outro trecho de dados para criar um par de chaves de uma maneira repetível. Contanto que se lembre da senha, o par de chaves pode ser re-gerado a partir dela. Uma carteira determinística é, assim, qualquer carteira para que uma

determinada chave privada pode ser previsivelmente recuperada apenas com a semente secreta original ou o número identificador da sequência do par de chaves desejado. Existem dois tipos de carteiras determinísticas: sequenciais e hierárquicas. Na carteira determinística sequencial, a semente é uma senha ou sequência de caracteres que podem ser repetidamente incrementados e com base na frase-senha, o *hash* gera novas chaves privadas. Já numa carteira determinística hierárquica, inicia-se com um único par de chaves denominado de mestra ou mestre. A chave privada deste par de chaves é a semente secreta. A chave pública principal é uma chave que pode ser gerada a partir da chave privada mestra (semente); que tem o poder de gerar todos os endereços em uma carteira Bitcoin, mas nenhum das chaves privadas. Cada par de chaves tem filhos. E a chave pública de um filho de um dado nó pai na árvore é gerado através da realização da curva elíptica multiplicação sobre a chave pública do pai. A chave privada do filho pode ser recuperada pelo proprietário realizando a mesma operação multiplicadora sobre a chave privada do pai: m pubkey / pubkey = m Privkey / Privkey. Pode-se ir de uma chave pai em uma chave filho, mas não em sentido inverso. Pode-se fornecer a chave pública mestre sem risco os fundos, mas só à privacidade.

Carteira web (*web wallet*). A funcionalidade de uma carteira de serviços web normalmente é armazenar, enviar e receber bitcoins. O usuário tem que confiar na fornecedora do serviço para manter seus bitcoins ou altcoins de forma segura e pronto para resgatar a qualquer momento. A carteira web mais segura e respeitada é https://blockchain.info/. Não é recomendado armazenar grandes quantidades de bitcoins em uma carteira web. Confira os capítulos: "ONDE SE GUARDAM AS BITCOINS E ALTCOINS?" e "COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?".

Casa de câmbio. Veja *Exchange*.

Casascius coins. Moedas colecionáveis físicas produzidas por Mike Caldwell. Cada moeda contém uma chave privada no âmbito de um holograma inviolável. O nome "Casascius" é formada a partir de uma frase "chamar os bois pelos nomes", como uma resposta a um nome da própria Bitcoin.

Cavalo de Tróia (*trojan horse*). Programa nocivo utilizado por *hackers* para invadir computadores. Ao contrário dos vírus, ela não se dissemina automaticamente, mas geralmente vem em um arquivo anexado por e-mail. Veja o verbete *Cracker* no Glossário e o termo *Trojan* no corpo do e-book.

Certificado digital (*digital certificate*). Registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital. Veja Assinatura e Autoridade certificadora no Glossário e o capítulo "CERTIFICADOS DIGITAIS".

***Change* (alterar)**. Nome informal para uma parte de uma saída de transação que é retornado para um remetente como uma "mudança" depois de passar essa saída. Desde saídas de transação não pode ser parcialmente esvaziado, pode-se gastar 1 BTC de 3 saída BTC ser apenas a criação de duas novas saídas: uma saída de "pagamento" com 1 BTC enviado para um endereço do beneficiário, e uma saída de "mudança" com o restante 2 BTC (menos taxas de transação) enviados para endereços do pagador. BitcoinQT (atualmente Bitcoin Core) sempre usa novo endereço a partir de um *pool* (piscina) de chave para uma melhor privacidade. Blockchain.info envia para um endereço padrão na carteira. Um erro comum quando se trabalha com uma carteira de papel ou de uma carteira cérebro é fazer uma transação de alteração para um endereço diferente e, em seguida, acidentalmente excluí-lo. Por exemplo, quando a importação de uma chave privada em uma carteira BitcoinQT temporária, fazendo uma transação e, em seguida, apagar a carteira temporária. Veja *Key pool*.

***Charge Back* (cobrar de volta)**. Também conhecido como contestação de pagamento, refere-se ao cancelamento de uma compra efetuada com cartão de crédito ou débito em uma loja virtual, normalmente, devido ao não reconhecimento da compra por parte do titular do cartão (por fraude). Desta maneira, o comerciante entrega o produto, mas não recebe o valor correspondente. No mercado negro essa desavença comercial se chama *dispute* (disputa).

***Chat* (conversar)**. Em inglês, significa bater papo. Existem programas de *chat* que permitem fazer conversas em tempo real pelo teclado.

Chave criptográfica (*cryptographic key*). Algoritmo que permite decodificar um arquivo criptografado. Há duas modalidades de chaves: uma pública (*public*) e outra privada (*private* ou *secret*). Veja: Assinatura (*signature*), Chave privada (*private key*) e Chave pública (*public key*). Confira, ainda, os capítulos: "CERTIFICADOS DIGITAIS", "SEGURANÇA DIGITAL", "ONDE SE GUARDAM AS BITCOINS E ALTCOINS?" e "COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?".

Chave privada *(private key)*. A chave privada é um pedaço secreto de dados que comprova a identidade, a autoridade ou a titularidade. Em resumo, é uma longa sequência de números e letras. No caso do Bitcoin, a assinatura criptografada prova o direito de gastar (transferir a titularidade, posse ou propriedade) as bitcoins que constam da *Blockchain* (identificadas através de uma, ou mais, chaves públicas que possuem a função semelhante a um cofre que somente é aberto com a chave privada única e exclusiva). As chaves privadas (*private keys*) são armazenadas nas carteiras (*wallets*) e nunca devem ser reveladas (mostradas) para ninguém; pois, pior do que a senha do serviço *Internet banking*, permitem a quem a conhece movimentar, de forma irreversível (não há estorno), todas as bitcoins correlatas. Veja: Chave criptográfica (*cryptographic key*) e Chave pública (*public key*).

Chave pública (*public key*). Uma chave criptográfica é um conjunto de bits utilizado com um algoritmo capaz de codificar e de decodificar informações. Sem a chave correta é impossível acessar a informação. Através do algoritmo de assinatura digital da curva elíptica (ECDSA - *Elliptic Curve Digital Signature Algorithm*) gera-se a chave privada com base num valor aleatório e através de um ponto de coordenadas 2D em uma curva elíptica derivada dessa chave privada, gera-se a chave pública através de vários *hashes* SHA-256 e operações RIPEMD-160, até que finalmente ocorra a conversão num formato chamado Base-58. Diferentemente da criptografia simétrica (ou criptografia de chave privada), que usa a mesma chave privada para criptografia e descriptografia; como o sistema de encriptação do Bitcoin é assimétrico (uso de par de chaves ou criptografia

de chave pública), apesar das chaves (privada e pública) serem diferentes, elas são matematicamente ligadas (a chave pública é criada a partir da chave privada), formando um par exclusivo (casamento monogâmico, fidedigno e eterno). Desse modo, para cada chave pública, existe uma única e exclusiva chave privada associada. Ainda mais, como as chaves privada e pública são relacionadas entre si; a operação executada por uma pode ser revertida pela outra. A chave privada é utilizada para assinar mensagens (no caso do Bitcoin, as transações) e a chave pública é usada para verificar se a assinatura está correta. Em resumo, a chave pública é gerada a partir da chave privada; a qual, por sua vez, surgiu de caracteres aleatórios. Como o endereço Bitcoin (*Bitcoin address*) é uma versão *hash* (resumida) da chave pública, na prática, endereço bitcoin e chave pública são a mesma coisa (não é bem a mesma coisa, mas são intimamente relacionados). Tanto é assim que há um termo misto: endereço público; que é disponibilizado e tornado acessível a qualquer pessoa que deseje efetuar um pagamento (transferir créditos ou a titularidade de unidades da moeda virtual) para o proprietário (titular) de tal endereço público. A chave pública é similar às informações bancárias necessárias para efetuar um depósito (nome do banco, número da agência, tipo de conta e o número da conta bancária) e a chave privada é semelhante à senha de referida conta bancária. Entretanto, o endereço público é algo simples como um endereço de e-mail; qualquer pessoa pode enviar e-mails para dito endereço de e-mail, mas somente quem tem a senha de acesso pode enviar e-mails através de dito endereço de e-mail. Em conclusão, pode-se dizer que chave pública (*public key*), endereço público (*public address*) e endereço Bitcoin (*Bitcoin address*) são sinônimos. Veja: Chave criptográfica (*cryptographic key*) e Chave privada (*private key*).

***Checkpoint* (ponto de verificação)**. Um *hash* de um bloco antes do qual o software cliente Bitcoin Core (antigo BitcoinQT) cliente transfere blocos sem verificação de assinaturas digitais por motivos de desempenho. Um ponto de verificação geralmente se refere a um bloco muito profundo (pelo menos vários dias de idade), quando é claro para todos que esse bloco é aceito pela esmagadora maioria dos usuários e a reorganização não vai acontecer além desse ponto. Ela também ajuda a proteger a maior parte da história de um ataque de 51%. Desde *checkpoints* afetar a forma como a cadeia principal é determinado, eles são parte do protocolo e deve ser

reconhecida por clientes alternativos (embora, o risco de reorganização após o ponto de verificação seria incrivelmente baixo).

***Checksum* (soma de verificação)**. Método usado para verificar a integridade de dados. São exemplos os algoritmos (códigos) MD5 e SHA. Veja *Hash*.

Chipset. Conjunto de componentes eletrônicos (chips), em um circuito integrado, que gerencia o fluxo de dados entre o processador, memória e periféricos. É normalmente encontrado na placa-mãe, mas também existe em outros *hardwares*. O *chipset* também determina quais as frequências de barramento a placa-mãe irá suportar e quais processadores poderão ser usados.

Ciberespaço (*cyberspace*). Termo inventado por William Gibson no seu romance Neuromancer. Designa-se habitualmente o conjunto de todas redes de computadores interligadas e de toda a atividade existente nelas. É uma espécie de planeta virtual, onde as pessoas e as máquinas se relacionam virtualmente através de meios eletrônicos.

***Cipherspace* (espaço cifrado)**. Qualquer rede de anonimato (Tor, I2p, Freenet, etc.).

Circuito integrado de aplicação específica (ASIC - *Application specific integrated circuit*). É um circuito projetado especificamente para resolver aplicação de computação muito específica. Ver ASIC.

Clearnet. Internet regular ou convencional (sem o Tor). Veja *Deep Web*.

Cliente (*client*). Em informática, é um processo ou programa que requisita serviços a um servidor.

Cliente leve (*Lightweight client*). Comparando a um nó completo (*full node*), o nó leve (parcial, incompleto ou simples) não armazena toda a *Blockchain* e, portanto, não é possível verificar totalmente qualquer transação. Existem dois tipos de nós leves: os que confiam totalmente um serviço externo para determinar o equilíbrio da carteira e a validade das

transações (por exemplo blockchain.info) e os aplicativos de execução de verificação de pagamento simplificado (SPV - *Simplified Payment Verification*). Clientes SPV não precisam confiar em qualquer serviço particular, mas são mais vulneráveis a um ataque de 51% do que os nós completos. Confira os verbetes: Nó e Nó completo. Veja, também, a definição de nó no corpo do e-book.

Clique (*click*). Pressão sobre o botão do mouse, que geralmente causa a mudança de abertura de uma nova página ou mensagem. É uma métrica importante para o mercado publicitário.

***Clock* (relógio)**. A maioria dos circuitos integrados complexos usa um sinal de *clock* (a partir de um oscilador de cristal) para sincronizar as diferentes partes do circuito. A medição do *clock* é feita em hertz (Hz), a unidade padrão de medidas de frequência. Um sinal de *clock* oscila entre os estados alto e baixo, gerando uma onda quadrada. O *clock* nada mais é do que a frequência com que o processador consegue executar as tarefas. Ou seja, quanto maior a frequência (o *clock*), menor será o tempo de execução e, portanto, mais rápido será o processador. Em suma, é a capacidade que o processador tem de desempenhar um número específico de tarefas em determinado período de tempo. Quando os dispositivos do computador recebem o sinal de executar suas atividades, dá-se a esse acontecimento o nome de "pulso de *clock*". Em cada pulso, os dispositivos executam suas tarefas, param e vão para o próximo ciclo de *clock*. Desse modo, a partir do *clock*, podemos entender também o tempo de latência (quantidade de ciclos para completar uma tarefa) de alguns componentes. Entretanto, o *clock* (frequência) não é o principal determinante da velocidade do processador. Há de levar em consideração a arquitetura do processador. Desse modo, por exemplo, processadores com dois núcleos tendem a ser mais velozes do que os antigos CPUs de núcleo único. No ramo da computação científica, para comparação de um ou mais computadores, usa-se a medição em *FLoating-point Operations Per Second* (operações de ponto flutuante por segundo), que é mais adequada. Veja *Overclocking*.

***Cloud Computing* (computação em nuvem)**. Significa rodar ou executar algum tipo de serviço em um *datacenter* (banco de dados), de forma compartilhada, em um serviço online (na Internet). Exemplo: Aprex

(http://www.aprex.com.br/), que oferece um conjunto de ferramentas para uso profissional, como calendário, gerenciador de contatos, lista de tarefas, armazenamento de arquivos, blog, serviço de e-mail marketing, apresentações, dentre outros. Tudo feito pela Web e, no caso de empresas, é possível até mesmo inserir logotipo e alterar o padrão de cores das páginas. Também existe o Google Cloud Platform (https://cloud.google.com/?hl=pt-br). Veja ERP.

***Cluster* (ou *clustering*)**. Técnica utilizada para colocar diversos processadores em paralelo, normalmente utilizada em servidores, para aumentar a capacidade de processamento individual de cada processador.

***Coach* (treinador)**. É um facilitador, instrutor ou entidade (pessoa, equipe, departamento, empresa, etc.) que atua como agregador das capacidades de cada elemento da cadeia (equipe, departamento, empresa, etc.).

Codecs. Programa com um algoritmo que serve para codificar e descodificar uma sequência de vídeo.

Código. Veja Linguagem e Software.

Código ASCII. Ver ASCII.

Código binário (*binary code*). Sistema (linguagem) de codificação, utilizado por máquinas com circuitos digitais para interpretar informações e executar ações, onde todos os valores (dados, informações, entradas, saídas, etc.) são representados apenas pelos caracteres 0 (zero) e 1 (um) ou sinais positivos (+) e negativo (-). Por outras palavras, o computador não lê igual aos humanos (letras, números, caracteres especiais, símbolos, desenhos, etc.). Ele só consegue ler sinais elétricos na sua forma mais simples: sem corrente ou com corrente, representados respectivamente pelos números 0 e 1. Veja Analógico, Bit, FAX, Modem e Digital no glossário e códigos binários no teor do e-book.

Código-fonte (*source code*). Texto ou linhas de programação que formam um software em sua forma original ou primária (escrita por um

programador através de uma linguagem como C++ ou Visual Basic); que, para poder ser executado, precisa ser convertido (compilado) para a linguagem de máquina (a única que o computador entende). Desse modo, em regra (na maioria das vezes), ao se comprar ou "baixar" (fazer o *download*) de um programa (software), se está adquirindo a linguagem de máquina e não o código-fonte. Um programador na posse de um código-fonte pode alterar a forma como o respectivo software funciona (por exemplo, adicionar, remover ou alterar recursos), adaptando às suas necessidades, interesses, conveniências, gostos e bel prazer. Saiba mais nos capítulos: "SOFTWARES LIVRE E *OPEN SOURCE*" e "CONSIDERAÇÕES SOBRE *START-UP* OU PROJETO DE *SOFTWARE*".

Código malicioso (*malicious code*). Pequenos softwares ou aplicativos, normalmente escritos em ActiveX ou Java, que se disseminam pela Internet e mídias e se instalam, sem autorização e, até mesmo sem aviso ou de forma camuflada, no dispositivo computacional do usuário, utilizando-se brechas na segurança ou descuido do usuário. Ver Malware.

Coinbase - Um script de entrada de uma transação que gera novas bitcoins ou o nome dessa própria operação. Não confundir com o site Coinbase.com. O termo inglês "coinbase" quer dizer "base da moeda". A transação coinbase é a primeira transação (ou transação de entrada) de um bloco; portanto, é a transação de geração do respectivo bloco. As transações possuem uma entrada (chamada também de coinbase), cujos dados (teor ou conteúdo) pode ser qualquer coisa. O bloco gênesis, por exemplo, possui uma referência ao artigo do Times de 03 de janeiro de 2009 para provar que mais blocos não foram criados antes dessa data. Coinbase também é usado para votar uma alteração de protocolo; ou seja, os mineiros inserem propostas no coinbase e se a maioria dos outros mineiros aprovarem, irá essa proposta ser submetida aos usuários comuns (não mineradores). Se estes aceitarem, simplesmente vai começar a ser aplicada a nova regra. Se essa aprovação for de apenas uma minoria, ou ocorre uma bifurcação gerando uma nova altcoin ou todos aceitam a nova regra. Entretanto, na transação coinbase (primeira transação ou transação de entrada de um bloco), não é utilizado o espaço destinado para as informações de entrada ("input"); diz-se, portanto, que referido campo fica vazio ou sem nada. Por outras palavras, a transação coinbase contêm apenas uma entrada com uma

referência zerada à uma transação anterior e dados arbitrários no lugar do script. Em resumo, a transação coinbase não possui informações de entrada. Explica-se. Enquanto que as demais transações (regulares, convencionais ou comuns) usam a seção "entradas" (*inputs*) para se referir as suas saídas de transações pai (os créditos do pagador constantes da *Blockchain* [cadeia de blocos] são considerados como saídas [saída de transação não gasta ou não desembolsada; ou seja, UTXO - *Unspent Transaction Outputs*] em favor do beneficiário, se tornando novas entradas), uma transação de geração (coinbase) não tem pai (origem ou pagador) e cria novas unidades da moeda absolutamente do nada. Estas unidades de bitcoins criadas do nada (sem *outputs* e sem *inputs*) serão usadas para pagar a recompensa ao minerador por ter conseguido minerar (criar) o respectivo bloco. Pode-se fazer uma analogia do bloco com um trem; ou seja, o primeiro componente (que vem na frente) é a locomotiva (transação coinbase) com seu maquinista ou operador (mineiro) e, atrás dela, estão os vários vagões (transações comuns) com os passageiros (usuários ou partes na transação) e as suas respectivas bagagens (valores das respectivas transações). É a locomotiva que transporta (movimenta) os vagões (transações), cujas despesas são pagas através dos bilhetes (taxas) dos passageiros (usuários) nos vagões. É por meio dos vagões (transações) que os passageiros com suas bagagens saem da ferroviária (*Blockchain*) e entram novamente na ferroviária (*Blockchain*). Apesar de o condutor do trem não ter comprado bilhete (passagem ou ingresso) e nem possuir nada no bagageiro dos vagões, ele também está sendo transportado e levando consigo alguma bagagem pessoal. Outro detalhe, no caso, é o próprio maquinista (minerador) do trem que efetua o trabalho de cobrador dos bilhetes (taxas) dos passageiros; portanto, ele leva consigo o valor recolhido na cobrança dos bilhetes. Reforçando, tal como uma compra (aquisição) de mercadoria (entrada) num estabelecimento comercial implica na prévia realização de uma saída da mesma mercadoria (tanto no estoque ou depósito do vendedor como também do fornecedor do vendedor), quando se envia bitcoins ou satoshis para alguém, na verdade se está criando uma saída (*output*) de transação não-gasta (UTXO) registrada para o endereço dessa pessoa e tornando-a disponível para ser gasta. Os UTXOs consumidos por uma transação são chamados de entradas (*inputs*) de transação e os UTXOs criados por uma transação são chamados de saídas (*outputs*) de transação. Quando os usuários fazem um pagamento, a carteira deles constrói uma transação ao selecionar a partir do UTXO disponível.

Por exemplo, para fazer um pagamento de 0,015 bitcoin, o aplicativo de carteira pode selecionar um UTXO de 0,01 e um UTXO de 0,005, usando ambos para somar a quantia de pagamento desejada. Dessa maneira, bitcoins ou satoshis se movem adiante de dono (titular) para dono (titular) numa cadeia sequencial de transações (similar à circulação de um cheque mudando de mãos) que consome e cria UTXOs. As transações consomem UTXOs quando as desbloqueiam com a assinatura (chave privada) do dono atual e criam UTXOs quando as vinculam ao endereço Bitcoin do novo dono. Desse modo, a exceção para a cadeia de *output* (saída) e *input* (entrada) é um tipo especial de transação chamada transação coinbase. Portanto, todas as transações na rede Bitcoin não são criadas igualmente. Uma transação coinbase é um tipo único de transação Bitcoin que só pode ser criada por um mineiro. Por outras palavras, a primeira transação em um bloco deve ser uma transação coinbase; a qual deve recolher e gastar quaisquer taxas de transações incluídas neste bloco. Em outras palavras, a transação coinbase (ou transação de base da moeda) é a transação que recompensa um mineiro por seu trabalho com o respectivo bloco. Todas as taxas de transações cobradas pelo minerador também são enviadas nesta transação. Outro detalhe, as bitcoins constantes de uma transação coinbase não podem ser gastas até que tenham recebido 100 (cem) confirmações na *Blockchain*. A transação coinbase funciona de forma similar ao tráfego de pacotes na Internet. Confira sobre os pacotes de dados na Internet no verbete Endereço IP. Saiba mais sobre UTXO no teor do e-book. Veja Mineração.

Coinbase.com. Site (https://www.coinbase.com/) de câmbio (compra e venda) de bitcoin e ethereum.

Cold storage (armazenamento a frio). Um tipo de carteira *off-line* (desconectada da Internet) segura para bitcoins ou altcoins (outras criptomoedas). Trata-se de um termo genérico para várias medidas de segurança que visam reduzir o risco de acesso remoto para as chaves privadas. Por exemplos, pode ser um computador normal desconectado da Internet, uma carteira de hardware dedicado, um *stick* USB com um arquivo de carteira, uma carteira de papel (*paper wallet*), etc.

Colored coin **(moeda colorida)**. Um conceito de adicionar um significado especial para determinadas saídas de transação. Isto poderia ser

usado para criar um produto comerciável no topo do protocolo Bitcoin. Por exemplo, uma empresa pode criar certa quantidade de ações e declarar uma única saída transação contendo a fonte dessas ações.

Comércio eletrônico (*e-commerce* ou *electronic commerce*). Método pelo qual se vendem mercadorias e serviços pela Internet. Pode ser de duas origens: venda para o consumidor final (conhecido como B2C) e negócios entre empresas (B2B).

***Compact size* (tamanho compacto)**. O nome original de um formato de número inteiro de comprimento variável usada na transação e bloco de serialização. Também conhecida como "encoding de Satoshi". Ele usa 1, 3, 5 ou 9 bytes para representar qualquer inteiro sem sinal de 64 bits. Valores inferiores a 253 são representados com um byte. Bytes 253, 254 e 255 indicam 16, 32 ou 64-bit inteiro que segue. Números menores podem ser apresentados de forma diferente. Em bitcoin-ruby é chamado de "var_int" e em Bitcoinj é VarInt. Bitcoin Core (antigo BitcoinQT) também tem representação ainda mais compacta chamada VarInt, que não é compatível com CompactSize e é utilizada no armazenamento em bloco.

Compilação. Ato de transformar o código-fonte em um código que o computador entenda (código objeto) e, assim, possa o computador realizar a função determinada pelo programador (criador ou autor do código-fonte); pois o computador não executa diretamente os comandos em forma de texto (linguagem humana).

Compilador. Programa que transforma uma lista de comandos em forma de textos (legível) para a forma de linguagem de máquina, que somente o computador identifica (compreende) e usa para execução.

Computação em nuvem. Ver *Cloud Computing*.

Computador zumbi (*zombie computer*). Nome dado a um computador infectado por bot, pois pode ser controlado remotamente e sem o conhecimento do seu dono. Veja Bot.

Comutador (*switch*). É uma ponte multiportas que utiliza um mecanismo de filtragem e de comutação que consiste em dirigir os fluxos de dados para as máquinas mais adequadas. O comutador transmite a mensagem apenas para a porta do destinatário, ficando as outras portas livres para outras transmissões que podem se produzir simultaneamente. O comutador é um aparelho muito semelhante ao hub, mas tem uma grande diferença: os dados vindos do computador de origem somente são repassados ao computador de destino. Isso porque o comutador cria uma espécie de canal de comunicação exclusiva entre a origem e o destino. Por outras palavras, o comutador distribui os dados para cada máquina destinatária, enquanto que o hub envia todos os dados para todas as máquinas que respondem. Veja *Switch*.

Confirmação (*confirmation*). Após o pagador enviar a ordem de pagamento à rede Bitcoin, o sistema mostrará o *status* (situação) "Transação não confirmada" (*unconfirmed transaction*); ou seja, que a transação foi enviada à rede P2P, mas ainda não foi incluída na *Blockchain*. A transação é vista instantaneamente por todos os membros da rede, mas só se torna "confiada" por todos quando está incluída em um novo bloco minerado (e não meramente candidato). Para ser incluída, a transação deve ser escolhida por um nó mineiro, ser incluída em um bloco de transações e este bloco ser inserido na *Blockchain*. Desse modo, quando um novo bloco for criado, em aproximadamente 10 (dez) minutos, as transações dentro desse bloco passam a ser aceitas como confirmadas (*confirmed*) pela rede e, com isso, os créditos recebidos já podem ser gastos pelo favorecido. Detalhe, a mesma transação é inserida, por diferentes mineiros pelo mundo, em vários blocos candidatos, mas somente um dos blocos candidatos, da rodada de 10 (dez) minutos, será inserido na *Blockchain*. Por outras palavras, somente o bloco candidato que apresentar o hash correto ou o mais preciso (e em caso empate, o que possuir a maior quantidade de prova de trabalho) será incluído na *Blockchain*. Desse modo, assim que o primeiro minerador, contendo essa transação em seu bloco candidato, alcançar o resultado de hash esperado pela rede, ele transmitirá o resultado de seu trabalho para que cada nó da rede possa validar por si próprio o trabalho do minerador, adicionar este novo bloco à sua própria cópia da *Blockchain* e continuar propagando esta nova escrita na *Blockchain*; que nada mais é do que um livro-razão espalhado por todos os nós ao redor do mundo de forma pública

e com a possibilidade de verificação por qualquer um que tenha acesso a esta informação. Veja *Transação* e *Verificação*.

***Content analytics* (análise de conteúdo)**. Utilizar tecnologia de análise de dados para pesquisar conteúdo digital em sites, redes sociais, rss *feeds*, etc. Por exemplo, utiliza-se para análise de mercado para saber qual tipo de conteúdo está sendo gerado nas redes sociais e no que as pessoas estão mais interessadas.

***Controlled delivery* - *CD* (entrega controlada)**. Trata-se de uma técnica de vigilância de mercadoria objetivando prender os envolvidos. Assim, por exemplo, uma remessa de drogas ilícitas é detectada, mas permite-se que prossiga seu tráfego sob o controle e vigilância das forças policiais, a fim de obter provas contra os organizadores desse tráfico ilícito de drogas.

Cookie. Não se trata de biscoito ou bolacha. Consiste num pequeno arquivo de texto gravado no computador do usuário quando ele visita um site. O *cookie* registra dados sobre a navegação, como o dia e a hora em que se acessou a página. Cada vez que o usuário visita o site novamente, o navegador (*browser*) envia o *cookie* de volta para o servidor para notificar atividades prévias do usuário; ou seja, torna o site personalizado através de sugestões com base no histórico, nos gostos e nas preferências do usuário. Defensores da privacidade na Internet questionam o uso de *cookies*, que podem ser usados pelos sites para rastrear o comportamento dos internautas. Praticamente todos os sites ou páginas da Internet utilizam *cookie*. Normalmente, se o usuário bloquear o uso de *cookies* não conseguirá acessar inteiramente o teor do site. Alguns sites avisam previamente que utilizam *cookies* e pedem a permissão do usuário. No sistema operacional Windows, o arquivo inetcpl.cpl consiste na pasta "Propriedades de Internet"; ou seja, nas configurações do *browser* (navegador da Internet) nativo (original) do sistema, o Internet Explorer. Desse modo, para excluir os cookies, clica-se na guia “Geral” das “Propriedades de Internet”, clica-se em “Excluir” no “Histórico de Navegação” e, depois, em “Excluir” e em “OK”. No navegador Microsoft Edge, clica-se nos três pontinhos do canto superior direito e depois em “Configurações”. Em seguida, rolasse a tela para baixo e clica-se no botão “Exibir configurações avançadas”; então procura-se pela seção “Cookies”. Já no Chrome, acessa-se as configurações através do botão

hamburguer localizado no canto superior direito. Clica-se no link para mostrar as configurações avançadas e procura-se pela seção “Privacidade”. Nessa página, clica-se no botão “Configurações de conteúdo” e, depois no tópico “Cookies”. Por fim, no Firefox, clica-se no botão hamburguer no canto superior direito e depois em “Opções”. Na lateral esquerda, clica-se em “Privacidade” e, por fim, em “Histórico”.

Cópia de segurança. Ver *Backup*.

CP. Abreviatura de *children porn* (pornografia infantil) normalmente utilizada na *Deep Web*.

CPD - Centro de Processamento de Dados. Veja *Data center*.

CPU. Sigla de *Central Processing Unit*, em português, Unidade Central de Processamento. É o cérebro do computador, onde a maior parte dos cálculos são feitas. No início do Bitcoin, era utilizado para minerar; porém, com o avanço das GPUs e, posteriormente, dos ASICs, ficou para trás. Veja Processador.

Cracker. Não se trata de bolacha ou biscoito. Para os infomaníacos (fissurados em informática), o termo cracker é diferente de *hacker*, que invaderia computadores para fins de testes, estudos ou por pura diversão. Confira no link uma relação exemplificativa de tipos de ataques *hackers*. O termo também designa programas que desbloqueiam senhas e outras travas de segurança dos softwares pagos (uma forma de pirataria); daí diz-se que o programa foi crakeado. Veja Hacker no Glossário e *Hacker* no teor do e-book.

Criptografia (*cryptography*). Ramo da matemática que permite criar provas matemáticas que fornecem altos níveis de segurança. Criptografia é a ciência de usar a matemática para criptografar e descriptografar os dados para uma comunicação segura. Ela permite que o usuário transmita os dados em rede insegura para que eles não possam ser lidos por ninguém, exceto o destinatário pretendido. Comércio on-line e serviços bancários usam criptografia. No caso do Bitcoin, a criptografia é usada para fazer com que seja impossível para qualquer um gastar fundos da carteira de outro usuário ou corromper a *Blockchain*. Também pode ser utilizada para encriptar uma carteira, de modo que ela não possa ser utilizada sem uma senha. Saiba mais sobre criptografia no teor do e-book.

Criptomoeda (*cryptocurrency* ou *cryptocoin*). Meio de trocas ou de pagamentos que se utiliza de criptografia para assegurar transações e

controlar a criação (emissão) de novas unidades da moeda digital. Em resumo, são moedas digitais que utilizam criptografia. Veja Altcoin.

***Cross selling* (venda cruzada)**. Técnica de *marketing* (técnicas e métodos destinados ao desenvolvimento das vendas) em que o lojista oferece a seus clientes produtos complementares àqueles que já foram ou que estejam sendo adquiridos. É similar à venda casada no Brasil.

Crypto News. Serviço oculto de notícias sobre privacidade, segurança, política e tecnologia (http://wittvywowuxp35s6.onion). Endereços contendo o termo ".onion" só são acessíveis pelo navegador Tor.

CSC - *Clients of Special Category* (clientes de categoria especial). Trata-se de uma definição dentro das leis contra lavagem de dinheiro (AML - *Anti-Money Laundering*). Conforme lista ilustrativa, esses clientes incluem: a) clientes não residentes; b) clientes de alto patrimônio líquido; c) confiança, instituições de caridade, ONGs e organizações que recebem doações; d) empresas com participações familiares ou beneficiários; e) pessoas politicamente expostas de origem estrangeira; f) ex-Chefe de Estado e Ex-político de alto nível e pessoas conectadas (família, conselheiros e empresas nas quais tais indivíduos têm interesse ou influência significativa); g) empresas oferecendo ofertas de câmbio; h) países onde a corrupção é altamente prevalecente, onde sanções são aplicadas, que são paraísos fiscais, patrocinadores de terrorismo internacional, centros financeiros *offshores* e fiscais e onde a fraude é altamente prevalente.; i) clientes não face a face; j) clientes com reputação duvidosa conforme informações públicas disponíveis; etc.

CSS - *Cascading Style Sheets* (folhas de estilos em cascata). Linguagem de folhas de estilo utilizada para definir a apresentação de documentos escritos em uma linguagem de marcação, como HTML ou XML.

A, B, C, **D**, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

***Dark net* (rede escura)**. Um termo geral que descreve os sites ocultos hospedados nos protocolos TOR / I2P e outras redes que não se pode

acessar de modo convencional, mas somente através de algum software especial. Veja *Deep Web*.

***Database* (banco de dados)**. É uma compilação de informações, organizadas de uma maneira a que o sistema possa acessar rapidamente uma delas.

***Data center* (centro de dados)**. Também conhecido como centro de processamento de dados (CPD), trata-se de uma instalação projetada para abrigar servidores e outros componentes como sistemas de armazenamento (*storages*) e processamento de dados e de ativos de rede (switches, roteadores, etc.) contando com *backup*, fontes de alimentação de emergência ou de reserva (no-breaks, baterias, geradores, etc.), controladores climáticos ou ambientais (ares condicionados, supressão de fogo, etc.) e vários dispositivos de segurança. Por outras palavras, serve para centralizar as operações e os equipamentos de TI (tecnologia da informação) de uma organização e onde ela os armazena, gerencia e dissemina seus dados. O objetivo principal de um *data center* é garantir a disponibilidade de equipamentos que rodam sistemas cruciais para o negócio de uma organização, tais como, por exemplos, o ERP - *Enterprise Resource Planning* (Planejamento de recurso corporativo) e o CRM - *Customer Relationship Management* (Gerenciamento de Relacionamento com o Cliente), garantindo, assim, a continuidade do negócio. Os *datacenters* abrigam, portanto, os sistemas mais críticos de uma rede e são vitais para a continuidade das operações diárias. Consequentemente, a segurança e a confiabilidade dos *datacenters* e suas informações são uma prioridade para as organizações.

Data Scientist. Literalmente significa um cientista de dados. Trata-se de uma pessoa perita (experta) em dados, estatísticas, manipulação de dados, etc. e que usa esse conhecimento para gerar valor a partir de *big data* (quantidade enorme de informações) e da *Internet of things* (Internet das coisas).

Data Warehouse. Armazenamento de dados

DBAN (*Darik's Boot and Nuke*). Software para apagar permanentemente todas as informações do HD (disco rígido).

DDoS - *Distributed Denial of Service* (ataque distribuído de negação de serviços). Trata-se de um ataque que utiliza um grande número de computadores sob controle de um atacante para enviar pequenas quantidades de tráfegos pela Internet com o objetivo de congestionar o acesso e drenar recursos de um servidor alvo. Não confundir DoS e DDoS com MS-DOS. Veja Bot e DoS.

***Deep Web* (Internet profunda)**. Sinônimo de *Dark Net*. Trata-se de zona da Internet que não pode ser detectada ou acessada pelos tradicionais motores de busca, com o que não estão catalogadas e nem indexadas (sendo ignoradas e desconhecidas destes), com o que, em tese, são garantidas as privacidade e anonimato para os seus frequentadores. Ainda mais, referida área da Internet não segue o padrão (protocolo) da *clearnet* (Internet convencional ou popular); desse modo seus endereços são diferentes e os *browsers* (navegadores) comuns não conseguem sequer processar e, muito menos, acessar os endereços das páginas, sites ou portais. Confira *Deep Web* no teor do e-book.

Defacer. Pessoa responsável pela desfiguração de uma página. Veja *Defacement*.

***Defacement* (desfiguração)**. Uma forma de vandalismo promovida por *hackers* em sites da Web (Internet). Geralmente há a substituição das páginas por uma mensagem política ou social, apagando parte ou totalidade do conteúdo original. Trata-se de vandalismo virtual. Veja Veja *Defacer*.

***Denial of Service* (DoS)**. Veja Negação de serviço.

Derp. Linguagem que expressa algo sem sentido ou estúpido. Um comentário sobre ação boba ou idiota. Gíria da Internet que significa cometer um erro estúpido ou agir estupidamente.

Desfiguração de página (*unconfiguration of page*). Também chamada de pichação (*graffiti*). Técnica que consiste em alterar o conteúdo da página

Web de um site. Veja *Defacement*.

Deterministic wallet. Ver Carteira determinística.

***Desktop* (área de trabalho)**. O computador da pessoa ou a tela inicial do computador. Pode ser mais facilmente entendido como "mesa de trabalho".

Dificuldade (*difficulty*). É uma medida de quão difícil é encontrar um *hash* (novo bloco) abaixo de um determinado alvo (*target*). As transações na rede Bitcoin somente são consideradas confirmadas quando pertencentes à uma cadeia principal; que é aquela com a maior dificuldade cumulativa de todos os blocos. Cada bloco na rede Bitcoin deve cumprir a meta de dificuldade para assegurar o intervalo de 10 (dez) minutos entre os blocos. Confira a explicação de dificuldade no teor do e-book.

Digital. Uma tradução em dígitos do mundo analógico (ou mecânico). Por exemplo, o cérebro humano funciona, basicamente, através de pulsos elétricos. Por exemplo, luz, som e odores são transformados por nossos órgãos sensoriais em um código feito de impulsos eletroquímicos que viajam ao longo dos neurônios (células nervosas que conduzem os impulsos nervosos) do corpo ao cérebro. Desse modo, o tecido nervoso possui a capacidade de responder aos estímulos sensoriais (luz, calor, etc.) através de alterações da diferença de potencial elétrico existente entre as superfícies interna e externa de sua membrana plasmática, se propagando ao longo da célula e de seus prolongamentos. Algo produz som quando vibra na matéria e, quando algo vibra na atmosfera, move as partículas de ar; as quais, por sua vez, movem outras ao redor delas, carregando a vibração pelo ar. Desse modo, quando um sino é tocado, o metal do sino vibra balançando de um lado para o outro empurrando as partículas de ar ao seu redor. Estas, então, colidem com as partículas que estão em sua frente e, assim, sucessivamente. Dessa maneira, o objeto vibrante envia uma onda de flutuação de pressão através da atmosfera. Assim que as ondas sonoras entram no canal auditivo do ouvido, elas vibram a membrana timpânica (tímpano). Quando o tímpano vibra, move o martelo de um lado para o outro, como uma alavanca. A outra parte do martelo é conectada à bigorna, que é ligada ao estribo. A outra ponta do estribo, sua placa de apoio, fica encostada na cóclea, na janela oval. Quando a compressão pela pressão do ar empurra o tímpano, os

ossículos se movem, de maneira que a placa do estribo empurra o fluido da cóclea. Quando a rarefação puxa o tímpano, os ossículos se movem de maneira que a placa puxa o fluido. Essencialmente, o estribo age como um pistão, criando ondas no fluido do ouvido interno para representar as flutuações da pressão do ar da onda sonora. As ondas sonoras aplicam força em cada milímetro do tímpano e o tímpano transfere toda essa energia para o estribo. O martelo, a bigorna e o estribo vibram solidários com o tímpano. As vibrações continuam pela parte interna do ouvido, onde uma estrutura espiral chamada cóclea as transformam em impulsos nervosos. Estes, por sua vez, são transmitidos ao cérebro por meio de um nervo auditivo. Por outras palavras, na cóclea ocorre uma função complexa de conversão de sinais, em resultado da qual os sons nela recebidos (do tipo mecânico) são transformados em impulsos elétricos que são depois encaminhados até ao cérebro através do nervo auditivo, onde são depois descodificados e interpretados. De modo semelhante, um áudio armazenado num CD ou num computador não passam de uma enorme quantidade de números zeros e uns; ou seja, bits. O que nós ouvimos desses bits é uma transcrição analógica dos códigos digitais, executada por nossa mente. Em suma, o tecido nervoso do corpo humano é responsável por receber e responder aos estímulos internos e externos; bem como pela respectiva troca rápida de informações. Portanto, a informação sobre o início e a intensidade de um estímulo é enviada ao cérebro pelo sincronismo e pela frequência destes impulsos elétricos. As células cerebrais, especificamente os neurônios, utilizam impulsos elétricos para se comunicarem entre si, além de fazer os músculos contraírem e os membros se moverem. Cada neurônio produz determinada descarga elétrica com o objetivo de este comunicar com os neurônios e outras células vizinhas. Quando esse impulso elétrico é excessivo surge a epilepsia e quando se perde parcialmente até chegar ao destino surge o Mal de Parkinson (ou doença de Parkinson). O cérebro é formado por bilhões de células (neurônios e glia), cada qual enviando pulsos elétricos a outras células gerando as flutuações voltaicas. As sinapses elétricas ocorrem através desses impulsos elétricos e a comunicação neste tipo de sinapses ocorre devido as junções comunicantes que permitem o fluxo de íons entre as membranas dos neurônios que estão se comunicando. Devido as essas junções comunicantes, as comunicações entre os neurônios que fazem sinapses elétricas são bidirecionais; ou seja, as comunicações ocorrem de ambas as direções, de um neurônio para o outro e não apenas através de um

neurônio pré-sináptico para um pós-sináptico. Os impulsos elétricos cerebrais formam ondas eletromagnéticas de 4 frequências (Beta, Alfa, Teta e Delta). A frequência Beta situa-se entre os 13 - 30 HZ e está associada à atenção, à acuidade visual e à coordenação. No estado Beta o indivíduo está acordado e com a mente concentrada, pronta para trabalhos (aprendizagem, análise e organização de informações) que requerem a atenção total. A faixa Alfa situa-se entre os 7 - 13 HZ e está associada à resolução de problemas, criatividade, memorização, relaxamento e pensamento abstrato e imaginação (visualizações). Neste estado a pessoa está relaxada, sua consciência interna aumenta, aumentando com isso a auto-perceção, a consciência dos pensamentos e os processos internos. Aumenta a criatividade, a ansiedade tende a diminuir e desfruta da sensação de paz e bem-estar. A faixa Teta situa-se entre os 4 - 7 Hertz. O indivíduo entra num estado ainda mais profundo de relaxamento, baixando a atividade cerebral quase ao nível do sono. Neste estado a pessoa sonha acordada, proporcionando-lhe um estado ideal para o acesso a memorias, aprendizagem acelerada, criatividade e reprogramação mental. Propicia também a criatividade e acesso a memórias a muito esquecidas e surgem imagens inconscientes. O estado Delta situa-se entre os 0.1 - 4 Hertz. Nesta frequência é produzido o hormônio do crescimento, além deste estado ser benéfico para a regeneração celular e cura. Neste estado, têm-se acesso mais profundo ao inconsciente e à intuição. Veja Analógico e Processador.

Digital certificate. Veja Certificado digital.

***Dispute* (disputa)**. Termo geralmente usado para descrever um desentendimento entre um comprador e um vendedor no mercado negro. Em relação a cartão de crédito ou débito essa desavença comercial se chama *charge back* (cobrar de volta) ou contestação.

Distributed Denial of Service. Veja DDoS.

DLL - ***Dynamic Link Library***. São bibliotecas de vínculos (ou links) dinâmicos com dados que podem ser acessados por vários programas instalados no computador. São rotinas pré-configuradas que podem ser carregadas e usadas para execução de determinadas tarefas. O uso de DLLs ajuda a promover a modularização do código, reutilização de código, uso de

memória eficiente e menor espaço em disco. Portanto, o sistema operacional e os programas carregam mais rápido, executam mais rapidamente e levam menos espaço em disco no computador. Confira o verbete Biblioteca.

DNS - *Domain Name System* (sistema de nomes de domínio). Protocolo da Internet que converte os nomes e endereços da Internet em seus números correspondentes e vice-versa. Veja Endereço IP.

DNS poisoning* (envenenamento do DNS) ou *DNS spoofing. Ocorre quando um servidor DNS (cuja função é realizar a tradução ou conversão de um nome de domínio para endereços IP) recebe dados não autenticados e armazena os mesmos em sua cache para otimizar o desempenho; tais dados podem ser falsos e, portanto, podemos ter o envenenamento da cache do servidor que fornece os dados não autenticados para seus clientes. Se um servidor DNS é envenenado, este pode retornar o endereço IP incorreto, desviando o tráfego para outro computador.

Domestic. Um termo que se refere a fazer um pedido de um vendedor que reside no mesmo país do comprador. A tradução literal da palavra seria doméstico, mas é melhor compreendida se traduzida por local. Assim "vendedor local" é melhor compreendido do que "vendedor doméstico".

DOS. Veja MS-DOS.

DoS (*Denial of Service*). Veja Negação de serviço.

Double opt-in. A dupla confirmação de que alguém se cadastrou para receber informações comerciais pela Internet. É feito geralmente automaticamente quando a pessoa se inscreve pela Internet e lhe é enviada uma mensagem para o e-mail (caixa postal) pedindo a confirmação da inscrição. Veja *Opt-in* e *Opt-out*.

***Double Spend* (gasto duplo)**. É quando um usuário mal-intencionado tenta passar as mesmas unidades de bitcoins ou altcoins para dois destinatários diferentes ao mesmo tempo. Por outras palavras, é uma tentativa de fraude consistente em gastar a mesma saída de operação duas vezes. Há duas formas principais de se tentar realizar um duplo gasto:

reverter uma transação não confirmada, fazendo com que a outra transação seja incluída em um bloco com maior chance ou probabilidade de confirmação (só funciona com os comerciantes que aceitam transações de confirmação de zero) ou pela mineração a corrente paralela, contendo a segunda transação, ultrapassar a cadeia principal onde a primeira transação foi incluída. Veja, também, ataque de 51%.

***Download* (transferir)**. Significa transferir (descarregar ou baixar) um conteúdo de um servidor web para um computador local. Oposto de *Upload*.

***Downtime* (tempo de inatividade)**. Tempo em que o computador fica parado (ocioso ou inativo) por problemas técnicos ou manutenção preventiva.

Doxx. Ato de postar em um fórum público as informações de identificação pessoal de um pseudônimo usado por um indivíduo ou das informações nela postadas.

Dread Pirate Roberts. O pseudônimo usado pelo administrador do original Silk Road. Especula-se que mais de uma pessoa pode ter vindo a utilizar este pseudônimo, mas "Ross William Ulbricht" foi indiciado pelo FBI como sendo o único proprietário.

Driver. Software ou conjunto de arquivos que contêm informações e instruções para o sistema operacional detalhando a melhor forma de funcionamento de um determinado dispositivo de hardware. *Driver*, que vem do verbo inglês *drive*, que significa o ato de conduzir (dirigir). *Driver* é, portanto, o condutor (operador ou motorista) de algo. A função do driver é fazer o computador e os periféricos (hardwares ou dispositivos) se comunicarem entre si, se entenderem e entrarem num acordo (trabalharem juntos). Cada dispositivo de hardware possui seu driver específico.

***Duck Duck Go* (DDG)**. Um motor de busca que respeita a privacidade (https://duckduckgo.com/).

***Dust* (poeira ou pó)**. Abreviatura de "dust transaction" (transação de pó). É quando a saída de uma transação é menor do que a taxa exigida pela

transação, quando sobra muito pouco (ou quase nada) depois de pagar a taxa ou quando uma transação de pequeno valor ocupa o precioso espaço na *Blockchain*. Bitcoin Core (antigo BitcoinQT) se recusa a transmitir ou a retransmitir transações "poeira" para evitar inutilmente o aumento ou tamanho das saídas de transação não gastos de índice (UTXO). Na versão 0.8.2 do Bitcoin-Qt, a equipe de *core-developers* (desenvolvedores principais) definiu como *dust transaction* uma transação com *output* (saída) menor do que 5.46 uBTC; cerca de R$ 0,007.

A, B, C, D, **E**, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

ECDSA - *Elliptic Curve Digital Algorithm* (algoritmo digital da curva elíptica). Trata-se do algoritmo de suporte para a assinatura, que é usado para verificar a propriedade durante uma transação (ao fazer uma transferência) de bitcoins.

Elétron. É uma partícula subatômica com carga elétrica negativa. Em física, partícula subatômica é a designação genérica daquelas cujas dimensões são muito menores que as de um átomo. Átomo é uma unidade básica de matéria que consiste num núcleo central de carga elétrica positiva envolto por uma nuvem de eletrons de carga negativa. O núcleo atômico é composto por protons e neutrons. Os eletrons podem aparecer no estado livre (sem estar ligado a qualquer átomo) ou ligado ao núcleo de um átomo. Os eletrons de um átomo estão ligados ao núcleo por força eletromagnética. Os átomos são objetos minúsculos cujo diâmetro é de apenas algumas décimas de nanômetros. Um nanômetro, milimícron ou milimicro é a subunidade do metro, correspondente a 1×10^{-9} metro; ou seja, um milionésimo de milímetro ou um bilionésimo do metro. A sua observação só é possível com recurso a instrumentos apropriados, como o microscópio de corrente de tunelamento. Os elétrons desempenham um papel essencial em muitos fenômenos físicos, tais como a eletricidade, o magnetismo e a condutividade térmica. Por ter carga elétrica, um elétron gera um campo elétrico em sua vizinhança. Quando se move em relação a um observador gera também um campo magnético. A antipartícula do elétron é denominada pósitron (também denominada antielétron); tem muitas características idênticas às do elétron, mas sua carga elétrica é positiva. Quando um elétron

colide com um pósitron, ambas as partículas são totalmente aniquiladas, produzindo fótons de raios gama. Nos condutores elétricos e em materiais semicondutores, a corrente elétrica flui através dos elétrons dos átomos que trafegam individualmente de um átomo a outro na direção do polo negativo ao polo positivo.

***Elliptic Curve Arithmetic* (aritmética da curva elíptica)**. Um conjunto de operações matemáticas definidas em um grupo de pontos em uma curva elíptica 2D. O protocolo Bitcoin a especifica no documento secp256k1 (https://en.bitcoin.it/wiki/Secp256k1).

***Emergency BTC Address* (endereço Bitcoin de emergência)**. Um endereço usado para enviar todos os fundos no caso de um desligamento do mercado. Este seria idealmente um endereço de armazenamento com nenhuma informação que possa ser utilizada para ligar o proprietário a sua identidade. Este endereço só seria verificado após a queda de um mercado, a fim de recuperar os fundos pendentes.

Emoji. Pequena imagem (ou desenho) digital ou ícone usados para expressar uma ideia ou emoção em comunicação eletrônica.

Endereço Bitcoin. Veja Chave pública.

Endereço público. Veja Chave pública.

Endereço IP (*IP adress*). O endereço IP (*Internet Protocol*) se refere ao endereço virtual, expressos em números, conforme definido pelo protocolo de Internet. Trata-se de uma identificação de um dispositivo em uma rede local ou pública. Cada dispositivo conectado na Internet possui um IP único; que é o meio que as máquinas usam para se localizarem e se comunicarem na Internet. Ele é o responsável por endereçar e encaminhar os pacotes (blocos de dados ou informações) que trafegam pela rede mundial de computadores. Os pacotes da Internet são divididos em duas partes: o cabeçalho, que, como um envelope, possui as informações de endereçamento da correspondência, e dados, que é a mensagem a ser transmitida propriamente dita. Cada pacote possui um endereço de destino e um endereço de origem e, a cada roteador (elementos distribuídos por toda a rede e interconectados que atuam como

estações de distribuição de correspondências) no caminho, o endereço de destino é verificado e o pacote reencaminhado para o próximo salto (ponto de distribuição) no caminho. Os protocolos de roteamento mais usados são: RIP (*Route Information Protocol*), OSPF (*Open Shortest Path First*) e BGP (*Border Gateway Protocol*). Para facilitar o uso da Internet utiliza-se de endereço de domínio do site ou página da Internet (exemplo: https://www.google.com.br/) ao invés do IP (exemplo: 216.58.201.163); algumas vezes, ainda, exige-se além do IP, depois de dois pontos (:), o número da porta do serviço desejado. Desse modo, cada endereço de domínio é convertido em um endereço IP pelo DNS - *Domain Name System* (sistema de nomes de domínio). Este processo de conversão é conhecido como resolução de nomes. Veja HTTP, IP, TCP/IP e URL.

Endereço MAC - *Media Access Control* (controle de acesso de mídia). Trata-se de um endereço físico associado à interface de comunicação, que conecta um dispositivo à rede. Por outras palavras, consiste na identificação e localização de um hardware (computador, roteador, smartphone, tablet, impressora, etc.) na rede. O endereço MAC também é conhecido como endereço físico. É formado de 12 algarismos ou dígitos hexadecimais (números e letras de 0 a F) separados de dois em dois por dois pontos (:) ou por um hífen ou sinal de menos (-). Não podem existir dois dispositivos com o mesmo endereço MAC.

Endereço *Vanity*. Um endereço bitcoin personalizado, criado usando o Vanitygen (https://bitcoinvanitygen.com/ e https://github.com/samr7/vanitygen). Por exemplo: 1BRAZUCA31xSxqRt3Pkh5eiuw9Kgh8ixUn3.

Endereço web. Uma sequência de palavras e símbolos que permite aos utilizadores da Internet encontrar cada página da *world wide web* (rede mundial de computadores). Veja Endereço IP.

Engenharia social. Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. É considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de

aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza engenharia social.

E–Procurement. Processo de cotação de preços, compra e venda on-line (pela Internet).

ERP - *Enterprise Resource Planning* (planejamento de recursos empresariais). Software que integra todos os dados e processos referentes a uma empresa em um único sistema de informação, promovendo com isso, a adequada gestão empresarial. Confira *Cloud Computing*.

***Escrow* (garantia)**. Nome dado ao ato de manter fundos em posse de terceiros, a fim de garantir o negócio. Por outras palavras, é a utilização de uma terceira pessoa neutra para assegurar que uma transação de pagamento irá ser feita a um vendedor em conclusão de itens enviados ou entregues para um comprador. Geralmente depois que uma compra é feita, os fundos são retidos e somente são liberados quando o comprador confirmar que o vendedor cumpriu os termos da compra. Geralmente, a terceira pessoa também irá oferecer arbitragem em caso de uma disputa ou desavença entre as duas partes. Saiba mais sobre o *escrow* no corpo do e-book.

Exchange. ***Change*** significa trocar ou mudar; portanto, câmbio. ***Exchange*** significa intercâmbio, trocar e vender. Outros significados de *exchange*: bolsa, letra, centro, permuta, corresponder, intercâmbio, mudar, divisa, correspondência, casa, cotação, descontar, câmbio ou corretor. ***Trade*** é trocar um item por outro (permuta). ***Trader*** é comerciante ou negociante. ***Swap*** é trocar, troca, barganhar, trocar-se, permuta ou barganha. *Swap* tem o sentido muito parecido com *exchange*. O papel da ***exchange*** é trazer compradores e vendedores todos juntos e aumentar a liquidez do Mercado. Por outras palavras, apenas aproxima vendedores e compradores e cobra uma comissão a cada transação. O ***exchanger*** (cambista) é a pessoa ou empresa que, em troca de uma taxa (*fee*), faz intercâmbios de dinheiro, cartões de crédito e uma variedade de outros bens e valores para o tipo de moeda solicitada por um indivíduo ou empresa. Cada casa de câmbio é uma propriedade de negócios independente e possui suas próprias políticas, regimento interno, regras, procedimentos, taxas, métodos e sistemas de financiamento, para atender à procura do mercado. *Exchange* é o local

utilizado para troca (compra e venda) de moedas e outros ativos. Desse modo, as *exchanges* (casas de câmbio) de bitcoins são utilizadas para trocar bitcoin por moedas convencionais (FIAT) ou outras criptomoedas (altcoins) e vice-versa. As *exchanges* (casas de câmbio) ou *trading* (comércio ou negociação) bitcoin são como bolsas de bitcoins que facilitam as transações entre particulares, sem que o comprador saiba quem é o vendedor e vice-versa. Nas *exchanges* é visível a disposição do preço segundo a oferta e a demanda; pois as pessoas colocam as chamadas ordens de compra ou de venda com um preço que elas acham justo. Se tiver alguém disposto a fazer a transação por essa quantia, a ordem é executada e se transferem os valores através da *exchange*. São como o site Mercado Livre intermediando o negócio entre vendedor e comprador. Também a *exchange* mostra o valor médio para comprar ou vender diretamente, executando as ordens automaticamente.

***Exit scam* (golpe final)**. Um termo usado para descrever uma situação em que um administrador de mercado ou um fornecedor quer se aposentar às custas do máximo dinheiro possível apropriado ilicitamente de seus usuários, clientes e compradores. Nesses casos, os vendedores normalmente oferecem algum grande negócio e, abusando da reputação que ganharam até o momento, exigem que os clientes não usem *escrow* ou qualquer outra garantia, recolhendo, assim, o máximo de dinheiro possível sem entregar o produto e/ou fazer o serviço antes de encerrar definitivamente as atividades da empresa (por exemplo, loja virtual) e fugir com a maior quantia possível de dinheiro ou ativos dos clientes. De modo semelhante, administradores do mercado geralmente bloqueiam os fundos dos usuários para impedir que eles os resgatem e, assim, ele possa desligá-los completamente logo depois e desaparecer com os recursos dos clientes.

Exploração de vulnerabilidade (*vulnerability scanning*). Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador.

Extra nonce. Um número colocado no roteiro da coinbase e incrementado por um mineiro cada vez que o *nonce* inteiro de 32 bits transborda. Este não é o caminho necessário para continuar a mineração, quando transborda o *nonce*, pois pode-se mudar a árvore de Merkle de

transações ou alterar uma chave pública usada para a recolha de um bloco de recompensa. Veja, também, o verbete *nonce* do glossário.

A, B, C, D, E, **F**, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

Facilitador de Pagamento (*payment facilitator*). Sistema intermediador de pagamento que permite o vínculo direto de uma loja virtual às mais diversas bandeiras e formas de pagamento.

FAQ - *Frequent Asked Questions* (perguntas frequentes). Espécie de tira-dúvidas com respostas para as perguntas mais comuns.

***Faucet* (torneira)**. Uma *faucet* é um site que distribui pequenas quantidades de bitcoin (satoshis, portanto) ou de outras criptomoedas gratuitamente. A razão para a distribuição pode ser a divulgação de uma nova altcoin; mas na grande maioria das vezes, é apenas um pretexto que os donos destes sites usam para trair visitantes e lucrarem com anúncios em suas páginas. Saiba mais no capítulo: "COMO GANHAR BITCOINS E ALTCOINS?".

FE - Finalize cedo (*end early*). É a liberação precoce (antecipada) de recursos (*release of resources*) antes de o vendedor saber que as condições do contrato foram cumpridas. Esse procedimento é usado para reduzir o risco de o vendedor flutuar os preços (da moeda, do ativo, da comódite ou da mercadoria) e contra o desligamento do mercado (*exit scam*).

Fiat money. Veja Moeda FIAT.

Filtro antispam. Programa que permite separar os e-mails conforme regras pré-definidas. Utilizado tanto para o gerenciamento das caixas postais como para a seleção de e-mails válidos dentre os diversos *spams* recebidos. Veja *Greylisting*.

***Firmware* (ou software embarcado)**. Conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico. O *firmware* é semelhante ao software; só que ao invés de ser

instalado num disco rígido, o *firmware* é instalado diretamente num chip (circuito integrado) de memória de hardware durante a fabricação do mesmo. Veja o verbete Boot.

***Firewall* (parede de fogo)**. Um sistema de segurança cujo principal objetivo é filtrar o acesso à uma rede.

Força bruta (*brute force*). Tipo de ataque que consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios desse usuário.

***Fork* (garfo ou forquilha)**. Apesar de a palavra *fork* significar garfo ou forquilha, o seu significado em informática é de bifurcação (*bifurcation*), cisão (*split*), divisão (*division*), cisma (*schism*), etc. É um procedimento similar à divisão celular que ocorre nos seres vivos, onde uma célula-mãe se divide em duas células-filhas, com toda a informação genética relativa à espécie (procedimento denominado mitose). Desse modo, as células se originam a partir de outras células que se dividem formando duas novas células. Também é similar ao surgimento dos gêmeos univitelinos (monozigóticos), que são formados a partir do mesmo zigoto (célula-ovo), que se divide formando dois embriões. Outro exemplo similar é a estrela-do-mar que se for cortada (dividida) em cinco partes, cada uma delas contendo um braço original e um segmento de seu braço central (como se estivesse fatiando uma pizza), cinco novas estrelas do mar crescerão. Portanto, *fork* se refere à uma ruptura (divisão) que resulta em dois braços do mesmo rio. Essa bifurcação pode ser de um código fonte (umas das formas de criação de uma altcoin) ou de uma *blockchain* (quando duas partes diferentes da rede veem diferentes correntes principais). Num certo sentido, a bifurcação (*fork*) ocorre cada vez que dois blocos da mesma altura são criados ao mesmo tempo. Ambos os blocos sempre têm as diferentes *hashes* (e, portanto, valores diferentes de dificuldade), de modo que quando um nó (*node* ou cliente da rede P2P) vê os dois, ele vai sempre escolher o mais difícil. No entanto, antes de ambos os blocos chegarem a uma maioria de nós, duas partes da rede P2P verá blocos diferentes como pontas da cadeia principal. Quando planejada (alteração do protocolo), avisam e preparam previamente os membros rede de que em determinada

data e horário (*deadline* ou data limite) ocorrerá a bifurcação. Mas a bifurcação também pode ser causada por um bug (falha, erro ou pane) no sistema, rede ou protocolo. Saiba mais no capítulo "*FORK*".

Forquilha. Veja *Fork*.

Fórum. Espaço para mensagens, debates (discussão) e perguntas e respostas sobre um assunto.

Foursquare. Rede social baseada em geolocalização que, assim como outras redes do mesmo tipo, utiliza os dados fornecidos pelo GPS do computador ou dispositivo móvel do usuário para registrar (fazer *check-in*) nos lugares por onde ele passa. Confira em https://pt.foursquare.com/.

***Framework* (estrutura)**. É um conjunto de bibliotecas para conseguir executar uma operação de grande porte. Consiste numa plataforma de desenvolvimento que possui lacunas que devem ser preenchidas pelo programador para funcionar conforme sua vontade. Portanto, é uma aplicação quase completa, mas com pedaços faltando para serem concluídos (terminados ou completados) conforme a necessidade, interesse ou conveniência. Devido à presença de código, um *framework* pode ser estudado a nível de código, executado, e reusado diretamente. Pode ser visto como um esqueleto de uma aplicação. *Framework* também designa um conjunto de arquivos de bibliotecas de códigos binários, de fontes ou de outros recursos para a aplicação que são relacionadas. Exemplos: sistemas de GUI - *Graphical User Interface* (interface gráfica do utilizador ou usuário), de operações web, alguns ORMs (*Object-Relational Mapping* ou mapeamento objeto-relacional), um conjunto de bibliotecas padrão de uma linguagem de programação, implementação de um padrão MVC - *Model-view-controller* (modelo-visão-controlador), etc. Confira o verbete Biblioteca.

Freenet. Uma plataforma *peer-to-peer* para comunicação. Confira em https://freenetproject.org/.

Freeware. Software distribuído gratuitamente e que permite ilimitado número de cópias, além de não exigir nenhum tipo de registro. Por outras

palavras, sua utilização não implica no pagamento de licenças de uso ou *royalties*. Não confundir "freeware" com "free software"; no primeiro o significado é de gratuito, e no segundo é de livre. O **software livre** pode ser vendido ou distribuído gratuitamente, modificado e redistribuído; mas em todos os casos existem leis que o protegem para impedir que alguém tome controle sobre ele. Nomeadamente, se for vendido por uma companhia, esta está obrigada a distribuir também o código fonte que permite a qualquer outro modificá-lo, copiar e até revender. Um programa livre não deve ser confundido com programas do **domínio público**, pois no caso do domínio público alguém pode fazer com que as fontes desapareçam e continuar a distribuir binários sendo o único em poder das fontes; isso seria ilegal no caso do Linux e a maior parte dos programas distribuídos com ele são.

Frequência (*frequency*). A frequência, na física, é uma grandeza que indica o número de ocorrências de um evento (ciclos, voltas, oscilações, vibrações, rotações, batimentos cardíacos, etc.) em um determinado intervalo de tempo. É um termo utilizado para indicar a repetição de qualquer fenômeno (evento periódico) em um período de tempo. Enfim, frequência é uma grandeza física associada a movimentos de característica ondulatória que indica o número de execuções por unidade de tempo. O tempo decorrido nessa ocorrência se chama período; ou seja, o tempo necessário para executar uma oscilação se chama período. A frequência é o inverso do período. Para processos cíclicos, tais como a rotação, oscilações ou ondas, a frequência é definida como um número de ciclos por unidade de tempo (normalmente no período de um segundo). A unidade de medida da frequência é o hertz (Hz). Uma revolução ou execução por segundo corresponde assim a 1 Hertz. Desse modo, 1 Hz corresponde a um evento que ocorre uma vez por segundo. Assim, 1 Hz significa 1 ciclo por segundo, 100 Hz significa 100 ciclos por segundo e assim por diante. Na física, onda é um pulso energético que se propaga através do espaço ou através de algum meio. É uma perturbação oscilante de alguma grandeza física no espaço e periódica no tempo. A onda é semelhante à reação de se jogar uma pedra na superfície de um lago; ou seja, surgem ondas circulares em volta do local onde caiu a pedra, as quais se propagam se afastando-se do ponto de origem e sofre um amortecimento gradativo à medida que se afasta do ponto inicial pela resistência encontrada pela água. Também pode-se fazer uma analogia com o enfileiramento de peças de dominó de forma vertical (em pé),

uniformemente espaçadas umas das outras, e ao se empurrar a primeira pedra da sequência, ocorre um efeito em cadeia no qual cada peça empurra a seguinte, derrubando toda a série. Portanto, a energia aplicada à primeira peça de dominó se desloca em todas as pedras enfileiradas até a última pedra do dominó. De igual modo, no exemplo da onda no lago, não são as partículas de água que se deslocam sobre a superfície do lago, mas sim a energia. A água e as pedras do dominó exemplificam, assim, os meios onde a energia se propaga. Diante disso podemos dizer que uma onda é a perturbação do meio caracterizada pelo transporte de energia e quantidade de movimento, sem o transporte de matéria. A distância percorrida pela onda durante o período se chama comprimento de onda. A diferença da parte mais baixa até a parte mais alta da onda é chamada de amplitude da onda. A parte mais alta da onda se chama crista ou pico da onda. A distância entre duas cristas ou picos consecutivos é o comprimento da onda. O trajeto percorrido para realizar um comprimento de uma onda se chama ciclo. O número de ciclos completados na unidade do tempo de um segundo chama-se frequência. O som viaja numa onda que nada mais é que oscilação de pressão. Os humanos percebem a frequência de vibração das ondas sonoras como um tom. Cada nota musical corresponde a uma frequência em particular, que pode ser medida em hertz. A transmissão de rádio é feita por meio de ondas. A luz também é radiação eletromagnética, tendo frequências no campo das dezenas aos milhares de tera-hertz (infravermelha e ultravioleta nos respectivos extremos). A radiação eletromagnética é costumeiramente descrita pela sua frequência, o número de oscilações dos campos elétricos e magnéticos perpendiculares por segundo expressa em hertz. Assim, radiações eletromagnéticas com frequências de poucos tera-hertz (entre as frequências mais altas de rádio e as mais baixas de luz infravermelha) muitas vezes é chamada de radiação tera-hertz. Em computação, a maioria das unidades de processamento central (CPU) são classificadas em termos de número de *clock* (relógio), normalmente medida em mega-hertz ou giga-hertz. Esse número refere-se à frequência do sinal temporizador mestre. Esse sinal é uma voltagem elétrica que muda de baixa para alta e diminui de novo em intervalos regulares.

FTP - *File Transfer Protocol* (protocolo de transferência de arquivos). O FTP pode ser utilizado para copiar arquivos da rede para o computador do usuário e vice-versa. É normalmente através do FTP que o desenvolvedor

de um site efetua o *upload* (envio) dos arquivos para o servidor (hospedeiro) do site. O FTP é utilizado para copiar e colar (teclas Ctrl + C e Ctrl + V) arquivos de forma simples, tal como se o usuário estivesse movimentando-os dentro das pastas do seu próprio computador (por exemplo, como se estivesse usando o Windows Explorer).

FUD. Medo, Incerteza e Dúvida.

Função de resumo (*summary function*). Método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado *hash*.

Função *hash* (*hash function*). Veja *Hash*.

A, B, C, D, E, F, **G**, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

Galaxy Deep Web Social Network – (http://hbjw7wjeoltskhol.onion/). É uma rede social muito ativa na *Deep Web*.

Gamification. Tornar o aplicativo, solução, software, website, etc. em algo mais divertido, como a experiência de um jogo eletrônico.

Garfo. Veja *Fork*.

Gasto duplo. Ver *Double Spend*.

***Gateway* (caminho de entrada)**. Sistema que faz a ponte entre dois sistemas incompatíveis.

***Gateway* de Pagamento**. Sistema responsável pela comunicação entre uma loja virtual e as operadoras de pagamento (contratadas à parte através de uma credenciadora ou diretamente com bancos) responsáveis pela plataforma de recebimento de valores referentes às vendas.

GCHQ - *Government Communications Headquarters*. Sede do departamento de comunicações governamentais do governo britânico;

equivalente à NSA - National Security Agency (Agência de Segurança Nacional) dos Estados Unidos (https://www.nsa.gov/).

Geek. Gíria inglesa que se refere a pessoas peculiares ou excêntricas, fãs de tecnologia, eletrônica, jogos eletrônicos ou de tabuleiro, histórias em quadrinhos, livros, filmes, animes e séries.

Genesis block. Ver Bloco gênesis.

Gigahashes/sec (Gh/s) - O número máximo de *hashing* possível por segundo, medido em milhares de milhões de *hashes* (milhares de Megahashes).

GMT - *Greenwich Mean Time* (Tempo Médio de Greenwich). Veja UTC - *Universal Time Coordinated* (tempo universal coordenado).

GnuPG (https://www.gnupg.org/). Conjunto de programas gratuito e de código aberto, que implementa criptografia de chave simétrica, de chaves assimétricas e assinatura digital.

Google Analytics (https://analytics.google.com/). Ferramenta gratuita que oferece análise e estatísticas avançadas para acompanhamento de visitas e conversões de uma loja virtual.

GPU (*Graphical Processing Unit*). Em português, unidade de processamento gráfico. É um chip projetado especificamente para processar cálculos matemáticos complexos, necessário para rodar jogos e softwares que utilizam muitos recursos gráficos. A GPU foi muito utilizada na mineração de bitcoin, devido ao alto poder de processamento de *hashes*; porém perdeu lugar para os ASICs. Ainda é muito utilizada para minerar altcoins com criptografia diferente de SHA-256 e Scrypt. Veja Mineração.

Grams (https://grams7enufi7jmdl.onion.to/). Motor de busca sobre *Black market* (mercado negro) na *Deep Web*. Veja Harry71.

***Greylisting* (listagem cinza)**. Método de filtragem de spams, implantado diretamente no servidor de e-mails, que recusa temporariamente um e-mail e

o recebe somente quando ele é reenviado. Servidores legítimos de e-mails, que se comportam de maneira correta e de acordo com as especificações dos protocolos, sempre reenviam as mensagens. Este método parte do princípio que *spammers* raramente utilizam servidores legítimos e, portanto, não reenviam suas mensagens. Veja Filtro antispam.

A, B, C, D, E, F, G, **H**, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

HackBB. Famoso fórum *hacking* phpBB.

Hacker. Experto ou fanático por computação especializado em desvendar criptografia e códigos de acesso a computadores, sistemas e softwares. Veja Cracker no Glossário e *Hacker* no teor do e-book.

***Halving* (reduzir para metade)**. Refere-se à redução da recompensa aos mineiros na rede Bitcoin a cada 210.000 blocos (aproximadamente a cada 4 anos). Desde o bloco gênesis até o bloco n.º 209.999, em dezembro de 2012, a recompensa era de 50 BTC.

Handheld. Computador de mão, também conhecido como PDA, pocket PC ou palm top. Equipamento portátil desenvolvido para servir como dispositivo de acesso, apesar de alguns modelos possuírem uma grande capacidade de memória e de processamento.

***Hard fork* (fork difícil)**. Significa quando a mudança de protocolo exige esmagadora maioria concordando com ele, sob pena de parte considerável dos usuários continuar seguindo as regras antigas. Veja *Fork*.

Hardware. Conjunto de materiais ou componentes físicos que integram ou constituem um computador ou dispositivo computacional. O hardware é a parte física (o que se pode tocar ou pegar nas mãos) do dispositivo computacional (computador, notebook, tablet, celular, câmera, smart TV, videogame, drone, robô, etc.), sendo integrada por alguns dos seguintes componentes (hardwares): placa-mãe ou de circuitos, chip e/ou processador, memórias, painel (tela, visor, monitor ou display), teclado, antena, sensores, microfone, autofalante, câmera, pilha e/ou bateria, cabos e fios, etc.

Podemos dizer que hardware é o corpo da máquina. Hardware, portanto, é o conjunto de peças, componentes e equipamentos que fazem o computador funcionar. Também se refere aos equipamentos acoplados (periféricos) em produtos que precisam de algum tipo de processamento computacional. Veja software.

Harry71 – Onion Spider Robot (http://skunksworkedp2cg.onion/). Trata-se de uma extensa lista atualizada diariamente, de sites da rede .onion. O proprietário executa um rastreador que verifica se os sites estão em alta, busca o link e título e despeja em seu site. Também contém algumas estatísticas sobre o tempo de atividade e seus hosts.

Hash. Um *hash* (ou escrutínio) é uma sequência de bits geradas por um algoritmo de dispersão (*dispersion algorithm*), em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando 1/2 byte cada. Faça um teste e confira em http://www.fyneworks.com/encryption/SHA-256-Encryption/index.asp.
Hash é a transformação de uma grande quantidade de informações em uma pequena quantidade de informações. É um método para transformar dados de tal forma que o resultado seja (quase) exclusivo e impossível de descobrir a informação original através de procedimento reverso (ou inverso). Por outras palavras, não é possível a partir de um valor de *hash* retornar à informação original. Diante disso se diz que o *hash* é uma função unidirecional porque não pode ser descriptografado de volta. Uma função de *hashing* é uma função criptográfica que gera uma saída de tamanho fixo (geralmente 128 a 256 bits) independentemente do tamanho da entrada. A esta saída se denomina de *hash* da mensagem (ou documento ou do que seja a entrada ou arquivo original). Esse resumo criptográfico (*cryptographic summary*) da mensagem através de algoritmos complexos que reduzem qualquer mensagem sempre a um resumo de mesmo tamanho se dá o nome de *hash*. Um resumo de mensagem (*message digest*) é o resultado obtido com a execução de um texto por meio de um algoritmo *hash*. Representa, assim, uma mensagem ou documento de maior extensão, assemelhando-se a uma impressão digital de um documento maior. Ao comparar o *hash* calculado (a saída da execução do algoritmo) com um valor de *hash* conhecido e esperado, pode-se conferir a integridade dos dados ou a autenticidade da assinatura ou identificação. O *hash* é comumente usado em transferência via

torrents e em cópias de CD (*Compact Disc*), DVD (*Digital Video Disc*) e BD (*Blu-ray Disc*) como forma de confirmar a integridade dos dados. Por exemplo, num arquivo com extensão (término ou final) .ISO (imagem UDF ou imagem replicada de um disco óptico) há o *checksum* para garantir que a cópia coincide com o arquivo original. Portanto, se a sequência de números e letras (resumo *hash*) for igual, significa que o arquivo não foi corrompido e, assim, trata-se de uma cópia fiel (idêntica, exata, precisa ou perfeita) do original. Programas como MD5 and SHA check utility, HashX, File Verifier ++ e HKsFV verificam a integridade de arquivos através de *hash*. O *message digest* não revela o conteúdo de um documento; ou seja, mesmo que a pessoa tenha acesso a ele, não conseguirá visualizar a mensagem original. Os valores retornados por uma função *hash* são chamados valores *hash* (*hash values*), códigos *hash* (*hash codes*), somas *hash* (*hash sums*), somas de verificação (*checksums*) ou simplesmente *hashes*. Saiba mais no capítulo "*HASH*" e em *hash*. Sobre algoritmo de dispersão (*dispersion algorithm*), saiba mais no verbete Árvore de Merkle do Glossário e em Árvore de Merkle no teor do e-book.

Hash256. O SHA - *Secure Hash Algorithm* (algoritmo seguro de *hash*) é uma série de funções *hash* criptográficas. Um *hash* criptográfico é como uma assinatura para um texto ou um arquivo de dados. SHA-256 é um membro das funções de *hash* criptográficas da família SHA-2 projetada pela NSA - *National Security Agency* (Agência de Segurança Nacional) dos Estados Unidos (https://www.nsa.gov/). Uma bitcoin é simplesmente um *hash* SHA-256 em formato hexadecimal. Veja SHA-256.

***Hash rate* (taxa de *hash*)**. Número de *hashes* processados por um minerador em um determinado período de tempo. A taxa de *hash* é a unidade de medida do poder de processamento da rede Bitcoin. A rede Bitcoin deve fazer operações matemáticas intensivas para fins de segurança. Assim, por exemplo, uma taxa de *hash* de 10 Th/s significa que se pode fazer 10 trilhões de cálculos por segundo. A medida de desempenho do hardware de mineração é expressa em *hashes* por segundo ou GH/s (Gigahashs por segundo). Veja Mineração.

Harvesting. Técnica utilizada por *spammers*, que consiste em varrer páginas Web, arquivos de listas de discussão, etc., em busca de endereços de

e-mail.

***Help* (socorro ou ajuda)**. Geralmente significa ajuda, mas em alguns casos, quer dizer socorro. No caso dos softwares se refere à ajuda ao usuário. Quase todos os programas disponibilizam parte do manual de instruções na própria tela. O tópico "ajuda", geralmente traz uma lista, em ordem alfabética, para o usuário procurar a explicação que necessita para resolver seu problema.

***Hidden service* (serviço escondido)**. Um apelido para o nome de domínio ".onion" (veja *Deep Web*) em razão de somente poder ser acessado através da rede Tor e não pode ser rastreado por um governo.

***Hidden wiki* (Wiki escondido)**. Um website na rede anônima (*anonymous network*) que permite a edição aberta de assuntos relacionados com os serviços ocultos e atividade em si.

Hiperlink. Nome que se dá às imagens ou palavras que dão acesso a outros conteúdos em um documento hipertexto. O *hiperlink* pode levar a outra parte do mesmo documento ou a outros documentos. Também é usada a palavra *link* (ligação). É semelhante a um ícone, só que invés de usar uma imagem ou desenho como acionador, utiliza-se de caracteres ou texto sublinhado e na cor azul, tal como a palavra "ícone" acima.

Hipermídia. A definição formal de hipermídia une os conceitos de hipertexto e multimídia ou multimédia (vários meios em simultâneo na transmissão de uma informação). Ou seja, um documento hipermídia (ou hipermédia) contém imagens, sons, textos e vídeos, como qualquer título multimídia. Além disso, usa ligações de hipertextos para permitir que o usuário salte de um trecho para outro do documento ou até mesmo para um documento diferente.

Hipertexto. Documento capaz de incluir em seu conteúdo ligações com outras partes do mesmo documento ou documentos diferentes. As ligações normalmente são indicadas através de uma imagem (ícone) ou texto em uma cor diferente ou sublinhado (link). Ao clicar na ligação, o usuário é levado até o texto ligado.

Hippie. Trata-se de um movimento de contracultura que prega modo de vida comunitário, uma espécie de socialismo libertário, ideais anarquistas de comunidades igualitárias, questões ambientais, estilo de vida nômade e em comunhão com a natureza, nudismo, emancipação sexual, amor livre e sem distinções, não violência, etc. É a turma do slogan "paz e amor" (em inglês, "peace and love"). Abraçam aspectos de religiões orientais como o budismo e o hinduísmo e das religiões das culturas nativas norte-americanas. O incenso e meditação são parte integrante da cultura hippie. Usam drogas como maconha, haxixe, LSD, Psilocibina (alcalóide extraído de um cogumelo), Mescalina (Peiote), Ayahuasca, Amanita Muscaria, Datura Stramonium, Brugmansia suaveolens, Atropa belladonna e Ibogaína visando a "liberação da mente", seguindo as ideias dos beats e de Timothy Leary, um psicólogo proponente dos benefícios terapêuticos e espirituais do LSD. Possuem rejeição à produtos industrializados, consumo de produtos artesanais, principalmente na alimentação a opção por produtos naturais e orgânicos. Normalmente é praticada a agricultura de subsistência e o comércio entre os moradores é realizado através da troca. Costumam usar roupas velhas e naturalmente rasgadas, para ir em oposição ao consumismo, ou então roupas com cores berrantes para fazer apologia à psicodelia, além de diversos outros estilos incomuns.

***Home page* (página inicial)**. Página de entrada de um Web site ou a página principal de uma determinada seção. Por analogia se refere à tela inicial de um aplicativo e, até mesmo, de um dispositivo computacional; só que neste último caso, o mais correto é dizer área de trabalho (*desktop*). Também se refere à página inicialmente carregada por um *browser* (navegador da Internet) assim que é aberto. Muitas vezes o termo é abreviado para simplesmente “home” e costuma-se usar o desenho de uma casa como ícone.

***Honeypot* (pote de mel)**. Um serviço oculto ou outra configuração de site pela aplicação da lei na tentativa de atrair as pessoas para armadilhas que participam de atividades ilegais. Outros usos citados incluem ajudar os militares e o governo a proteger os seus segredos e para o FBI - *Federal Bureau of Investigation* (polícia federal dos Estados Unidos) defender grandes empresas.

***Host* (anfitrião ou hospedeiro)**. Computador hospedeiro (*host computer*); também chamado de nó (*node*). Computador ligado permanentemente à rede, que, dentre outras coisas, armazena arquivos e permite o acesso de usuários. Computador principal de um sistema de computadores ou terminais.

HTML - *HyperText Markup Language* (linguagem de marcação de hipertexto). Uma das linguagens utilizadas para desenvolver e produzir websites (páginas da Internet); ou seja, permite a criação de documentos a serem disponibilizados pela Internet. HTML é uma derivação de SGML (*Standard Generalized Mark-up Language*) e, assim, permite a criação de documentos que podem ser lidos em praticamente qualquer tipo de computador e transmitidos pela Internet; inclusive por correio eletrônico (*e-mail*). Utiliza URLs (endereços de documentos na Web). Os documentos HTML podem ter ligações de hipertexto entre si e, também, pode-se criar um documento HTML com ligação para qualquer outro arquivo na Internet. Para escrever documentos HTML não é necessário mais do que um editor de texto simples e conhecimento dos códigos que compõem a linguagem. Os códigos (conhecidos como *tags*) servem para indicar a função de cada elemento da página Web (Internet).

HTTP - *HyperText Transfer Protocol* (protocolo de transferência de hipertexto). Protocolo de comunicação que viabiliza as ligações entre os clientes (usuários) de WWW (Internet) e os Web sites. A sigla HTTP é encontrada nos endereços de páginas Web (as URLs) seguida de dois pontos e duas barras invertidas (://). Ela informa ao servidor de que forma deve ser atendido o pedido do cliente. Veja Endereço IP, IP, TCP/IP e URL no Glossário e HTTP no corpo do e-book.

***Hub* (concentrador ou ponto central)**. Denominação dada ao equipamento para onde convergem dados que saem de uma ou várias fontes e seguem para um ou vários destinos, dependendo do tipo e do comando recebido. Dispositivo que interliga os computadores de uma rede local com um número restrito (pequeno) de máquinas. Em redes de maior porte utiliza-se um *switch*; mas um roteador (*router*) é mais eficiente ainda. O uso do hub pode incluir (ser usado em conjunto) um *switch* e um roteador. Trata-se de

dispositivo multi tomadas RJ45 que amplia o sinal da rede (base 10/100). Sua forma de trabalho é a mais simples se comparado ao switch e ao roteador. Através de uma solicitação (dados vindos de um computador) destinada a um computador da rede, a mensagem será enviada para a totalidade dos computadores da rede. Isso reduz consideravelmente o tráfego e provoca problemas de escuta da rede. Além disso, no momento que ocorre essa mensagem com cópia para todos, nenhum outro computador consegue enviar sinal. A liberação somente ocorre após o sinal anterior ter sido completamente distribuído.

Hushmail (https://www.hushmail.com/). Um provedor de e-mail (correio eletrônico) que se concentra na privacidade e criptografia. Ele afirma ser seguro, na medida em que nem mesmo os funcionários da empresa pode ler o conteúdo dos e-mails dos usuários.

Hybrid Cloud Computing (computação em nuvem híbrida). Quando se desconfia que o serviço de nuvem (*cloud*) não é totalmente seguro e se coloca parte de um serviço de processamento para rodar dentro da infraestrutura da própria empresa.

A, B, C, D, E, F, G, H, **I**, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

I2P - *Invisible Internet Project* (*projeto internet invisível*). Originalmente concebido como uma maneira de ser capaz de usar o chat IRC (*Internet Relay Chat*) anonimamente, tornou-se uma das redes anônimas mais populares. Embora seja semelhante ao Tor, as principais diferenças incluem o fato de que a I2P se concentra em obter acesso a sites dentro da rede, e não para a Internet em geral. Detalhes podem ser encontrados em https://geti2p.net/pt-br/.

Ícone (*icon*). Símbolo gráfico (pequena figura) que é uma maneira rápida de executar uma ação (exemplo, clique no ícone da impressora para imprimir). Trata-se de uma representação gráfica de um botão ou tecla virtual para acionar algum software, executar algum comando (tarefa) ou abrir algum documento. Ver Atalho e *Hiperlink*.

IDS - *Intrusion Detection System* (sistema de detecção de intrusão). Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

IEEE - *Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Elétricos e Eletrônicos). Uma organização composta por engenheiros, cientistas e estudantes, que desenvolvem padrões para a indústria de computadores e eletroeletrônicos (https://www.ieee.org/).

IMAP - *Internet Message Access Protocol* (protocolo de acesso a mensagem da internet). Similar ao POP (*Post Office Protocol*), trata-se de um protocolo para o recebimento de mensagens de e-mail (correio eletrônico); só que sincroniza a caixa de e-mails com o conteúdo do servidor.

***In memory analytics* (na análise de memória)**. Rodar a análise de dados diretamente na memória RAM do equipamento, ao invés de acessar o disco rígido, que é mais lento.

***In memory database management system* (no sistema de gerenciamento de banco de dados de memória)**. Inserir enorme quantidade de dados no servidor de memória RAM para rodar bem mais rápido.

***Input* (entrada)**. Normalmente significa entrada ou inserção de dados. Também se refere ao endereço de origem de uma transação bitcoin. Uma única transação pode ter múltiplos endereços de origem. Uma transação Bitcoin faz referência à uma saída (*output*) de transação anterior como uma nova entrada de transação e dedica todos os valores Bitcoin de entrada à uma nova saída. Uma entrada é uma referência à uma saída a partir de uma operação anterior. Muitas entradas são frequentemente listadas em uma transação. Todos os valores de entrada da nova transação são adicionados e o total (menos a taxa de transação) são completamente usados pelas saídas da nova transação. Uma entrada em uma transação Bitcoin contém quatro campos: um script de assinatura, um número sequencial, a referência à saída anterior e o roteiro de assinatura que permite gastar os referidos créditos. A entrada é autorizada se scriptPubKey retorna *true* (verdadeiro ou positivo). A entrada, basicamente, é a parte de uma transação que indica de onde veio

o pagamento; normalmente será um endereço bitcoin. Veja *Output* e *Transação*.

Interceptação de tráfego (*traffic interception*). Técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

Internauta (*Internet user*). Pessoa que navega (acessa) na Internet.

Internet. O significado da palavra Internet é rede mundial de computadores. Trata-se de uma rede global de computadores, com protocolos padronizados (TCP/IP, HTTP, URL, HTML, FTP, POP, SMTP, etc.), dispersos por todo o planeta e trocando dados e mensagens. Veja WWW.

***Internet Banking* (ou *e-banking*)**. É o banco online. Através dele se faz operações (consulta saldo e faz pagamentos, transferências, investimentos, etc.) sem ter de ir até uma agência bancária. Veja Banco Digital e *Home Banking*.

Intranet. Uma rede fechada (privada ou particular), que funciona interligando os computadores de uma mesma entidade, instituição, organização, empresa ou corporação, no mesmo prédio ou em vários prédios em diversos países. A Intranet, diferentemente da Internet, somente pode ser acessada por quem faça parte da organização.

Invasão (*invasion*). Ataque bem-sucedido que resulte no acesso, manipulação ou destruição de informações em um computador por um terceiro não autorizado. Veja Ataque.

Invasor (*invader*). Pessoa responsável pela realização de uma invasão.

IoT - *Internet of things* (Internet das coisas). Qualquer coisa conectada à Internet gerando e recebendo dados e informações que resultam num *big data*.

IP - *Internet Protocol* (protocolo da internet). É o protocolo responsável pelo roteamento de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP, desenvolvida e usada na Internet. O roteamento de pacotes permite dividir a informação em blocos que podem ser enviados separadamente e depois reagrupados no destino. Veja Endereço IP, HTTP, TCP/IP e URL.

IP Spoofing* ou *server spoofing. Técnica utilizada por crackers para mascarar o IP do computador. Utilizando endereços falsos, os crackers podem atacar servidores ou computadores domésticos sem serem rastreados, pois o endereço que é enviado para os destinatários é falso.

IRC - *Internet Relay Chat*. Um sistema de comunicação em tempo real que permite a fácil transferência de mensagens na forma de texto. Destina-se a discussão de grupo em sessões chamados canais.

ISDN - *Integrated Services Digital Network*. No Brasil, a sigla usada é RDSI - Rede Digital de Serviços Integrados. Uma rede digital capaz de fornecer serviços de voz, dados, imagens, etc.

ISO - *International Organization for Standardization* (Organização Internacional para Padronização). O formato (extensão, término ou final) ".ISO" de arquivo que contém todas as informações sobre o conteúdo de um CD (*Compact Disc*), DVD (*Digital Video Disc*) ou BD (*Blu-ray Disc*) para fins de gravação de uma cópia autêntica. Desse modo, basta abrir referido arquivo através de um programa gravador de CD, DVD ou BD para que os dados sejam gravados na respectiva mídia física e, assim, se uma cópia exata do CD, DVD ou BD original. Por outras palavras, o arquivo .ISO é uma cópia virtual do teor de um CD, DVD ou BD para que não seja preciso ter o CD, DVD ou BD físico original para poder ser feita uma cópia física

idêntica. Apesar do nome imagem, referido arquivo não se trata de uma arte gráfica (figura, foto, desenho, etc.) e, portanto, não pode ser aberto em programas de visualização de imagens (artes gráficas).

ISP - ***Internet Service Provider*** **(provedor de Internet)**. Fornecedor de serviços de Internet; a empresa que fornece o acesso à Internet.

A, B, C, D, E, F, G, H, I, **J**, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

Java. Linguagem de programação desenvolvida pela Sun Microsystems (adquirida pela Oracle Corporation em 2009). Por sua facilidade de uso e a possibilidade de rodar, sem necessidade de mudanças em outros sistemas operacionais, a linguagem Java tornou-se uma das preferidas pelos programadores da web. A palavra java, é uma gíria para café, daí a xicarazinha que aparece no logotipo.

JavaScript. É uma linguagem de programação baseada em *scripts* (instruções escritas para serem seguidas) e padronizada pela ECMA - *European Computer Manufacturers Association* (https://www.ecma-international.org/); uma associação especializada na padronização de sistemas de informação. **Não se deve confundir JavaScript com Java**; linguagem de programação desenvolvida pela Sun Microsystems (https://www.java.com/pt_BR/). JavaScript e Java são completamente diferentes, possuem propósitos diversos e requerem *plug-ins* diferentes. O JavaScript tem como característica rodar programas localmente (do lado do cliente ou usuário). O JavaScript fornece às páginas web a possibilidade de programação, transformação e processamento de dados enviados e recebidos, interagindo com a marcação e exibição de conteúdo da linguagem HTML - *HyperText Markup Language* (Linguagem de Marcação de Hipertexto) e com a estilização desse conteúdo proporcionada pelo CSS (*Cascading Style Sheets*) nessas páginas. A mais famosa biblioteca JavaScript é a jQuery (https://jquery.com/); já o Node.js (https://nodejs.org/) é um conjunto de ferramentas *opensource* que permite criar servidores web para execução remota de aplicações JavaScript. Serviços importantes como PayPal, LinkedIn e Groupon usam Node.js para funcionar. Javascript não é propriamente uma linguagem de programação; é uma linguagem de

"scripting" que não é compilada e executada. Java é uma linguagem de programação OOP (*Object-oriented programming*), ao passo que Java Script é uma linguagem de scripts OOP (programação orientada a objetos). Java cria aplicações executadas em uma máquina virtual ou em um *browser*, ao passo que o código JavaScript é executado apenas em um *browser*. O JavaScript não cria *applets* (pequeno software que executa uma atividade específica dentro de outro maior) ou aplicações independentes. Na sua forma mais comum, o JavaScript fica embutido nos documentos HTML e pode fornecer níveis de interatividade para páginas Web que não são acessíveis com um HTML simples. A execução do Javascript é feita pelo navegador (browser) e dele depende. Já os programas construídos com a linguagem Java são independentes de plataforma, compilados na "máquina virtual Java". A relação entre a máquina virtual Java (JVM) e a máquina real na qual o programa deve ser executado é feita pelo navegador. Java é uma linguagem orientada a objetos. O código Java precisa ser compilado, ao passo que os códigos JavaScript estão totalmente em texto. Embora seja possível escrever programas procedurais em Java, a linguagem é concebida para a criação de objetos. Javascript, por sua vez, não é orientada a objetos, e não permite a definição de classes como é feita em Java, com herança e implementação de interfaces. Entretanto, ainda assim é possível escrever programas orientados a objeto em Javascript, através da definição de funções. Em Java, na sintaxe da linguagem, as operações e funções estão definidas para tipos específicos de variáveis, e a tentativa de aplicar uma operação ou função numa variável de tipo diferente ao definido resulta em erro, enquanto em Javascript tudo é permitido. Em Java, toda variável tem de ser declarada e definida, especificando-se seu tipo, antes de ser usada. Em Javascript não existem tipos de variáveis; qualquer variável pode receber qualquer tipo de valor, numérico, booleano ou mesmo cadeia de caracteres. Não é necessário definir a existência das variáveis antes de usá-las, como em Java, desde que a primeira coisa que se faça com elas seja atribuir-lhes um valor. Uma variável pode ter num momento um valor numérico e depois ser uma cadeia de caracteres; desde que a operação faça algum sentido para o compilador, é possível aplicar operações ou funções a variáveis com tipos diferentes daqueles para os quais a operação faz sentido matemático. Escrever e executar programas em Javascript é muito mais simples e fácil do que em Java. Em Java é necessário conhecer as classes que compõem as interfaces gráficas que permitem a interação e o controle do

programa pelo usuário, as chamadas GUI (*Graphical User Interface*) e suas propriedades e métodos, de forma a integrar recursos de interação ao programa. Em Java é possível escrever dois tipos de programa, o aplicativo (*application*) e o *applet*, e para escrever qualquer um dos tipos é necessário conhecer muitos detalhes da estrutura geral da linguagem. É necessário ter instalado no computador um ambiente para o desenvolvimento de programa em Java, o chamado JDK (*Java Development Kit*), que compila e executa os programas. Javascript, por sua vez, usa os objetos criados com HTML, que são definidos de forma muito mais simples, e podem também ser manipulados pelo código Javascript de forma muito mais simples. Para escrever e testar programas em Javascript só são necessários um editor de texto do tipo de um bloco de notas e um navegador ("browser"). Embora esse ambiente ofereça condições muito fracas para a depuração de programas, permite que se execute programas simples de forma muito conveniente.

A, B, C, D, E, F, G, H, I, J, K, **K**, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

Kernel (núcleo ou cerne). É a parte do sistema operativo que gere o processador. Trata-se do componente central do sistema operativo da maioria dos computadores; ele serve de ponte (elo de ligação) entre aplicativos (software ou parte lógica) e o processamento real de dados feito a nível de hardware (parte física). Em linhas gerais, o kernel é o sistema nervoso central do computador (centro de módulo de um sistema operacional); pois ele é a ligação entre o processamento dos dados e os programas; bem como é responsável por fornecer todos os serviços essenciais requeridos por todas as partes do sistema operacional e pelos programas e aplicativos. Cada sistema operacional tem um kernel; por exemplo, o kernel do Linux é usado em vários sistemas operacionais, incluindo Linux, FreeBSD, Android e outros. Em outras palavras, o principal objetivo do kernel é gerenciar o computador com seus recursos, intermediar a comunicação entre componentes de hardware e software e permitir que os aplicativos sejam executados e façam uso dos recursos que a máquina tem. O kernel é a parte do sistema operativo que é carregado em primeiro lugar e mantém-se na memória principal. Assim que se liga o computador, o kernel é acionado e começa a detectar todos os hardwares que ele possui (monitor,

placa de vídeo, etc.) e o que eles precisam para funcionar. Depois que o sistema operacional é carregado, o kernel assume outras funções: gerenciar os processos, os arquivos, a memória e os dispositivos periféricos, fazendo com que ele seja o organizador de tudo o que acontece na máquina. Os serviços de um kernel são solicitados por outras partes do sistema operacional ou aplicativo através de um conjunto especifico de interfaces de programas, às vezes conhecidos como chamadas do sistema. Normalmente, um kernel (ou qualquer centro comparável de um sistema operacional) inclui um manipulador de interrupções que lida com todas as solicitações ou operações de entrada e saída concluídas que competem pelos serviços do kernel. Um gerenciador determina quais programas compartilham o tempo de processamento do kernel e em que ordem. Já um supervisor é que realmente dá uso do computador para cada processo quando ele é agendado. Um kernel também pode incluir um administrador dos espaços de endereço do sistema operacional na memória ou no armazenamento, compartilhando estes entre todos os componentes e outros usuários dos serviços do kernel. O kernel tem, ainda, a responsabilidade de decidir, a qualquer momento, qual dos programas que estão sendo executados no momento devem ser alocados para o processador (ou processadores). Cada vez que se conecta dispositivos ao computador (um pendrive, por exemplo), o kernel age na gestão da memória e na comunicação dos arquivos presentes nele com os programas e o hardware. Por permanecer na memória, o kernel é geralmente carregado em uma área protegida de memória para impedir que ele seja substituído por programas ou outras partes do sistema operacional. A arquitetura do kernel de um sistema pode ser monolítico, híbrido ou micronúcleo. No monolítico os controladores de dispositivos e as extensões de núcleo são executadas no espaço de núcleo, com acesso completo ao hardware. No híbrido é essencialmente um micronúcleo e tem um código (não essencial) no espaço do núcleo para que as operações executadas sejam mais rápidas. Já no micronúcleo alguns processos são executados no núcleo e os restantes são executados no espaço do usuário. O kernel não deve ser confundido com o sistema básico de entrada e saída (Sistema Basic Input / Output), mais conhecido por BIOS. O BIOS é o programa que inicia o sistema operacional após o computador ser ligado. Também gerencia o fluxo de dados entre o sistema operacional e os dispositivos (hardwares) conectados ao computador. Quando o BIOS inicializa (inicia) o computador, ele primeiro determina se todos os dispositivos (hardwares) estão no lugar e, em seguida,

ele carrega o sistema operacional (ou partes importantes dele) na memória de acesso aleatório do computador (RAM) do disco rígido. Com o BIOS, o sistema operacional e suas aplicações são liberadas de ter que entender e conferir detalhes exatos (como os endereços de hardware) sobre os dispositivos de entrada e saída conectados. Embora o BIOS seja teoricamente sempre o intermediário entre o microprocessador e as informações de controle do dispositivo de entrada e saída e o fluxo de dados, em alguns casos, o BIOS pode providenciar que os dados fluam diretamente para a memória de dispositivos (como placas de vídeo) que exigem fluxo de dados mais rápido e eficaz.

Key. Ver Chave.

Keylogger (registrador de chaves). Tipo específico de *spyware*. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente a ativação do keylogger é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de *Internet Banking*.

***Key pool* (chave de piscina)**. Algumas aplicações de carteira que criam aleatoriamente novas chaves privadas, formando um conjunto de chaves pré-geradas que ainda não foram utilizadas. Quando uma nova chave é necessária para a mudança de endereço ou um novo pedido de pagamento, a aplicação fornece a chave mais antiga da piscina e substitui esta por uma nova, mantendo-se, assim, a quantidade de chaves no estoque (Bitcoin Core mantém 100 chaves por padrão). Objetiva garantir que as chaves usadas recentemente sejam salvas em *backup* (armazenamento externo). Sem uma piscina de chave poder-se-ia criar uma nova chave, receber um pagamento no respetivo endereço público e, em seguida, poder ter o disco rígido do computador pifado antes de poder ter tido a chance de fazer um *backup* desta chave. Uma piscina de chave garante que esta chave já conste de um *backup* de vários dias antes de ser usada. Carteiras determinísticas não usam piscina de chave, porque elas precisam para fazer *backup* de uma única chave secreta.

***Keyword* (palavra-chave)**. Palavra-chave para utilização em um sistema de busca.

***Kilohashes/sec* (kH/s)**. Número de tentativas possíveis de resolver um *hash* em um dado segundo, medido em milhares de *hashes*.

KYC - *Know Your Customer* (conheça seu cliente). São políticas que instituições governamentais impõe às empresas para assegurar quem conhecem com quem estão fazendo negócios; ou seja, possuem dados e documentos de seus clientes.

A, B, C, D, E, F, G, H, I, J, K, **L**, M, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

Lammer* ou *Script Kiddy. Termo utilizado por *hackers* mais experientes para depreciar *crackers* inexperientes que utilizam o trabalho alheio (dos outros) para realizar suas invasões. Além disso, quando conseguem fazer uma invasão, "assinam" em busca de fama, notoriedade, reconhecimento e credibilidade na comunidade *hacker*.

LAN (*Local Area Network*). Sigla para rede local; a rede particular de computadores à qual a máquina do usuário está conectada. Por outras palavras, trata-se da ligação de computadores em rede através de cabos físicos.

Latência (*latency*). Intervalo de tempo entre o início de uma atividade e o momento em que os efeitos desta se tornam aparentes. Latência também é conhecida como PING - *Packet Internet Network Grouper* (Agrupador de Pacotes da Internet) e possui correlação com a largura da banda de conexão à rede, que corresponde ao número total de atividades durante um determinado tempo. Desse modo, é a taxa de bits que uma rede de transferência suporta. As duas medidas são inversamente proporcionais. Sites como https://simet.nic.br/ ajudam a analisar a conexão à Internet. Se a quantidade de atividades ultrapassa o limite da rede, vão ocorrer atrasos na hora de executá-las. Esses atrasos na comunicação do computador são denominados de *lag*. ***Lag*** é um problema de performance ao executar uma tarefa acima de sua capacidade, o que ocasiona lentidão e travamentos consecutivos. Portanto, o erro ou falha *lag* relaciona-se à diferença de tempo entre a ordem de execução e sua execução ou exibição; ou seja, o atraso no

tempo de resposta. O *lag* (atraso) geralmente ocorre com conexões ruins de Internet e em jogos pesados; onde, por exemplo, dá um comando e demora alguns segundos para ser realizado no jogo ou quando a cena aparece para um e ainda não para outro. Outro exemplo é quando está conversando pelo Skype e demora-se alguns segundos para a pessoa receber o áudio do que você falou no microfone.

***Layout* responsivo**. Layout de website que se ajusta automaticamente ao tamanho da tela do dispositivo pelo qual está sendo visualizado (celular, tablet, notebook, PC, etc.).

Liberte. Distribuição Linux similar ao TAILS e Whonix com o objetivo de permitir que todos possam se comunicar com segurança e de forma segura nos ambientes hostis.

***Library* (lib)**. Ver Biblioteca.

Linguagem. Forma pela qual são dadas instruções ao dispositivo computacional. É a língua com que os programadores conversam com as máquinas. Existem várias alternativas que os programadores podem escolher e elas se dividem em duas categorias: as linguagens de alto nível e as linguagens de baixo nível. As de baixo nível são extremamente sofisticadas e dificílimas de aprender porque se aproximam mais da linguagem de máquina; enquanto que as de alto nível são aquelas cuja sintaxe se aproxima mais da nossa linguagem e se distanciam mais da linguagem de máquina. Veja Programa e Software.

Link (ligação). Elo de ligação que redireciona o usuário para algum tópico, documento, arquivo ou site. Veja Atalho e Hiperlink.

Link patrocinado. É um tipo de link apresentado em destaque nos resultados das pesquisas feitas pelo usuário em sites de busca (como, por exemplo, https://www.google.com.br). Quando o usuário clica em um link patrocinado, o site de busca recebe do anunciante um valor previamente combinado. Veja AdWords.

Linux. O Linux é um sistema operacional (tal como o Windows e o OS X); só que, por ter fama de ser difícil para pessoas sem grandes conhecimentos de informática, ele é mais adotado em servidores. Da mesma forma que o Windows da Microsoft e o Mac OS da Apple, o Linux é baseado em Unix. O Linux não foi desenvolvido para fins comerciais e seu software e desenvolvimento são feitos em código aberto; ou seja, é gratuito. O código fonte do Linux está disponível sob a licença GPL (versão 2) para que qualquer pessoa o possa utilizar, estudar, modificar e distribuir livremente de acordo com os termos da licença. O Linux possui distribuições como Ubuntu, Debian, Linux Mint, Kurumi, Fedora, Madriva, etc.

Litecoin (LTC). Altcoin que utiliza Proof of Work e é baseada na função Scrypt. No início, era resistente a ASICs, o que a fez ser conhecida como a prata das criptomoedas, atrás apenas do ouro, o bitcoin. Veja Criptomoeda.

Liquidez (*liquidity*). Capacidade de comprar ou vender um ativo facilmente, mesmo em grandes quantidades.

Lista negra. Veja *Blacklist*.

***Log* (registro)**. Registro de eventos e atividades relevantes (por exemplos, de conexão, de acesso a aplicações, etc.) num sistema computacional, que são utilizados para restabelecer o estado original de um sistema, um administrador conhecer seu comportamento no passado e numa auditoria ou diagnóstico de problemas (conferir histórico de instalações, atualizações, erros, falhas, etc.) em sistemas computacionais. Diante dessas considerações, pode-se definir log como sendo a informação sobre as alterações que foram aplicadas aos itens de dados a partir de transações e que é utilizada para restaurar um banco de dados para o estado de consistência mais recente. É similar ao *cookie*, mas se trata do que acontece com o sistema operacional para fins de investigação sobre eventual problema ou falha.

***Long* (longo)**. Posição comprada. Quando se abre uma posição de compra e lucra com a subida do preço do ativo, moeda, ação, etc.

***Login* (entrar) / *Logon* (iniciar sessão)**. Identificação de um utilizador perante um computador, rede, sistema ou site. Fazer o login ou logon é o ato de dar a identificação de utilizador (usuário) autorizado. Veja *Logout* (sair), *Online* e *Offline*.

***Logout* (sair)**. Ato de sair ou desconectar de um determinado sistema, rede, computador ou site; ou seja, é a finalização do acesso, o fim da sessão ou o encerramento do uso naquele momento. É o oposto de *Login* (entrar) / *Logon* (iniciar sessão).

***Love letter* (carta de amor)**. Uma nota oficial do serviço postal enviado para o destinatário deixando-o saber que seu pacote (entrega física de correios ou transportadora) foi apreendido. Em alguns casos, os vendedores enviam cartas falsas para criar a falsa impressão de um pacote apreendido e enganar o comprador.

A, B, C, D, E, F, G, H, I, J, K, L, **M**, N, O, P, Q, R, S, T, U, V, W, X, Y e Z.

MBR - *Master Boot Record* (registro de arranque [inicialização] principal). Parte do disco rígido que contém a inicialização do sistema operativo. É o registro de inicialização.

MAC address. Veja Endereço MAC.

Macro. Sequência de comandos (pequeno programa) para automatizar procedimentos.

Main chain. Veja Cadeia principal.

***MainNet* (rede principal)**. No Bitcoin, trata-se da sua rede principal e sua *Blockchain*. O termo é usado principalmente em comparação com a *TestNet* (rede de teste).

Malicious code. Ver Código malicioso.

Malvertising - ***Malicious advertsing*** **(anúncios maliciosos)**. Tipo de golpe que consiste em criar anúncios maliciosos, por meio de serviços de publicidade, em diversas páginas Web. Geralmente, o serviço de publicidade é induzido a acreditar que se trata de um anúncio legítimo e, ao aceitá-lo, intermedia a apresentação e faz com que ele seja mostrado em diversas páginas. Também pode ser denominado de *malicious advertising* (publicidade maliciosa)

Marketplaces **(mercados)**. Sites criados para permitir o comércio entre vendedores e compradores. Quando usado no contexto da venda de mercadorias ilegais, costumam fornecer anonimato para o comprador e o vendedor. Um método de *escrow* pode ser usado para garantir o negócio e reduzir o risco de novos fornecedores e vendedores aplicarem golpes. Muitos dos mercados são configurados como “hidden services” (serviços ocultos) operando longe do padrão HTTP / HTTPS. Usando "pontos de encontro" (*rendezvous points*), os usuários de rede Tor podem se conectar aos serviços ocultos, sem um conhecer a identidade de rede do outro (https://www.torproject.org/docs/tor-hidden-service.html.en).

M-commerce - **Mobile Commerce (comércio móvel)**. Loja virtual acessada por algum dispositivo mobile.

MD5. Algoritmo de *hashs* de 128bits, desenvolvido pela RSA Data Security, com o qual é possível gerar um *hash* de 32 caracteres independente do formato, nome ou tamanho do arquivo. Veja *Hash*.

Megadados. Veja *Big data*.

Memória. A capacidade de o computador processar e armazenar dados está relacionada à memória. Memória vem do latim *memor*, pensante. Existem dois tipos principais ou básicos de memória, a ROM e a RAM. A **ROM** - *Read Only Memory* (Memória Somente Para Leitura), ocupa um espaço pequeno e faz o computador funcionar ao ser ligado ou lê os dados contidos numa mídia portátil ou externa (CD-ROM, pendrive, HD externo, etc.). Já a **RAM** - *Random Access Memory* (Memória de Acesso Randômico), é a que trabalha junto com o processador quando o computador está em operação. O processador armazena na memória RAM as

informações com os quais trabalha; portanto, a todo momento, operações de gravação, eliminação e acesso aos dados são realizadas. Quanto mais memória RAM um computador tiver, mais rápido ele será. Randômico, palavra que significa ao acaso, vem do francês *randir*, galopar sem destino. No contexto da Informática, significa que a memória RAM não é uma série de instruções escritas e predeterminadas. A memória RAM permite a gravação e regravação dos dados, já na memória ROM a gravação de dados ocorre uma única vez; não sendo possível apagar ou editar nenhuma informação, mas tão somente acessar a mesma. Quando o computador é desligado, o teor da ROM permanece intacto, mas na memória RAM não fica nada armazenado; pois ela é apenas uma executora de tarefas. Diante disso uma diferenciação é chamar a memória ROM de estável ou permanente e a RAM de volátil ou provisória. Existem variedades de memória ROM: PROM (*Programmable Read-Only Memory*), EPROM (*Erasable Programmable Read-Only Memory*), EEPROM (*Electrically-Erasable Programmable Read-Only Memory*), EAROM (*Electrically-Alterable Programmable Read-Only Memory*), Flash, CD-ROM, DVD-ROM, etc. A memória RAM pode ser do tipo SRAM (*Static Random-Access Memory* - RAM Estática), DRAM (*Dynamic Random-Access Memory* - RAM Dinâmica) e MRAM (*Magnetoresistive Random-Access Memory* - RAM Magneto-resistiva). Veja cache.

Mempool - ***Memory Pool*** **(piscina de memória)**. Termo técnico para uma coleção de transações não confirmadas que ficam armazenadas por um minerador da rede Bitcoin até que expire ou seja incluída na cadeia principal. Por padrão, o Bitcoind descarta as transações não confirmadas após 24 horas. Em resumo, são operações à espera de confirmação (inclusão na *Blockchain*). Depois que uma transação Bitcoin transmitida para a rede é aprovada pelo processo de verificação por todos os nós disponíveis, ela é enviada para a "mempool", onde fica aguardando até que um mineiro a pegue para ser incluída no próximo bloco. Recorda-se, por oportuno, que uma transação só é confirmada quando está permanentemente incluída na *Blockchain*. Portanto, a *mempool* é basicamente a área de espera do nó minerador para todas as transações pendentes. Todos os nós mineradores possuem uma capacidade diferente de memória RAM para armazenar as transações não confirmadas. Desse modo, cada nó minerador possui sua própria versão das transações pendentes; o que explica a variedade de

tamanhos. Apesar de a transação ainda não ter sido incluída na cadeia de blocos, cada nó da rede é informado sobre essa transação. A transação pode ser deixada sem confirmação por um longo período de tempo (não incluída na cadeia de blocos) devido às seguintes razões: a) se tem baixa prioridade (as moedas mais longas possuem mais alta prioridade); b) devido a um montante de transação muito grande; e, c) devido a uma baixa taxa. Enfim, o valor da taxa de transação é fator determinante para a velocidade de inclusão (confirmação). Recorda-se, assim, que a taxa cobrada através da transação vai para o mineiro para incentivá-lo a manter a mineração. Desse modo, um mineiro pode incluir a quantidade de transações que ele prefere; assim, ele pode aumentar automaticamente sua recompensa. Dentro da rede Bitcoin, o usuário pode configurar uma taxa que ele prefere, mas ele precisa ter em conta que, se for muito baixa (pequena), a transação pode ficar sem confirmação por um longo tempo. Veja Mineração e *Key pool*.

Megahashes/sec (MH/s). Número de tentativas possíveis de resolver um *hash* em um dado segundo, medido em milhões de *hashes*.

Mercado Negro. Veja *Black market*.

Merkle. Ver Árvore de Merkle.

Metadados ou metainformação. Consistem em dados sobre outros dados (ou informação sobre informação) para fins de descrição, administração, uso, preservação, etc. Os metadados, portanto, representam informações que caracterizam a informação documentada. Por outras palavras, são informações que acrescem aos dados e que têm como objetivo informar-nos sobre eles para tornar mais fácil a sua organização. Desse modo, são marcos ou pontos de referência que permitem circunscrever a informação sob todas as formas; ou seja, resumos de informações sobre a forma ou conteúdo de uma fonte. Portanto, um item de um metadado pode dizer do que se trata aquele dado, geralmente uma informação inteligível por um computador. Em essência, os metadados respondem o que, quem, quando, onde e como sobre cada faceta da informação, auxiliando a organização na sua publicação e suporte. Existem vários tipos de metadados: descritivos (que servem para identificação e localização), administrativos (criação, direitos, controle de acesso, etc.) e estruturais (que relacionam os objetos). Exemplo de

metadados na gestão de arquivos físicos: localização física, n.º de caixa, etiqueta de pasta, sistema de classificação, etc. Os metadados têm tradicionalmente sido vistos como separados do núcleo duro da informação; ou seja, a que está relacionada com as transações do negócio. Definições e regras de negócio, detalhes de segurança, informação de domínios e *tags* XML são exemplos de metadados. Desse modo, por exemplo, os metadados, permitem catalogar e organizar coleções de fotografias de forma automatizada; além de serem amplamente utilizados por mecanismos de busca (Google, Bing, Yahoo, etc.) para retornar resultados de pesquisa de imagens. Os metadados podem ser utilizados no combate à pirataria e na localização de cópias não autorizadas de dados (imagens, vídeos, documentos, etc.) através da Internet. Inclusive, podem ser adicionados nos metadados o nome do autor e as informações de direitos autorais (*copyright*). Numa câmera digital, por exemplo, normalmente inserem-se automaticamente metadados sobre a foto ou o vídeo informando a marca e modelo da câmera usada. Além disso, podem carregar informações da localização exata (como longitude, latitude e altitude) de onde foram capturadas as imagens. Para tanto, a câmera precisa ter um GPS embutido ou externo. Desse modo, por exemplo, quando essa imagem for aberta no Picasa ou Lightroom, o usuário consegue ver em um mapa onde ela foi tirada. Por fim, ressalta-se que textos diversos podem ser adicionados aos metadados.

microBit (uBTC). Milionésima parte de 1 bitcoin ou 0.000001 BTC.

miliBit (mBTC). Milésima parte de 1 bitcoin ou 0.001 BTC.

Mineração (*mining*). Um processo de encontrar válidos *hashes* de um cabeçalho do bloco através da iteração milhões de variantes de cabeçalhos de bloco (usando *nonce* e *nonce* adicional) a fim de encontrar um *hash* inferior ao alvo (ver também dificuldade). O processo de mineração possui gastos com hardware, Internet e energia elétrica e é remunerada através de taxas de transação e por recompensas por blocos gerados (moedas recém-geradas). Veja, também, o verbete *nonce* do glossário.

Minerar (*mine*). Ato de gerar novos bitcoins resolvendo problemas criptográficos com um computador ou hardware específico. Veja Mineração (*mining*).

Mineiro (*miner*). Uma pessoa, um software e/ou um hardware que executa mineração. Veja Mineração (*mining*).

Mixer. Serviço utilizado para embaralhar *inputs* (entradas) e *outputs* (saídas) de transações, a fim de manter a privacidade e diminuir o nível de rastreamento.

***Mixing* (misturando)**. Um processo de troca de moedas com outras pessoas, a fim de aumentar a privacidade do histórico (sequência) de pagamentos. Às vezes ele é associado com a lavagem de dinheiro. Um banco convencional protege a privacidade do cliente, escondendo as transações de terceiros. No Bitcoin qualquer pessoa pode fazer uma análise estatística do histórico de transações e determinar, por exemplo, quantas bitcoins a conta possui. Embora ainda seja possível implementar as regras do KYC (*Know You Cliente*) a nível de cada comerciante, a mistura permite separar as informações sobre a linha (sequência) histórica e a parte envolvida. A maioria dos casos de uso importante para a mistura são: 1) receber um salário como um único grande pagamento mensal e, em seguida, gastá-lo em pequenas transações; 2) fazer um único pagamento revelando a ligação de muitos pequenos gastos privados. Em ambos os casos as contrapartes podem cumprir com as leis de CSC (*Clients of Special Category*) / AML (*Anti Money Laundering*) e relatar a identidade do pagador e as quantias transferidas, mas nenhum deles precisa saber sobre o outro. Portanto, misturando bitcoins depois de receber e misturá-los novamente antes de fazer um grande pagamento resolve o problema de privacidade.

***mHealth (ou m-health)* - *Mobile Health Monitoring* (monitorização móvel da saúde)**. Prática da medicina e da saúde suportada por dispositivos móveis. O termo é mais comumente usado em referência ao uso de dispositivos de comunicação móveis, como telefone celular, tablet e PDA (*personal digital assistant*), por serviços de saúde e informação. Por exemplo, um sistema de monitoramento móvel para monitorar um ciclista usando sensores sem fio de baixo peso ou peso leve. As informações biométricas e ambientais referentes ao ciclista são capturadas, transmitidas e armazenadas em um banco de dados remoto com pouca interação do usuário. Os usuários remotos têm acesso em tempo real às informações capturadas

através de um aplicativo da Web. Possíveis aplicações para este sistema incluem o monitoramento de um soldado no campo de batalha e o monitoramento de um paciente durante um passeio de ambulância.

***Mobile Marketing* (*marketing móvel*)**. Se refere ao uso de dispositivos móveis para atividades de marketing.

Modem. A palavra modem vem da junção das palavras modulador e desmodulador. Trata-se de um aparelho capaz de converter os dados numéricos do computador em sinais analógicos (procedimento de modulação); ou seja, permite que os dados binários trafeguem através da linha telefônica por modulação de amplitude ou de frequência, assim como a voz quando se utiliza o telefone para falar. Quando esse sinal é recebido por outro modem, este reverte o processo (procedimento de demodulação). Ambos os modens devem trabalhar com os mesmos padrões; que especificam, dentre outras coisas, a velocidade de transmissão (bps, baud, etc.), nível e algoritmo de compressão de dados, protocolo, etc. De modo similar, numa transmissão de **fax**, a luz do aparelho atravessa as partes claras do documento físico, mas não as partes escuras, criando, assim, uma cópia do documento formada por milhares de pontos (píxeis) em preto e branco. Os dados processados indicam em linguagem de computador, quais são as partes atravessadas pela luz e os trechos onde houve o bloqueio da luz. Desse modo, a imagem do documento físico se torna um arquivo digital (dados binários ou um monte de números 0 e 1 representando os pontos pretos e brancos). Então esse arquivo digital segue para o modem, onde ele é transformado num sinal elétrico e é enviado através da linha telefônica. Antes, os números 0 dão origem a sinais com frequência de 800 hertz, enquanto os números 1 viram sinais de 1.300 hertz. Já no aparelho de fax receptor ou destinatário, ocorre o procedimento inverso; ou seja, os sinais elétricos são reconvertidos em dados digitais. Depois, esses dados são enviados para a impressora, que decodifica a mensagem e imprime uma cópia do documento em preto e branco.

Moeda FIAT. Abreviatura de moeda fiduciária. É a moeda baseada na coerção (obrigatória ou de curso forçado) por imperadores, reis e presidentes e não baseada em decisões voluntárias pelo povo. Em síntese, é a moeda sem valor intrínseco que é usada como moeda porque o governo

assim decretou. Trata-se de um título não lastreado em nenhum metal precioso, que possui valor devido à confiança que as pessoas e instituições dão a ele; bem como pelas imposições institucionais e governamentais. Dólar, euro e real são exemplos de moedas fiduciárias. Trata-se da moeda principal ou oficial, com fé púbica e proteção legal, que não depende de outras para existir ou para se basear o seu valor, com a qual se pode comprar qualquer coisa e efetuar qualquer tipo de pagamento monetário.

Moeda fiduciária. Veja Moeda FIAT.

MOOC - *Massive Open Online Course* (curso online aberto e massivo). Um curso, sem custos, em que estudos são disponíveis para toda a Internet e para um grande número de pessoas.

Molly. Expressão que, normalmente, faz referência a drogas ilícitas (ilegais), baratas e impuras (adulterada ou misturadas). O nome foi pensado como derivado da palavra molécula ("molecule"). Também pode se referir à droga MDMA (metilenodioximetanfetamina), mais conhecida por ecstasy. Confira uma lista do que o ecstasy ou molly pode conter em https://www.ecstasydata.org/results.php.

Motor de pesquisa (*search engine*). Um programa, normalmente disponível num site, para realizar pesquisas e encontrar informações na Internet. Exemplo, https://www.google.com.br.

MS-DOS - *MicroSoft Disk Operating System* (sistema operacional de disco MicroSoft). Trata-se do sistema operativo da Microsoft, não gráfico, usado na linha de computadores IBM PC e prévio ao aparecimento do sistema operacional Windows 95. Enquanto o MS-DOS usa uma interface de linha de comando, o Windows usa uma interface gráfica do usuário. O MS-DOS, lançado pela primeira vez em agosto de 1980, usava uma linguagem de programação exclusivamente baseada em texto para permitir que os usuários trabalhassem com o PC ou interagissem com eles. Os comandos foram digitados em computadores em um local de prompt de comando específico na tela do computador usando um teclado padrão. Os comandos tinham que ser precisos. Os usuários tinham que especificar o comando que eles queriam, como eles queriam que ele fosse executado, e que programa ou

sistema no computador que desejavam usar. Isso exigia que os usuários aprendessem regras específicas de linguagem e sintaxe para usar seu computador corretamente. Não confundir MS-DOS com DoS.

MSM - *Principal Media Stream* (principal fluxo de mídia). Grandes agências de notícias projetadas para a massa de consumo comum.

Multi-assinatura de transação (*M-of-N* - *Multi-signature Transaction*). Uma transação que pode ser gasta usando x assinaturas, quando são necessárias y chaves públicas, onde x é menor ou igual a y.

Multimídia. Termo utilizado para definir um documento de computador composto de elementos de várias mídias (áudio, vídeo, ilustrações, texto, etc.) e que contêm interatividade; ou seja, permite a participação (interação) do usuário. Para ser mais preciso, utiliza-se a expressão multimídia interativa.

***Multi Signature Escrow*.** Quando um endereço é assinado pelo comprador e pelo vendedor com suas chaves privadas. O comprador envia fundos (recursos ou valores) para um endereço *escrow* e o vendedor envia o produto. Se ambas as partes estão satisfeitas com o desenrolar (conclusão) do negócio, eles assinam o endereço e liberam os fundos que estão depositados numa conta garantia.

A, B, C, D, E, F, G, H, I, J, K, L, M, **N**, O, P, Q, R, S, T, U, V, W, X, Y e Z.

***Nameless* (sem nome)**. Sem identificações ou sem identidades; ou seja, todos os nomes utilizados são aleatórios.

Navegador (*browser*). Programa utilizado para navegar (acessar) na Web (Internet). Permite utilizar praticamente todos os recursos da rede mundial de computadores; tais como, por exemplos, visitar sites, entrar em redes sociais, acessar o correio eletrônico, realizar transferências (envio e recebimento) de arquivos, participar de grupos de discussão, etc. Veja Browser.

Navegar (*to browse*). Acessar e percorrer as páginas da Internet. O termo se popularizou por influência do *browser* (navegador) Navigator, da Netscape.

Near Field Communication. Veja NFC.

Negação de serviço (*DoS* - *Denial of Service*). Tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Os alvos típicos são os servidores web, onde o ataque procura tornar as páginas web indisponíveis através de sobrecarga (excesso de requisições). Portanto, não se trata de uma invasão do sistema, mas sim de queda (derrubada) do sistema pelo excesso de demanda consistente na criação artificial de um número elevado de solicitações simultâneas. Já um ataque de negação de serviço distribuído (***DDoS*** - *Distributed Denial of Service*) é uma variação do ataque DoS que emprega um número muito grande de computadores invasores para subjugar o alvo com tráfego falsificado. Para alcançar a escala adequada, os DDoS são frequentemente realizados por *botnets* que podem cooptar milhões de máquinas infectadas para participar involuntariamente do ataque, mesmo que elas não sejam o alvo do ataque em si. O uso de filtros e configurações de rede avançadas dispersam as conexões maliciosas, permitindo que o alvo (site, servidor ou sistema) continue atendendo as solicitações legítimas. Desse modo, em caso de ataque DoS, roteadores e switches são configurados para bloquear os endereços de origem ou, se for muito forte, do alvo, para que a rede inteira não seja afetada. Outra técnica de defesa é usar servidores de *proxy* reverso (em que um computador fica de ponte para outro) ou mesmo cache (quando uma informação fica armazenada em um computador para não ter de solicitá-la novamente). No caso da rede Bitcoin, em caso de comportamento suspeitos ou presumíveis de DoS, os respectivos nós ficam com seus IPs bloqueados por 24 horas para evitar DoS. Além disso, alguns ataques teóricos como 51% de ataque pode ser usado para negação de serviço de toda a rede. Não confundir DoS com MS-DOS.

***Net* (rede)**. Termo utilizado como sinônimo para Internet.

***Netiquette* (netiqueta)**. Conjunto de regras de etiqueta que disciplinam o comportamento na Internet. Ensina, por exemplo, como se comportar em

grupos de discussão e como escrever mensagens de forma a preservar a eficiência da rede e ampliar o potencial de comunicação; bem como o que é considerado ser mal-educado ou ofensivo. Por exemplo, escrever em letras maiúsculas é considerado como se a pessoa estivesse gritando.

***Network* (rede)**. Quando dois, ou mais, computadores se interligam eles formam uma rede e assim, são capazes de partilhar recursos. Ligando-se duas ou mais *networks* forma-se uma internet.

***Newbies* (novatos)**. Como são chamados os usuários recém-chegados à rede; principalmente quando cometem erros básicos como enviar uma mensagem pessoal para um grupo de discussão.

***Newsgroups* (grupos de notícias)**. Grupos de notícias ou de discussão. São fóruns de debates, onde os participantes interagem entre si: um faz uma pergunta ou afirmação e os demais comentam (reforçam, confirmam, respondem, replicam, criticam, questionam, indagam, etc.).

NFC - *Near Field Communication* (comunicação de campo próximo). Tecnologia que permite a dois aparelhos próximos realizarem troca de dados (similar ao Bluetooth); e, inclusive, efetuar transferência de dinheiro ou pagamento com cartão de crédito.

Nó (*node*). Dispositivo conectado à rede P2P. No caso do protocolo Bitcoin se trata do cliente (participante) que utiliza um programa de computador para retransmitir as transações para os outros nós (membros da rede), criando, assim, uma rede descentralizada. Em resumo, qualquer computador que se conecta à rede Bitcoin é denominado de nó. Existem nós completos (possuem a cópia integral da *Blockchain*) e os de teor reduzido ou leve, com funcionalidade reduzida. Saiba mais nos capítulos: "*PEER-TO-PEER* (P2P)", "COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?" e "COMO A BITCOIN É FEITA?". Veja Cliente leve.

Nó completo (*full node*). São aqueles que possuem a cópia integral da *Blockchain* e aplicam plenamente todas as regras do protocolo Bitcoin. Os nós completos baixam e verificam todos os blocos e transações da rede; ou seja, rodam os algoritmos de hash e de consenso, bem como realizam os

protocolos de geração de blocos, conferência de cadeia e validação e confirmação das transações. Desse modo, um nó completo não necessita de confiar em qualquer serviço externo para validar as transações. Veja Cliente leve.

Nonce. Significa "número usado uma vez". Trata-se de um número de 32 bits em um cabeçalho do bloco, que é utilizado reiteradamente no processo de prova-de-obra durante a mineração de bitcoins. Cada vez que o *nonce* for alterado, o *hash* do cabeçalho do bloco é recalculado. Confira, ainda, a definição de *nonce* no texto do e-book e o verbete Alvo (*target*) no glossário. Veja Mineração.

Número de confirmação (*confirmation number*). Número de confirmação é uma medida da probabilidade de que a transação poderia ser rejeitada a partir da cadeia principal. Zero confirmações significa que a transação não foi confirmada. Uma confirmação significa que a transação está incluída no último bloco na cadeia principal. Duas confirmações significa que a transação está incluída no bloco anterior ao mais recente. E assim por diante. A probabilidade de a transação ser revertida diminui exponencialmente com mais blocos sendo acrescentados após o bloco onde se encontra. Desse modo, depois que uma transação é enterrada sob 6 (seis) ou mais blocos na *Blockchain* (após cerca de uma hora), a probabilidade de um duplo gasto (*double spend*) desce perto de zero. Veja Reorganização (*reorganization*).

A, B, C, D, E, F, G, H, I, J, K, L, M, N, **O**, P, Q, R, S, T, U, V, W, X, Y e Z.

***Offline* (fora da linha)**. Significa fora do ar ou desconectado. É o oposto (contrário) de *Online*.

Onion. Pseudo (imitação) DNS (*Domain Name System*) utilizado para sites ou serviços na rede The Onion Router, conhecida como Tor. Trata-se, assim, de sites escondidos através da rede Tor. O nome vem do “onion router” usado pelo Tor. A URL da Onion é composta de um *hash* de informação utilizada para identificar o sistema correto.

Onion Browser. Um navegador da Web como o TBB - *Tor Browser Bundle* (pacote do navegador Tor). Trata-se, portanto de um navegador web projetado para trabalhar com a rede Tor e procurar os serviços ocultos e sites normais anonimamente, sem vazamento de informações do usuário.

OnionForum. O Fórum original do Tor.

Onionland. Termo geral para descrever o Tor

OnionNet. Primeira rede de IRC projetada para Onionland.

***Onion Routing* (Onion encaminhamento)**. A técnica de comunicação anônima sobre uma rede de computadores. As mensagens são criptografadas e repetidamente enviava através de vários nós da rede. O processo é comparável ao descascar uma cebola, cada nó remove uma camada de criptografia descobrindo instruções de roteamento para a camada seguinte.

***Online* (conectado)**. Termo utilizado para designar todo o tipo de transação (comunicação ou troca de dados) entre computadores. Online significa estar em linha, ligado ou conectado à rede, sistema ou a outro computador. Oposto de *Offline*.

Opt-in. Regra de envio de mensagens que define que é proibido mandar e-mails comerciais; a menos que exista uma concordância prévia por parte do destinatário. Veja *Opt-out* e *Double Opt-in*.

Opt-out. Regra de envio de mensagens que define que é permitido mandar e-mails comerciais; mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens. Veja *Opt-in*.

OPSEC. Segurança de Operação. O processo de proteção de pequenos pedaços de dados que poderiam ser agrupados para formar um quadro maior ou expor a identidade.

OrBot. Versão móvel do roteador Tor para o Android. Projetado para trabalhar tanto com outro *browser* (navegador) ou ser configurado para funcionar como *proxy* para qualquer sistema que o suporta. Também pode

ser usado em um dispositivo enraizado para fornecer um *proxy* transparente que irá forçar todos os aplicativos a usar o Tor para conectar.

***Order Book* (livro de pedidos)**. Lugar onde ficam todas as ordens passivas tanto de compra quanto de venda esperando serem executadas.

Órfão ou bloco órfão (*orphan* ou *orphaned block*). Um bloco válido que já não é uma parte de uma cadeia principal. Geralmente acontece quando dois ou mais blocos da mesma altura (posição) são produzidas ao mesmo tempo. Quando um deles se torna uma parte da cadeia principal, outros são considerados "órfãos". Órfãos também pode acontecer quando a *Blockchain* é bifurcada devido a um ataque (ver ataque de 51%) ou um *bug*. Em seguida, uma cadeia de vários blocos pode ficar abandonada. Normalmente, uma transação está incluída em todos os blocos da mesma altura, pelo que a sua confirmação não é atrasada e não há gasto duplo. Ver também *fork*.

Organic search. Veja Busca orgânica.

***Output* (saída)**. Uma saída de transação não gasta (*transaction exit does not spend*) ou UTXO, trata-se, em síntese, do valor (montante) informado num pagamento (transação) para ser creditado num endereço Bitcoin. É possível que uma transação tenha múltiplos *outputs*. Além de referido valor, por óbvio, constam as regras para desbloquear referido valor de saída do local de onde se encontra. A saída de transação é feita na forma de um script que cria uma alienação no valor a ser transferido, o qual somente será resgatado se uma solução for apresentada ao script. Desse modo, a saída (*output*) de transação é desbloqueada através da chave privada associada (correlata) ao endereço público do destinatário (favorecido). Explica-se. Os valores creditados entram bloqueados na conta do favorecido e só são desbloqueados por este quanto ele resolver efetuar uma transação (gastar seus créditos). O scriptpubkey é o script de bloqueio que determina as condições que precisam ser atendidas para que os valores de uma transação sejam gastos. A função scriptsig é o script de desbloqueio que resolve as condições colocadas na transação pela scriptpubkey. Assim que a transação é enviada à rede Bitcoin, ela será verificada pelos clientes (nós) conectados à rede Bitcoin. Em termos simples, uma transação informa para a rede Bitcoin que o dono de uma quantidade de bitcoins autorizou a transferência

de alguns destes bitcoins para outro dono. O novo dono agora pode gastar esses bitcoins ao criar uma nova transação que autoriza a transferência para um outro dono, e assim por diante, em uma cadeia de posse de bitcoins. Veja *Input* e *Transação*.

Overclocking. Procedimento de forçar um componente de um computador (processador, memória, *chipset* da placa-mãe, placa de vídeo, etc.) a trabalhar (rodar) numa frequência (velocidade) mais alta do que a especificada pelo fabricante. Apesar de aumentar o desempenho, pode resultar em superaquecimento, instabilidade no sistema e, até mesmo, danificar o *hardware*. Veja *Clock*.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, **P**, Q, R, S, T, U, V, W, X, Y e Z.

P2P (*Peer-to-peer*). *Peer-to-peer* (ponto a ponto ou pessoa para pessoa) se refere a sistemas que funcionam como um coletivo organizado, permitindo que cada indivíduo interaja diretamente com os outros. Cada usuário ou membro é denominado de nó (*node*) e serve de estação transmissora e repetidora. No caso da rede Bitcoin, é construída de tal maneira que cada utilizador está transmitindo as operações de outros utilizadores. Saiba mais nos capítulos: "*PEER-TO-PEER* (P2P)", "COMO SÃO FEITOS OS PAGAMENTOS EM BITCOIN?" e "COMO A BITCOIN É FEITA?".

P2P Escrow. Comumente se refere às transações que usam endereços P2SH, como definido pelo BIP 016. O P2SH (*pay-to-script-hash*) permite pagar para um *script* ou *hash* de roteiro (endereço começando com 3) ao invés de um *hash* de chave pública (endereço começando com 1). A chave pública é fornecida por um vendedor e usada para criar um endereço *escrow* que exige que dois de três assinem para transferir os créditos, que foram previamente enviados pelo comprador. De extrema importância é o *redeemScript* que detalha as informações necessárias para resgatar fundos de enviar para o endereço; que é um *hash* do *redeemScript*. O objetivo deste método é que nenhuma parte tem informação suficiente para tomar fundos destes endereços P2SH. Mesmo que o mercado seja bloqueado ou retirado do ar, os fundos não podem ser apreendidos, e o comprador e vendedor

podem, com o *redeemscript*, finalizar uma operação fora do envolvimento do mercado.

Pacote (*package*). A informação que é transmitida pela Internet é separada em pacotes. Cada pacote contém, além do conteúdo que está sendo transmitido (imagem, mensagem, etc.), endereços do remetente e do destinatário e informações essenciais para que os pacotes de um mesmo arquivo sejam reagrupados no destino. Saiba mais sobre os pacotes de dados na Internet nos verbetes Endereço IP e IP - Internet Protocol.

***Page Views* (visualizações de página)**. Trata-se do número total de vezes que uma página da Internet é visualizada pelos Internautas.

***Password* (senha)**. Código usado para acessar um sistema fechado ou abrir algum arquivo, pasta ou programa restrito (protegido por senha).

Patch. Palavra inglesa que se traduz para remendo. Trata-se de um programa ou ficheiro utilizado para corrigir um erro do sistema ou de um dado programa. Por outras palavras, é a atualização, correção de erros ou versão mais atualizada de um programa. Normalmente são "baixadas" (feito *download*) de forma automática pelo próprio software ou este avisa ao usuário a existência da atualização para ser baixada. Também costuma constar no site do fabricante (do hardware ou do software) para ser baixada.

Pastebin. Um site utilizado para armazenar o texto para um determinado período de tempo. É popular na *deep web*, porque é uma maneira fácil de compartilhar informações anonimamente.

Parallel Construction. Construção paralela (ou em separado) é um processo de aplicação da lei de construir um paralelo. Trata-se de uma base científica para uma investigação criminal, a fim de esconder a forma como a investigação começou.

***Pay-per-click* (PPP)**. Significa pago por clique. É um tipo de publicidade na Internet em que o anunciante paga apenas quando um utilizador clica no link do anúncio para o seu site.

PEPs - *Python Enhancement Proposals* (Propostas de aprimoramento do Python). Python é uma linguagem de programação de alto nível, interpretada, de script, imperativa, orientada a objetos, funcional, de tipagem dinâmica e forte. Veja: RFC e BIP.

Periférico (*peripheral*). É qualquer aparelho que pode ser conectado à CPU - *Central Processing Unit* (unidade central de processamento ou processador) de um computador, como, por exemplos, monitores, impressoras, CD-ROMs externos, etc. A palavra periférico se refere à expressão periferia (afastado do centro). As palavras periférico e periferia se originam da palavra grega *periphereia*, o perímetro de um círculo. Em resumo, pode-se dizer que periféricos são componentes acessórios ou complementares de um computador. Veja hardware.

PGP (*Pretty Good Privacy*) e GPG (*Gnu Privacy Guard*). PGP foi introduzido em 1991, e foi formalizada com a RFC 2440 (https://www.ietf.org/rfc/rfc2440.txt) e RFC 4880 (https://tools.ietf.org/html/rfc4880). Usa uma combinação de criptografia de chave pública e de chave simétrica para garantir que as mensagens possam ser entregues sem um terceiro ter acesso ao conteúdo da mensagem. Além disso, permite uma mensagem ser assinada cuja assinatura ou autoria seja indiscutível. Muitos algoritmos diferentes podem ser usados para a criptografia, mas os métodos mais utilizados são RSA (a sigla advém dos sobrenomes de seus criadores: Rivest, Shamir e Adleman) para a criptografia de chave pública e o AES (*Advanced Encryption Standard*) para a cifra simétrica. É de extrema importância as chaves públicas serem verificadas, a fim de saber que a mensagem está sendo entregue para o destinatário correto ou é do remetente correto.

Phablet. Smartphone (telefone inteligente) que possui uma tela de tamanho intermediário entre um celular típico e um tablet.

Pharming. Tipo específico de *phishing* que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS.

Phishing. Ato de usar técnicas de engenharia social para obter informações pessoais, como nomes de usuário e senhas. Por outras palavras, é um ataque informático destinado a roubar os dados de autenticação de uma pessoa. É comum ser feito através de mensagens de correio electrónico que são enviadas em nome de um serviço, por exemplo, de um banco online e que pedem a inserção dos dados de autenticação. Outros exemplos são mandar mensagem dizendo ser um administrador pedindo a senha ou criar um site fraudulento que tenha aparência de ser bem conhecido site de mercado, a fim de ganhar o nome de usuário e senha.

Pidgin OTR. Software seguro de mensagens instantâneas (IM - *Instant Messaging*). Pidgin é um cliente livre e de código aberto que permite organizar e gerir o seu serviço de mensagens instantâneas. O *Off-the-Record* (OTR) *plug-in* projetado para uso com Pidgin garante autenticação e protege as comunicações entre os usuários do Pidgin (https://pidgin.im/).

***PIN Code - Personal Identification Código Number* (código de identificação pessoal)**. Método de validação secundário para proteger contra a perda de fundos se o nome de usuário e senha são descobertos. Geralmente, ele só é solicitado durante a transferência de fundos para fora do mercado ou para confirmar e finalizar ordens.

Piscina de mineração (*mining pool*). Serviço que permite que os proprietários de hardware de mineração antes separados possam unir forças e, assim, dividir a recompensa proporcionalmente ao trabalho apresentado. A probabilidade de encontrar um *hash* (bloco válido) é proporcional à *hashrate* (taxa de *hash*). Desse modo pequenos mineradores individuais podem levar meses antes de encontrar uma grande recompensa por bloco. Portanto, piscinas de mineração permitem o fluxo mais constante apesar da teórica renda menor (dividir o prêmio). Normalmente, as piscinas de mineração são centralizadas. Desse modo, o proprietário da piscina é quem distribui os intervalos de valores de *nonce* entre seus trabalhadores (mineradores) e determina o conteúdo do bloco. A P2Pool (http://p2pool.org/) é uma piscina totalmente descentralizada. Veja Mineração, *Pool* e *Mempool*.

***Plug & Play* (plugue e use)**. No *Plug & Play*, os softwares necessários para o funcionamento do equipamento (periférico ou acessório) já veem pré-instalados na memória do computador e, assim, basta apenas "espetar" (encaixar numa porta [USB, HDMI, etc.] ou num *slot*, seja diretamente ou através de um cabo) o dispositivo para que ele esteja pronto para ser usado.

***Plug-in* (ligue)**. Significa um módulo de extensão, de complemento ou de inserção. Em síntese, trata-se de um pequeno arquivo acoplado a um programa, acrescentando-lhe mais funções. É um programa usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica. Os plugins podem ter várias ou específicas funções. O habitual (comum) é que o plugin seja executado através do software principal, com aquilo que interage através de uma certa interface. Geralmente os plugins são leves e não comprometem o funcionamento do software e são de fácil instalação e manuseio.

Pod Slurping. Prática de roubo de informações por meio de dispositivos portáteis pré-configurados para a atividade. Podem ser utilizados pendrives, iPods e muitos outros aparelhos de armazenamento portátil. Há ataques diretos desta maneira e também ataques que apenas abrem portas (acesso) dos computadores para invasões.

***Pool* (piscina)**. Conjunto (grupo) de mineradores que se unem para minerarem coletivamente os blocos e depois dividirem a recompensa. As piscinas de mineração são uma ótima maneira para aumentar a probabilidade de êxito conforme a dificuldade aumenta.

***Pop-up* (emergir)**. É aquele anúncio que surge ("pipoca") de repente na tela, numa pequena janela (quadrinho à parte), antes mesmo de o site entrar no ar (ser carregado ou tornar-se visível) e que não tem como não ser visto. Por isso mesmo, ele custa muito mais caro, de trinta a cinquenta vezes mais que um *banner*.

Portal. Site que funciona como porta de entrada à Internet, oferecendo desde serviços como e-mail (correio eletrônico) e bate-papo (*chat*) até links para sites de conteúdos diversos.

POP - *Post Office Protocol* (protocolo de correios). Protocolo responsável pelo recebimento das mensagens de e-mail (correio eletrônico). Portanto, ele permite que todas as mensagens contidas numa caixa de e-mail possam ser transferidas sequencialmente para um computador local. Veja SMTP.

POP - Procedimento Operacional Padrão (*standard operating procedure*). Trata-se da descrição detalhada de todas as operações necessárias para a realização de uma tarefa; ou seja, é um roteiro padronizado para realizar uma atividade.

PoS - *Proof of Stake* (prova de participação). Trata-se de um mecanismo criado como forma de minimizar o impacto ambiental causado pela mineração de bitcoins, baseado no sistema de *Proof of Work* (PoW). Ao contrário do PoW, o mecanismo de PoS não requer a realização de cálculos computacionais intensivos e consequente dispêndio com energia elétrica durante a mineração. O PoS depende de os usuários manterem uma certa quantidade da moeda em suas carteiras e/ou em execução para manter a respectiva *blockchain* (*datacenter* ou bando de dados) segura. Dessa forma, as criptomoedas baseadas em PoS são muito mais eficientes no consumo de energia elétrica e podem oferecer transações mais ágeis. Saiba mais em Mineração e PoS.

PoW - *Proof of Work* (prova de trabalho). É um sistema que fixa a capacidade de mineração de uma criptomoeda ao poder computacional. Ao que seria um processo simples, é adicionada uma variável, a fim de tornar o processo de mineração mais difícil. Quando um bloco é gerado, o processo de criação deve necessariamente ter consumido tempo e poder de computação. Assim, um bloco gerado é considerado prova de trabalho. Saiba mais em Mineração e PoW.

PPP - *Point-to-Point Protocol* (protocolo ponto-a-ponto). Um dos protocolos necessários para manter uma conexão IP através de uma linha telefônica comum. O PPP é necessário para utilizar navegadores gráficos para a Web e é bastante superior ao Slip, outro protocolo com a mesma função.

***Predictive Analytics* (análise preditiva)**. Técnica de análise de acúmulo de dados constantes e confiáveis, através da qual se realiza uma previsão (antecipação de acontecimentos); exemplo, a previsão do tempo.

Private Key. Veja Chave privada.

Processador (*processor*). Circuito integrado (microprocessador ou cérebro eletrônico em um chip) que realiza as funções de cálculo e tomada de decisões de um dispositivo computacional. Pode-se fazer uma comparação do hardware do computador com o cérebro humano (agrupamento de dezenas de bilhões de neurônios); ambos são os componentes físicos de seus respectivos sistemas. Já a mente humana é semelhante ao software; ou seja, é imaterial, digital e intangível e não analógica (confira o verbete Digital). A mente consciente é a atividade cerebral relacionada ao processamento dos sensores (audição, visão, tato, olfato e paladar) e das informações (executar as funções lógicas), ao pensamento, à memória temporária (veja memória), à tomada de decisões e a realização das atividades. Já a mente subconsciente é a atividade cerebral relacionada à memória permanente. O subconsciente está logo abaixo da consciência e é facilmente acessível; por exemplo, uma informação arquivada na memória permanente é facilmente acessada e manipulada pelo consciente. Por outras palavras, as mentes consciente e subconsciente atuam de forma complementar uma a outra. O consciente consulta as informações gerenciadas pelo subconsciente; o qual, por sua vez, aceita qualquer coisa que nele for programado pela mente consciente (ou seja, o consciente comanda o subconsciente). A mente inconsciente, por sua vez, é a atividade cerebral relacionada às atividades auxiliares da mente consciente sobre as questões mais simples, rotineiras, básicas e triviais. O inconsciente também possui informações armazenadas; mas elas, em regra, não podem ser acessadas e, muito menos, manipuladas. Por outras palavras, o inconsciente é a única memória que não pode ser ter acessada diretamente. Desse modo, a mente consciente do cérebro humano seria similar ao processador (razão, lógica ou raciocínio), buffer (tráfego das informações) e cache (memória recente). O subconsciente seria equiparado ao Kernel. E o inconsciente seria equivalente ao BIOS e ao *firmware* (veja Boot). Veja o verbete CPU. Saiba mais em processador no teor do e-book.

***Processing time* (tempo de processamento)**. Tempo requerido por um mercado ou fornecedor, a fim de completar uma transação. No caso da rede Bitcoin, trata-se de esperar por confirmações suficientes na *Blockchain* para garantir que uma transferência (creditamento, pagamento ou depósito) tenha sido efetivada com sucesso ou garantia.

Profundidade (*depth*). Profundidade se refere a quantidade de blocos na *Blockchain* após o bloco referido. Desse modo, uma transação com 6 (seis) confirmações pode ser chamada de 6 blocos profundos (ou 6 *blocks deep*).

Programa-cliente (*customer program*). Trata-se de um dispositivo computacional ou um programa que requisita serviços a um servidor. A Internet é toda baseada em uma estrutura cliente/servidor. Para cada tipo de cliente, há um servidor correspondente. Na Web, os programas clientes são os navegadores, enquanto os servidores são os programas que armazenam as páginas e verificam as autorizações dos usuários para acessar determinados arquivos; além de executar programas especiais.

Programa (*software*). Uma lista de instruções e comandos para que o dispositivo computacional saiba como o que fazer e como proceder. Para isso, há várias linguagens que podem ser utilizadas: Cobol, Fortran, C, Basic, etc. Veja software e Linguagem.

Protocolo (*protocol*). Um conjunto de regras padronizado que especifica o formato, a sincronização, o sequenciamento e a verificação de erros em comunicação de dados. Dois computadores devem utilizar o mesmo protocolo para poderem trocar informações. O protocolo básico utilizado na Internet é o TCP/IP. Veja Endereço IP, HTTP, IP, TCP/IP e URL.

Proxy. Consiste num computador intermediário numa ligação, que recebe os pedidos de uma rede e dá-lhes seguimento. Por outras palavras, trata-se de um servidor que age como elo de ligação, recebendo requisições de clientes (especificadas através de um URL), solicitando recursos (arquivo, conexão, página, etc.) de outros servidores. Em suma, é um computador que oferece o serviço de rede de computadores para permitir que outros computadores possam fazer conexões de rede de forma indireta. De forma mais simples, trata-se de um servidor posicionado entre um computador cliente (onde o usuário ou operador humano está) com um navegador da Internet, por exemplo, e o servidor real, onde estão armazenados os dados da Internet solicitados. Assim que o cliente solicita uma conexão, arquivo ou outro recurso disponível em um servidor diferente, o *proxy* atende à solicitação conectando-se ao servidor especificado ou através da memória cache (armazenando das páginas recentemente ou mais acessadas). Dois algoritmos de cache simples são *Least Used* (LRU) e *Least Used* (LFU). Um exemplo comum é a rede interna de um estabelecimento, onde nenhum computador (terminal) possui acesso direto à Internet, mas somente através do computador servidor das redes interna e externa. Diante disso, o *proxy* pode possuir filtros, bloqueios e redirecionamentos das requisições feitas pelos usuários. Ao contrário de uma VPN, um *proxy* é um serviço que só muda o que os sites de endereços de IP podem ver dentro do seu navegador, em vez de todos os aplicativos no computador. Veja Servidor.

***Proxy* aberto**. *Proxy* mal configurado que pode ser abusado por atacantes (invasores) e utilizado como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

Public address. Veja Chave pública.

Public key. Veja Chave pública.

***Pump and dump* (bombear e descartar)**. É o processo de inflação artificial do preço de um bem que foi produzido ou adquirido a um custo baixo em altas quantidades. Isso se dá geralmente através de publicidade agressiva e falsas informações. A publicidade gerada leva outras pessoas a adquirirem este bem, aumentando a demanda e consequentemente o preço

(*pump*). Quando o valor se encontra alto o suficientemente, o responsável pela valoração (inflação) vende estes bens em sua posse (*dump*), o que força o preço para baixo e prejudica a todos outros proprietários desde bem.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, **Q**, R, S, T, U, V, W, X, Y e Z.

QR code. Código de barras bidimensional que pode ser convertido em texto, URL, número de telefone, geolocalização, etc. É muito utilizado para codificar e facilitar a leitura de chaves privadas e endereços bitcoins, por ser facilmente escaneado é usado na maioria dos telefones celulares equipados com câmera.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, **R**, S, T, U, V, W, X, Y e Z.

RAM - *Random Access Memory* (memória de acesso aleatório). Principal memória temporária do computador. É apagada (esvaziada ou limpa) quando se desliga o computador. Veja ROM, Cache e Buffer.

RAT - *Remote Administration Tool* (ferramenta de administração remota). Um software que permite que um operador remoto controle um sistema ou computador como se tivesse acesso físico ou presencialmente no mesmo.

***RedeemScript* (resgatar script)**. É um script (roteiro) semelhante em função de um roteiro de chave pública (pubkey). Uma cópia dele é um hash para criar um endereço de P2SH (usado em um verdadeiro roteiro pubkey) e outra cópia é colocada no roteiro de despesa da assinatura para impor suas condições. Por outras palavras, em vez de se creditar (pagar) para o endereço público de uma pessoa, o faz para o de um roteiro (script). Portanto, **P2SH** é a sigla de "Pay to Script Hash" (pague para script hash). Um endereço P2PKH ou saída P2PKH consiste num endereço que compreende um *hash pubkey* (chave pública) e sua correspondente saída. Os dados gerados por um gastador (pagador) são, quase sempre, utilizados como variáveis para satisfazer um roteiro pubkey. O script PubKey é incluído na saída que define as condições que devem ser cumpridas para que

aquelas bitcoins sejam gastas. Os dados para cumprir as condições podem ser fornecidos em um script de assinatura denominado de ScriptPubKey. Uma saída em uma transação contém dois campos: um do valor para a transferência de zero e um do roteiro PubKey para indicar que condições devem ser cumpridas para aquelas bitcoins possam ser transferidas. Veja P2P Escrow.

Reorganização (*reorganization*). Na rede (protocolo) Bitcoin, a reestruturação de cadeias de blocos é o termo utilizado para referir-se à situação em que um cliente (nó) da rede descobre uma nova cadeia de blocos bem formada, dificilmente mais longa, que exclui um ou mais blocos que o cliente pensava anteriormente serem parte da cadeia de bloqueios bem formada mais difícil. Estes blocos excluídos se tornam órfãos. Em resumo, na rede Bitcoin, quando um bloco aparentemente válido é substituído por um bloco, isso é chamado de reorganização na *Blockchain* (cadeia de blocos) e o bloco substituído é chamado um bloco de órfão. A reorganização da cadeia é um fenômeno cliente-local; ou seja, a rede Bitcoin inteira não reorganiza simultaneamente. Quando uma reorganização acontece, as transações dos blocos órfãos são movidas para a *mempool* (piscina de transações não confirmadas); mas aquelas que já tinham sido incluídas na cadeia principal se tornam inválidas. Diante disso, podemos dizer que uma transação é confirmada quando foi incluída num bloco e não ocupa o último bloco na cadeia de blocos (bloco mais recente na *Blockchain*). No entanto, embora raro, é possível aos últimos x blocos se tornarem órfãos em uma reorganização. Portanto, nunca se pode dizer com certeza que uma transação é confirmada; vez que é sempre possível que seja aparentemente incluída na cadeia de blocos (*blockchain*), mas possa ser substituída por uma grande reorganização. Na prática, a comunidade adotou 6 (seis) blocos como um período padrão de confirmação. Isto é, uma vez que uma transação é incluída num bloco na cadeia de blocos e é seguida por pelo menos 6 (seis) blocos adicionais, a transação é chamada de confirmada. Veja Número de confirmação.

***Resolution* (resolução)**. Procedimento utilizado quando há uma disputa entre um comprador e o respectivo vendedor. Geralmente utiliza-se de um árbitro para determinar como os fundos de *escrow* serão movimentados.

***Reviews* (rever)**. O corpo de comentários deixados em um site, juntamente com mais informações obtidas por canais externos. Usado por compradores para determinar se eles devem ter um fornecedor ou comprador como legítimo.

RFC - *Request for Comments* (pedido de comentários). São documentos técnicos desenvolvidos e mantidos pelo IETF - *Internet Engineering Task Force* (Grupo de Trabalho de Engenharia da Internet); instituição que especifica os padrões que serão implementados e utilizados em toda a Internet. Saiba mais em https://www.ietf.org/.

ROM - *Read Only Memory* (memória somente de leitura). Tratasse da memória não volátil (permanece mesmo quando computador é desligado). Só de leitura significa que não pode ser alterada ou deletada (apagada) pelo utilizador. A BIOS, por exemplo, é gravada em uma espécie (tipo) de memória ROM; ou seja, EPROM. Veja RAM, Cache e Buffer.

Rootkit. Espécie (tipo) de código (software) malicioso (malware). Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou administrator) em um computador; mas, sim, para manter o acesso privilegiado em um computador previamente comprometido. Veja Ataque.

Roteador (*router*). Computador, software ou material dedicado que serve para interligar computadores ou redes efetuando automaticamente o redirecionamento correto dos pacotes de informação de uma máquina para outra. Trata-se de um equipamento mais eficiente do que um *switch*; pois além de poder fazer a mesma função deste, ainda tem a capacidade de escolher a melhor rota que um determinado pacote de dados deve seguir para chegar ao seu destino. Existem dois tipos básicos de roteadores: estático e dinâmico. O estático é mais barato e escolhe sempre o menor caminho para os dados, sem considerar se aquele caminho tem, ou não, congestionamento. Já o dinâmico é mais sofisticado e considera se há, ou não, congestionamento na rede. Ele trabalha para fazer o caminho mais rápido (ou menos congestionado), mas que nem sempre é o de menor distância; pois de

nada adianta usar o caminho mais curto se esse estiver congestionado. Ainda mais, muitos dos roteadores dinâmicos são capazes de fazer compressão de dados para elevar a taxa de transferência. Veja Endereço IP (*IP adress*), HTTP, Hub, IP, TCP/IP e URL.

Ruby. Linguagem de programação interpretada multiparadigma, de tipagem dinâmica e forte, com gerenciamento de memória automático, originalmente planejada e desenvolvida para ser usada como linguagem de *script*.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, **S**, T, U, V, W, X, Y e Z.

Saas - S*oftware as a service* (software como um serviço). Modo de comercialização de um software, caracterizando-o como serviço, onde o cliente paga uma taxa mensal para utilização do mesmo e o fornecedor se responsabiliza por toda estrutura necessária à disponibilização do sistema.

***Samples* (amostras)**. No contexto de um mercado, um elemento de custo baixo livre ou enviado para um comprador bem conhecido, a fim de estabelecer a legitimidade. Isto prova que o vendedor tem acesso a um produto e é capaz de fornecê-lo de maneira segura. Da parte que o recebe, é esperado que avalie e comente sobre a qualidade e demais detalhes do produto (*feedback*).

Satoshi. Menor divisão de uma bitcoin (0.00000001 btc); ou seja, um centavo de bitcoin.

Satoshi Nakamoto. Pseudônimo usado pelo criador do protocolo original do Bitcoin. Antes de seu "desaparecimento", em meados de 2010, mantinha-se ativo postando informações técnicas no fórum BitcoinTalk e modificando a rede Bitcoin. Ele foi o responsável por criar a maior parte do protocolo, raramente aceitando contribuições de terceiros.

***Scam* (golpe)**. Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras. Confira *scam* no texto do e-book.

Scammer. Trata-se do golpista; ou seja, aquele que tenta fraudar ou aplicar golpes. Por exemplos, pode ser um fornecedor que não envia os produtos, envia produtos de má qualidade, falsificados ou adulterados, ou envia pequenas quantidades corretamente para ser aprovado na compra teste e depois não envia nada na compra grande. Também pode ser cometido por um vendedor que, por exemplo, alega que não recebeu os bens que foram entregues ou que os bens eram de má qualidade, falsificados ou adulterados.

***Scamcoin* (moeda fraudulenta)**. Trata-se de uma altcoin criada com o objetivo de aplicar golpe nos usuários e, assim, enriquecer o(s) seu(s) criador(es), mediante os mais diversos procedimentos, tais como, por exemplos, *pump-and-dump* (bombear e descartar), pré-mineração, etc.

Scareware. Malwares que são acessados pelos usuários mais ingênuos ou desavisados, pois ficam escondidos em *banners* maliciosos. Podem ser percebidos em páginas da web que mostram informações como, por exemplos: “Seu computador está infectado! Clique aqui para limpar sua máquina!” ou “Você foi sorteado e ganhou um prêmio! Clique aqui para receber seu prêmio!”.

***Screenlogger* (registrador de tela)**. Tipo específico de *spyware*. Programa similar ao keylogger, que é capaz de armazenar, nos momentos em que o mouse é clicado, a posição do cursor e a tela apresentada no monitor ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de *Internet Banking*.

Script. Também conhecido como linguagem de *scripting* ou linguagem de extensão, é uma linguagem de programação executada do interior de programas e/ou de outras linguagens de programação; mas não se restringindo a esses ambientes. Serve para estender a funcionalidade de um programa e/ou controlá-lo, acessando sua API (*Application Programming Interface* ou Interface de Programação de Aplicativos) e é muito usado como ferramenta de configuração e instalação em sistemas operacionais (*shell script*), como por exemplo, em alguns da família Linux, que usam a linguagem bash. São também frequentemente usados em jogos, como por

exemplo, os jogos Impossible Creatures e Tibia, que usam a linguagem Lua para controlar as ações dos personagens e o ambiente de batalha.

Scrypt - Criptografia alternativa ao PoW (*Proof of Work*) do bitcoin (SHA-256), designada para ser mais utilizada por CPUs e GPUs, oferecendo uma resistência aos ASICs.

Search. Significa pesquisa.

***Search engine* (motor de busca)**. Motor de pesquisa. Sistema que recepciona palavras chaves ou frases e efetua a pesquisa das mesmas na Internet.

Selfie. Uma foto que alguém tira de si mesmo, tipicamente com um smartphone ou uma webcam e depois a posta (publica) em redes sociais;

SEO - *Search Engine Optimization* (otimização do mecanismo de busca). Consiste num conjunto de técnicas que visam otimizar a localização e um website frente aos principais sites de busca, tornando-o mais facilmente encontrado em motores de buscas orgânicas.

SEPA - *Single European Payments Area* (espaço de pagamentos único europeu). Trata-se de um sistema de pagamento integrado entre os países da Zona do Euro (comunidade europeia), que permite transferir fundos entre bancos e países diferentes. A operação de transferência é semelhante ao TED/DOC existente no Brasil, mas no caso da SEPA, engloba todos os países que utilizam a moeda Euro.

Server Spoofing. Ver *IP Spoofing*.

Servidor (*server*). Consiste num software ou num computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente ou terminais. Por outras palavras, trata-se de um computador especialmente desenvolvido e/ou configurado para receber e transmitir informações, bem como fornecer produtos e serviços de software a outros computadores conectados a ele por uma rede interna (privada). Em resumo, um servidor é um computador mais potente do que um

desktop comum; vez que são desenvolvidos e/ou configurados para trabalharem com cargas de trabalho mais pesadas e com mais aplicativos. De modo semelhante, um servidor pode se referir ao local onde está armazenado (hospedado) um site, portal, sistema ou serviço da Internet. Desta forma, quando um servidor, além de gerir a rede interna, também administra o acesso à rede externa (Internet), ele é denominado de servidor *proxy*. Explica-se. Como os computadores clientes (locais) não possuem acesso externo, eles precisam requisitar ao servidor *proxy* essa conexão externa; o qual a efetuará servindo de intermediário. Veja *Proxy*.

***Session hijacking* (sequestro de sessão)**. Quando um usuário malicioso intercepta cookies com dados do início da sessão da vítima em algum serviço online. Assim, o cracker consegue acessar a página do serviço como se fosse a vítima e realizar todos os roubos de informações e modificações que desejar.

SHA - *Secure Hash Algorithm* (algoritmo seguro de hash). Trata-se de uma família (SHA-0, SHA-1, SHA-2, SHA-3, etc.) de funções *hash* criptográficas publicadas pelo NIST - *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos) como um FIPS - *Federal Information Processing Standards* (processamento federal padrão de informações dos Estados Unidos). Veja *Hash*.

SHA-256. Função matemática do tipo *hash* utilizada no Bitcoin em diversos contextos; inclusive durante o processo de mineração. Confira Hash256 e Mineração.

Shareware. Software que pode ser experimentado gratuitamente antes da compra. Alguns *sharewares* funcionam somente durante um período determinado de avaliação, outros apenas mostram mensagens periodicamente lembrando o usuário que não se trata de um produto gratuito.

Shilling. Sobre alguém ou alguma coisa ao tentar fazer parecer autêntico.

***Shipping* (remessa)**. Processo de uma embalagem do fornecedor e do envio de mercadorias.

***Short* (baixo)**. Posição vendida; quando se abre uma posição de venda e lucra com a queda do preço do ativo, moeda, ação, etc.

Shortcut. Ver Atalho.

Signature. Ver Assinatura.

Sistema (*system*). Conjuntos de elementos ou recursos que se relacionam ou operam entre si. Em computação, um sistema é qualquer combinação dos diversos tipos de hardwares e softwares.

Sistema Operacional (*operational system*). O programa (software) básico e, normalmente, pré-instalado, sem o qual um computador não funciona. Cada ação do usuário (desde um clique no mouse ou apertar de uma tecla) é recebida, interpretada e executada pelo sistema operacional. O sistema operacional controla todos os componentes conectados (encaixados ou plugados) no gabinete ou diretamente na placa-mãe; incluindo, assim, os periféricos (impressoras, teclados, monitores, etc.). Há vários tipos e versões de sistemas operacionais: MS-DOS, Windows, Linux, OS, etc. Veja software e hardware.

Site. Uma espécie de casa virtual de uma pessoa, empresa ou instituição. É um grupo de documentos HTML relacionados e arquivos associadamente que residem em um servidor (computador hospedeiro). A maioria dos sites tem uma *home page* (página inicial) como ponto de partida; funcionando frequentemente como uma espécie de índice geral do site.

SLIP - *Serial Line Internet Protocol* (protocolo de Internet de linha serial). Trata-se do resultado da integração dos protocolos modens que precedem a sequência de protocolos TCP/IP; ou seja, um protocolo antigo de ligação simples da Internet (simples transmissão de dados entre duas máquinas; ou seja, envia unicamente dados seguidos de um carácter de fim de transmissão), fraco em controles (não efetua e nem controla endereço e nem controle de erro), que, por ser obsoleto, foi substituído pelo PPP.

Slot. Num computador são os encaixes livres (vagos) na placa-mãe (interior do computador) ou no gabinete (exterior do computador) em que é possível encaixar placas ou outros hardwares ou periféricos.

SMiShing. Similar a *phishing*, mas destinado a celulares (SMS).

SMS - *Short Message Service* (serviço de mensagens curtas). Tecnologia utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS - *Multimedia Messaging Service* (serviço de mensagens multimédia), permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

SMS4Tor. Autodestruição de mensagens. Serviço online semelhante ao do Privnote 9 https://privnote.com/), mas destinado para a rede Tor (Onion) e não requer JavaScript (Privnote RequireJS). O procedimento consiste em digitar uma mensagem no site, criar um link personalizado e compartilha com o destinatário da mensagem. O link (ligação) só irá funcionar uma vez. Desse modo, quem abre primeiro é o único que pode ler a mensagem. Trata-se de uma alternativa mais fácil de usar do que o PGP - *Pretty Good Privacy* (privacidade muito boa). Exemplo: https://www.igolder.com/pgp/encryption/.

SMTP - *Simple Mail Transfer Protocol* (protocolo de transferência de correio simples). É o protocolo padrão para envio de e-mails (correio eletrônico) através da Internet. Veja POP - *Post Office Protocol*.

***Sniffer* (farejador)**. Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras; ou seja, sem criptografia.

Sniffer Attack. Tipo de ataque realizado por softwares que capturam pacotes de informações trocados em uma rede. Se os dados não forem criptografados, os atacantes podem ter acesso às conversas e outros logs registrados no computador atacado.

Soft opt-in. Regra semelhante ao *opt-in*, mas neste caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Dessa forma, não é necessária a permissão explícita por parte do destinatário para receber e-mails desse remetente.

***Software* (programa)**. *Software* é uma palavra inglesa que acabou sendo adotada e popularizada na sua forma original. A palavra inglesa "soft" se refere a qualquer coisa mole ou macia; já "ware" significa pertencente a uma mesma espécie. Essa expressão foi pensada como forma de diferenciar os programas da parte "hard" (dura, rígida ou física) do aparelho. Em suma, *software* significa programa de computador. Trata-se de uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. É um programa (código ou conjunto de instruções) desenvolvido para realizar uma determinada função ou várias tarefas em um dispositivo computacional. *Software* é a manipulação, instrução de execução, redirecionamento e execução das atividades das máquinas. É toda a parte lógica de um dispositivo computacional (aparelho eletrônico que possui um chip ou processador). O *software* pode ser entendido como a mente (composta por elementos que não são palpáveis) que comanda o funcionamento da máquina. Por outras palavras, é o *software* que dá vida à máquina; sem ele a máquina não funciona (não faz nada). É como se fosse o espírito do aparelho computacional. *Software* é a parte imaterial de um aparelho computacional. É o elemento lógico e intangível de um dispositivo computacional. E o sistema operacional é o *software* mais importante de um computador, pois dele depende o funcionamento da parte física da máquina; os demais *softwares* funcionam dentro do sistema operacional. Veja programa e hardware.

Source code. Ver Código-fonte.

Spam. Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. *Blams*, abreviatura de *blog spams*, são os *spams* em blogs.

Spamcop. Instituição que oferece diversos serviços antispam, sendo o mais conhecido o que permite reclamar automaticamente de *spams* recebidos.

Spammer. Indivíduo que pratica o uso abusivo de recursos da Internet através de *spams*.

Spam zombie. Computador infectado por código malicioso (bot), capaz de transformar o sistema do usuário em um servidor de e-mail (correio eletrônico) para o envio de *spam*. Em muitos casos, o usuário do computador infectado demora a perceber que seu computador está sendo usado por um invasor para esse fim.

Spoof. Mascarar informações para evitar rastreamento.

Spoofing. A criação e publicação de sites na Web que imitam sites genuínos com a intensão fraudulenta de obter dados pessoais ou o pagamento abusivo de bens e serviços.

Spooler. Programa que controla a fila de impressão; ou seja, organiza as ordens de impressão dadas para a impressora.

***Spyware* (ou *spy*)**. Programa espião automático que, sem o conhecimento e consentimento do usuário, recolhe informações sobre o usuário (sexo, idade, localidade, locais frequentados, costumes, gostos, compras, pesquisas feitas, etc.) e as transmitem pela Internet a uma entidade. Os *spywares* podem ser desenvolvidos por firmas comerciais que desejam monitorar o hábito dos usuários para avaliar seus costumes; bem como para vender esses dados para empresas de marketing. Não deixa de ser uma espécie de *malware*. É similar ao *cookie*, mas diferencia por ser muito mais abrangente e estar oculto do usuário.

SQL injection. Uma técnica de injeção de código de banco de dados, usado para atacar os dados de aplicações nas quais maliciosas instruções, na linguagem SQL - *Structured Query Language* (linguagem de consulta estruturada), são inseridas em um campo de entrada para execução conduzida. Muitos mercados foram desligados ou perderam o seu dinheiro por causa desse tipo de ataque.

SSL - ***Secure Sockets Layer***. Em português, camada de conexão segura. São protocolos criptográficos que oferecem segurança à comunicação na Internet para serviços como e-mail (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados.

Stealth **(furtividade)**. Consiste em métodos de dissimulação ou camuflagem; comumente utilizados por fornecedores durante a embalagem de um item a ser enviado pelos Correios. Por outras palavras, modifica-se a aparência ou aplica-se um disfarce para que o item ou o negócio fique com aparência legítimo. Também pode ser a estratégia de escondendo o produto ilícito dentro de outro lícito ou que dificulta sua identificação pelo cheiro ou raio-x. Em suma, objetiva passar despercebido numa inspeção simples ou rápida.

Storage **(armazenamento)**. Dispositivo projetado especificamente para o armazenamento de dados, que permite a conexão via rede com um servidor ao *storage*, facilitando assim a expansão da capacidade de armazenamento sem impacto na produção, garantindo maior flexibilidade e confiabilidade no armazenamento.

Switch **(comutador)**. Em uma rede de telecomunicações, um *switch* é um dispositivo que canaliza os dados de entrada de qualquer uma das múltiplas portas de entrada para a porta de saída específica que levará os dados em direção ao destino pretendido. Trata-se do nó central de uma rede em estrela, tendo como função o chaveamento (ou comutação) entre as estações que desejam se comunicar. Em resumo, os comutadores operam semelhantemente a um sistema (central) telefônico com linhas privadas (PABX - *Private Automatic Branch Exchange* ou Troca automática de ramais privados). No PABX quando uma pessoa liga para outra, a central telefônica conecta-as numa linha dedicada (ramal), possibilitando um maior número de conversações simultâneas. Desse modo, no circuito de comutação de rede telefônica, um ou mais *switches* são usados para configurar os ramais dedicados conforme a necessidade, demanda ou requisição. Procedimento mais semelhante é o da central de interfones da portaria de um prédio; o seja, a central interliga momentaneamente pares de interfones para que falem entre si. Se não houvesse a central seria preciso um interfone individual (cabeamento direto e exclusivo) para poder falar com cada

apartamento. O *switch*, portanto, é um dispositivo utilizado em redes de computadores para reencaminhar pacotes (frames) entre os diversos nós (clientes ou terminais). Assim como os concentradores (hubs) possuem portas, com a principal diferença de que o comutador segmenta a rede internamente; ou seja, cada porta corresponde um domínio de colisão diferente impedindo colisões entre pacotes de segmentos diferentes. Outra importante diferença, um *switch* gerenciável pode criar VLANS; deste modo a rede gerida será dividida em menores segmentos, onde identifica cada porta e envia os pacotes somente para a porta destino, evitando assim que outros nós recebam os pacotes. Portanto, numa rede Ethernet local (LAN), um interruptor determina a partir do dispositivo físico (MAC - *Media Access Control*) qual porta deve ser usada e, de modo semelhante, em relação à Internet, o comutador determina a partir do endereço de IP (*Internet Protocol*) qual porta será utilizada pelos pacotes de dados. Veja Hub e Roteador (*router*).

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, **T**, U, V, W, X, Y e Z.

Tabela ASCII. Ver ASCII.

***Tag* (etiqueta)**. Normalmente se refere a um transponder (junção das palavras em inglês "transmit" e "responder" pelo fato de transmitirem uma resposta ao sinal do leitor) de RFID - *Radio-Frequency Identification* (identificação de radiofrequência), consistente num pequeno objeto que pode ser colocado em uma pessoa, animal, equipamento, embalagem ou produto, dentre outros. O sistema NFC - *Near Field Communication* (comunicação de campo próximo) utiliza o RFID. A etiqueta RFID costuma gravar e transmitir dados por ondas de radiofrequência permitindo controlar e monitorar objetos de forma segura e inteligente. As etiquetas (*tags*) NFC são formadas, basicamente, por um pequeno chip de rádio (de silício identificador de radiofrequência), acompanhado de uma antena simples (que lhe permite responder aos sinais de rádio enviados por uma base transmissora) e alguma quantidade de memória para armazenamento de dados. Normalmente, esses dispositivos funcionam no modo passivo; ou seja, não é necessário deixá-los ligados constantemente à uma fonte de energia. A RFID sem chip é um termo genérico para sistemas que usam

energia de rádio frequência para transmitir dados, mas não armazena um número serial em um microchip de silício no transponder. Algumas *tags* (etiquetas ou adesivos) sem chip usam plásticos ou polímeros condutivos em vez de microchips de silício. Outras *tags* sem chips usam materiais que refletem de volta uma parte das ondas de rádio irradiadas para eles. Um computador faz uma fotografia instantânea das ondas transmitidas de volta e usa-as como uma impressão digital para identificar o objeto com a *tag*. Empresas estão experimentando a incorporação de fibras refletoras de rádio frequências em papel para evitar fotocópias não autorizadas de determinados documentos. Há tintas que refletem as ondas de rádio em determinadas frequências, permitindo que os agricultores, por exemplo, tatuem um transponder RFID sem chip em um animal para fins de identificação. As etiquetas RFID, portanto, são geralmente passivas (sem alimentação), que podem variar em frequência, capacidade de memória e características de funcionamento. As *tags* passivas são alimentadas pela energia das ondas eletromagnéticas emitidas pela antena do leitor. A antena da *tag* captura essa energia, utilizando parte dela para a alimentação da etiqueta e a outra parte para o envio das informações ao leitor. Portanto, a antena da *tag* passiva só consegue enviar um sinal caso ela receba o sinal enviado pela antena do leitor. Dito de outra maneira, ela só responde caso ouça a um chamado. Caso contrário, ela não emite nenhum sinal ou, por outra, permanece "em silêncio". Já as *tags* ativas não precisam ser alimentadas pela emissão das ondas eletromagnéticas, pois elas possuem uma bateria interna que desempenha essa função. Elas, também, possuem um modulador de radiofrequência, com o que conseguem criar um novo sinal de radiofrequência sem a necessidade da presença do leitor. A antena das *tags* ativas fica, portanto, emitindo sinais o tempo todo esperando que a antena de um leitor os encontre. Isso significa que o sinal das *tags* ativas tem maior alcance, apresentando maior probabilidade de ser captado. Suas desvantagens, consistem no fato de que a bateria tem vida útil limitada, além de aumentar o custo e o tamanho das *tags*. Ainda existem as *tags* semi-passivas ou semi-ativas. É o meio termo entre a ativa e passiva. Elas, como as ativas, possuem uma bateria interna para sua alimentação. Entretanto, como as passivas, elas precisam da presença do leitor para comunicar suas informações; pois elas não possuem um modulador e não são, portanto, capazes de criar um novo sinal de radiofrequência. Em resumo, além das etiquetas passivas que somente respondem ao sinal enviado pela base

transmissora, também existem as etiquetas semipassivas e as ativas, dotadas de bateria, que lhes permite enviar o próprio sinal.

Tails. Um sistema operacional feito especialmente para atividades anônimas, que não deixa rastros no computador e que é inicializado a partir de um CD ou USB (https://tails.boum.org/index.pt.html).

Target. Ver Alvo.

Taxa de transação (*transaction fee*). Na rede Bitcoin, também conhecida como *mining fee* (taxa de mineração) ou *miners' fee* (taxa dos mineiros); consiste numa pequena taxa necessária para uma transação ser processada pelos mineradores. Trata-se de um pequeno valor com que o autor de transação paga para um mineiro incluir a transação em um bloco. A taxa é expressa como a diferença entre a soma de todos os valores de entrada e de saída. Ao contrário dos sistemas tradicionais de pagamento, os mineiros não requerem explicitamente taxas e a maioria dos mineiros permitir transações livres (gratuitas).

TCP/IP - *Transmission Control Protocol / Internet Protocol* (protocolo de controle de transmissão / protocolo de internet). Conjunto de padrões da Internet que orienta o tráfego de informações e define o endereçamento e o envio de dados. Para que dois computadores se comuniquem na Internet, é preciso que ambos utilizem o TCP/IP. Veja Endereço IP, HTTP, IP e URL.

***Template* (modelo)**. Página usada como base do desenho de todas as páginas num site.

Terahashes/sec (TH/s). Número de tentativas possíveis de resolver um *hash* em um dado segundo, medido em trilhões de *hashes* (TH/s).

***TestNet* (rede de teste)**. Uma rede alternativa ao Bitcoin usada para testes; ou seja, um conjunto de parâmetros utilizados para testar uma rede Bitcoin. *TestNet* é como *MainNet* (rede principal do Bitcoin), mas possui um bloco gênese diferente (que foi reajustado várias vezes). *Testnet* usa endereços um pouco diferentes do formato padrão para evitar confusão com

os endereços Bitcoins e todos os nós e mineradores estão ajustados para transações não-padrão. As moedas de *Testnet* são separadas e distintas de bitcoins reais e supostamente não possuem nenhum valor. Isso permite que desenvolvedores de aplicativos ou testadores de Bitcoin experimentem, sem ter que usar bitcoins reais ou se preocupar em quebrar a cadeia principal da rede Bitcoin.

***The Marketplace* (I2p)**. Mercado criado na rede I2P. Definido por uso de uma rede de anonimato alternativo e uso de P2SH aborda a manter todos os fundos em depósito durante o processo de encomenda. Tende a ser elogiado por sua segurança ou ridicularizado por os erros não-intuitivo que o modelo oferece. Você pode encontrar um guia de uso completo em breve no blog. Veja *P2P Escrow* e *RedeemScript*.

Tilt. Designação comum para o travamento de videogames e arcade, algo equivalente à paralisação de um computador ou ao BSOD - *Blue Screen Of Death* (tela azul da morte) do sistema operacional Windows. O termo surgiu das antigas máquinas de fliperamas (semelhante ao jogo pinball onde tem que ficar acertando e ricocheteando uma esfera sem deixá-la cair fora do tabuleiro). Quando muito sacudidas ou inclinadas, desligavam-se automaticamente e na tela, piscando sem parar, aparecia a palavra "TILT". Mas, apesar da pane, essa palavra não significa erro, mas sim estava indicando que o usuário estava balançando demais a máquina (estava trapaceando). Explica-se. A palavra inglesa "tilt" significa inclinar ou inclinação. A expressão "tilt", portanto, é semelhante às expressões "deu pane" ou "deu pau"; ou seja, quer dizer que a máquina travou ou enlouqueceu. Veja Bug.

***Timestamp* (carimbo de data / hora)**. Trata-se de uma representação padrão de tempo como um número de segundos desde 1 de janeiro de 1970 GMT - *Greenwich Mean Time* (tempo médio de Greenwich ou hora de Greenwich).

Tipo de *hash* (*hash type* ou *hashtype*). Os significados das palavras tipo e função são invertidos (trocados) nos algoritmos de hash. Assim quando se diz função, está na verdade se referido ao tipo, espécie ou modelo. Já quando se fala em tipo está se referindo à função, tarefa, operação ou

procedimento específico de cada script, algoritmo ou linha de comando dentro do mesmo software e, até mesmo, da mesma espécie de hash. Por óbvio, podem coexistirem mais de uma espécie de algoritmo de hash no mesmo software ou algoritmo. Há dois pontos principais que podem ajudar a identificar a espécie de hash; 1) O comprimento do hash, pois cada função de hash tem um comprimento de saída específico; e, 2) O alfabeto utilizado (quais as letras e os caracteres especiais existem). O script HashTag.py e sites como https://www.onlinehashcrack.com/hash-identification.php, http://md5decrypt.net/en/HashFinder/ e https://md5hashing.net/hash_type_checker ajudam a identificar a espécie de função criptográfica que foi usada para gerar o hash consultado. No protocolo Bitcoin existem alguns "tipos" (funções) básicos de hashes que afetam as saídas (*outputs*): OP_CHECKSIG é um script de código de operação utilizado para verificar se a assinatura para uma entrada de TX é válida. Já scriptPubKey verifica se a chave pública (na verdade um hash) é um valor específico e se OP_CHECKSIG aprovou. O Hashtype SIGHASH_ALL (padrão) requer que todas as saídas sejam hash e, assim, assina todas as todas as entradas e saídas; mas o SIGHASH_NONE só assina as entradas e limpa todas as saídas e, assim, qualquer um pode alterar o local para onde as bitcoins estão indo, a menos que outras assinaturas usando outros hashes protejam as saídas. O SIGHASH_SINGLE exige como única saída assinada aquela que corresponda (mesmo valor do índice) à entrada. Também permite a modificação de outras saídas e o número de sequência de outras entradas. SIGHASH_ANYONECANPAY, remove todas as entradas, exceto a atual; ou seja, assina apenas a atual entrada. O comportamento real é mais sutil do que esta visão geral, devendo verificar o código-fonte para melhor entendimento.

TLDR (*too long, didn't read*). Em português, "longo demais, nem li"; uma resposta para postagens extensas demais ou uma reprimenda para introduzir um sumário de textos curtos.

To hash. Para calcular uma função *hash* de alguns dados. Se a função *hash* não é explicitamente mencionada, é aquela definida pelo contexto. Por exemplo, "uma transação para *hash*" significa calcular Hash256 de representação binária de uma transação.

Tor (*The Onion Router*). Em português, o Roteador Cebola, é um protocolo de roteamento, usado por pessoas que querem manter sua privacidade na rede. Usa o "onion routing" (roteamento Onion) para fornecer acesso anônimo à Internet por meio da criptografia de uma mensagem várias vezes com cada relé removendo uma camada antes que o destino final seja alcançado. Confira em https://www.torproject.org/. Veja *Deep Web*.

***Tor Browser Bundle* (TBB)**. Em português é pacote do navegador Tor. Trata-se de uma versão modificada do Firefox que permite usar facilmente a rede anônima Tor. Ele é compatível com Windows, OS X e Linux.

Tor Exit Node. O último *relay* (retransmissão) em que os dados percorrem de seu criador ou emissor original (um computador) antes de chegar ao destinatário; normalmente consiste num servidor que intermedia o acesso do usuário (destinatário). Para o destinatário, o tráfego parece se originar a partir do nó de saída.

Tor Node. A transmissão de dados, seja um ponto de conexão, um ponto de distribuição (*middle node*) ou um ponto final (nó de saída ou *exit node*).

Torchat. Serviço de mensagens instantâneas que funciona fazendo com que cada usuário crie um "hidden service" (serviço oculto), que pode ser usado para contatá-los via Tor.

Torch (*Tor Search Engine*). É motor de pesquisas na Deep Web (http: //xmh57jrzrnw6insl.onion/).

***Trade* (comércio)**. O ato de utilizar estratégias para lucrar com a compra e a venda de ativos ou moedas

***Trader* (comerciante)**. Pessoa que pratica *trade*, seja por hobie, seja como meio de trabalho e fonte de renda.

***Trading* (negociação)**. Veja *Exchange*.

Transação (*transaction*). Trata-se do ato de transferência de créditos na rede Bitcoin. É a ordem de pagamento; ou seja, a saída de valores em poder

do emitente da ordem em benefício do destinatário indicado (favorecido) através de um endereço Bitcoin (endereço ou chave pública). Por outras palavras, uma transação é quando os valores são enviados de um endereço bitcoin para outro. De outro modo, trata-se de dados binários que descrevem como bitcoins são movidos de um proprietário para outro. Representa, portanto, a transferência de um certo valor proveniente de uma ou mais fontes de fundos, chamado *input*, para um ou mais destinos, chamado *output*. Toda a transação (exceto a coinbase) tem uma referência a uma ou mais operações anteriores (entradas) e uma ou mais regras sobre como gastar essas bitcoins (saídas). A transação contém uma prova de posse para cada quantia de bitcoins (*inputs*) que é transferida, na forma de uma assinatura digital assinada pelo dono (consiste na chave privada), que pode ser validada por qualquer membro (nó ou cliente) da rede, de maneira independente. Consiste a transação numa linha, de dupla entrada (partidas dobradas), num registro contábil público e descentralizado; ou seja, na *Blockchain*. As transações movimentam valores a partir de *inputs* (entradas) de transação para *outputs* (saídas) de transação. Um *input* (entrada) é o lugar de onde vem o valor da moeda, geralmente um *output* (saída) de uma transação prévia. Desse modo, um *output* de transação designa um novo dono para o valor ao associá-lo com um script de travamento. Esse script de travamento exige uma assinatura ou outra forma de validação (script de destravamento) para a retirada dos fundos em transações futuras. *Outputs* de uma transação podem ser usados como *inputs* em uma nova transação, dessa maneira criando uma cadeia de posses à medida que o valor é movido de um endereço para outro. Por outras palavras, a transação é o ato de desbloquear um crédito anteriormente recebido e dar-lhe um novo beneficiário, repassando esses créditos com um bloqueio que somente o seu beneficiário pode desbloquear quando for realizar uma transação. Cada transação contém um ou mais "inputs" (entradas), que são débitos em uma conta (endereço público) bitcoin. Do outro lado da transação, também existem um ou mais "outputs" (saídas) que são créditos adicionados em uma conta bitcoin. Explica-se. Apesar de os créditos consistirem numa saída da conta do pagador, primeiramente eles tiveram que configurar uma entrada e, logo em seguida, serem convertidos numa saída. E, de modo inverso, apesar dos créditos do favorecido ser uma entrada, eles já são previamente posicionados como uma saída que exige o respectivo desbloqueio. Os *inputs* e *outputs* (entradas e saídas ou débitos e créditos) somados não

necessariamente resultam na mesma quantia. Ao invés disso, os *outputs* são um pouco maiores do que os *inputs*, e essa diferença se dá devido à taxa de transação; que é um pequeno pagamento coletado pelo minerador que inclui a transação na *Blockchain*.

Transação confirmada (*confirmed transaction*). A confirmação significa que uma transação foi processada pela rede Bitcoin e é altamente improvável que seja revertida. A transação recebe confirmação quando é incluída em um bloco alocado na *Blockchain* e à cada novo bloco subsequente na *Blockchain*. Cada confirmação diminui exponencialmente o risco de uma operação inversa ou dupla. A probabilidade de uma transação vier a ser rejeitada é medida em quantidade (número) de confirmações. Veja Confirmação (*confirmation*) e número de confirmação.

Transação de entrada (Txin - *transaction input*). Uma parte de uma transação que contém uma referência a uma transação anterior de saída e um roteiro que pode provar a propriedade do valor de saída. O script normalmente contém uma assinatura e, portanto, chamado scriptSig. As entradas consomem totalmente o valor de saída. Então, em caso de o usuário pagador só querer usar parte do valor, será necessário incluir um adicional de mudança de saída (veja *Change* (alterar)) para enviar a porção restante ou troco de volta para o seu dono (no mesmo ou outro endereço).

Transação de saída (Txout - *transaction output*). Uma saída (*output*) contém uma quantidade a ser enviada e um roteiro que permite ainda mais os gastos. O *script* normalmente contém uma chave pública (ou um *hash* de uma chave pública) e uma verificação de assinatura opcode. Apenas um proprietário de uma correspondente chave privada é capaz de criar uma outra transação que envia esse valor para outrem. Em cada transação, a soma dos valores de saída deve ser igual ou menor do que a soma de todos os valores de entrada. Veja *Change* (alterar).

Transação não confirmada (*unconfirmed transaction*). É a transação (Tx) que não está incluída em qualquer bloco na *Blockchain*. Também conhecida como transação "0 confirmed" (sem nenhuma confirmação). As transações não confirmadas são retransmitidas pelos nós (clientes) da rede P2P do Bitcoin e permanecem em suas *mempools* (piscinas de memória) até

que o nó aas incluam na *Blockchain* (só um minerador pode fazer isso) ou decide jogá-las fora. Veja Confirmação (*confirmation*), número de confirmação e *Verificação*.

Transação não-padrão (*non-standard transaction*). Qualquer transação (Tx) válida que não seja padrão. As transações não-padrão não são retransmitidas e nem minadas pelo padrão Bitcoin Core (antigo BitcoinQT), mas estão existem na *TestNet* (rede de teste). Entretanto, se alguém coloca uma operação não-padrão em um bloco, ele será aceito por todos os nós da rede Bitcoin. Na prática, isso significa que as transações incomuns vão demorar mais tempo para serem incluídas na *Blockchain*. Se algum tipo de transação não-padrão se tornar útil e popular, ela pode ficar com o nome padrão e ser adotada pelos usuários.

Trojan horse. Veja Cavalo de Tróia.

TrueCrypt (http://truecrypt.sourceforge.net/). Aplicativo de código aberto usado para criptografar dispositivos de armazenamento, como discos rígidos e drives flash USB. É também utilizado para criar discos virtuais criptografados contidos num ficheiro que monta de forma semelhante a dispositivos de armazenamento reais.

Tumbler. Trata-se de um método para tornar anônima a fonte das criptomoedas através da misturação dos fundos das transações com outros fundos, com a intenção de confundir a trilha de volta à fonte original do fundo. O mesmo que bitcoin mixer. Veja *Mixing*.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, **U**, V, W, X, Y e Z.

Unix. Sistema operacional lançado em 1971 por Ken Thompson e Dennis Ritchie. Quando apareceu, o Unix tinha inúmeras vantagens, era distribuído gratuitamente, funcionava em qualquer computador e era tão flexível que podia ser moldado e reprogramado pelo próprio usuário; além de ser poderoso o suficiente para suportar grandes quantidades de dados. Entretanto, era preciso ser um iniciado em computação para entendê-lo. Em razão de sua flexibilidade, surgiram centenas de versões do Unix. Usado

principalmente por universidades e cientistas, a linguagem Unix caiu no gosto dos entendidos em microcomputadores, com o que surgiu o Linux; uma versão mais amistosa e mais acessível.

***Upload* (envio)**. Ato de transmitir (enviar ou carregar) um arquivo ou informação de um computador local para outro computador. É o contrário de *Download*.

***Up Selling* (acima da venda)**. Estratégia de marketing em que o lojista oferece um produto ou serviço superior ou em maior quantidade àquele que está sendo originalmente adquirido (comprado ou contratado).

URL - *Uniform Resource Locator* (localizador padrão de recursos). É o endereço de um recurso disponível em uma rede. Trata-se do padrão de endereçamento da Web. Permite que cada arquivo na Internet tenha um endereço próprio, que consiste de seu nome, diretório, máquina onde está armazenado e protocolo pelo qual deve ser transmitido. Cada página da rede tem sua própria URL. Um URL é composto de um protocolo, que pode ser tanto HTTP (um protocolo de comunicação), FTP (forma rápida de transferir arquivos na internet), etc. Veja Endereço IP, HTTP, IP e TCP/IP.

USB - *Universal Serial Bus* (barramento serial universal). Trata-se de um sistema de comunicação entre um dispositivo computacional e seus diversos periféricos. O exemplo mais conhecido é o cabo de celular que liga o celular a computador através das portas USB existentes nos dois dispositivos. O pendrive também se conecta através de uma porta USB. Veja Barramento.

UTC - *Universal Time Coordinated* (tempo universal coordenado). Trata-se do protocolo ou convenção que define o fuso horário de referência a partir do qual se calculam todas as outras zonas horárias do mundo. O UTC é o sucessor do Tempo Médio de Greenwich (**GMT** - *Greenwich Mean Time*). Ao contrário do GMT, o UTC não se define pelo Sol ou pelas estrelas, mas trata-se de uma medida derivada do Tempo Atômico Internacional (TAI - *Temps Atomique International*). Entretanto, GMT é um fuso horário; já UTC não é uma zona de tempo, mas um padrão de tempo que é a base para o tempo civil e zonas de tempo em todo o mundo. TAI é uma

escala de tempo que utiliza a potência combinada de cerca de 400 relógios atômicos de alta precisão. Pelo GMT, o fuso horário é contabilizado a partir do meridiano de Greenwich: para oeste o fuso é negativo, já para o leste é positivo. Recorda-se que as zonas horárias ou fusos horários são cada uma das vinte e quatro áreas ou meridianos (divisão da duração do dia no transcurso do giro do Globo) em que se divide a Terra e que seguem a mesma definição de tempo. A Terra possui 360° (é redonda) e o dia é composto por 24 horas (ciclo da luz do Sol circundando a Terra). Desse modo, divide-se os 360° por 24 horas, totalizamos 15°; o que corresponde a 60 minutos (1 hora) por cada paralelo ou fuso horário. Por exemplo, para o fuso horário de Brasília, é aplicado o UTC – 3. Isso significa que a hora é medida menos 3, levando em conta o UTC (Tempo Universal Coordenado). Durante os meses de horário de verão, muda para a medição para UTC – 2. Os estados que não seguem o horário de Brasília, possuem UTC's diferentes. Confira os horários pelo mundo no site: http://24timezones.com/hora_certa.php. O site http://www.timezone.me/pt/time-zone-converter ajuda na conversão rápida de fusos horários. Já o site http://www.convertworld.com/pt/zonas-horarias/sao-paulo-brasil.html facilita a visualização das zonas dos fusos horários para facilitar a conversão. Veja, ainda, os sites http://www.timezoneconverter.com/cgi-bin/tzc.tzc e https://www.timeanddate.com/time/map/.

Utilitários (*utilities* ou *tools*). Programas (*softwares*) auxiliares ao sistema operacional que podem ser extremamente úteis. Possuem as mais diversas funções: compactação de dados, sistemas de alerta contra vírus, aumento de desempenho de máquinas, *overclock*, limpeza de discos rígidos, acesso à Internet, partilha de conexões, etc.

UTXO Set. Uma coleção (conjunto) de saídas de transações que ainda não foram utilizadas (UTXO).

UTXO - *Unspent Transaction Output* (saída da transação não desembolsada). São créditos enviados (transação) a um usuário, e este beneficiário ainda não os gastou (não efetuou nova transação) com os mesmos créditos. Saiba mais sobre UTXO no teor do e-book.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, **V**, W, X, Y e Z.

***Vendor* (fornecedor)**. Quem vende o produto em um mercado; ou seja, um vendedor (*salesman*). Essa transação ou produto pode ser de natureza ilegal, semilegal ou completamente legal.

***Vendors Roundtable* (mesa redonda de fornecedores)**. Prática utilizada em sites para permitir que fornecedores levantem questões sobre o mercado ou compradores sem levantar alarme na população em geral.

Verificação (*verification*). Consiste no procedimento efetuado pela rede Bitcoin de verificar se quem quer transferir créditos (efetuar um pagamento), realmente possui a quantidade de bitcoins necessária. Esse procedimento é efetuado por qualquer cliente (nó ou ponto) da rede P2P e de forma cumulativa. Cada cliente que faz esse procedimento e obtêm resultado positivo (afirmativo, válido ou de sucesso), repassa a informação adiante na rede. Mas se o resultado é negativo, o cliente (nó) apenas rejeitará a transação e retornará uma mensagem informando a rejeição. Explica-se. Transações rejeitadas não são retransmitidas para fins de evitar sobrecarga, *spams* ou alguma espécie de ataque à rede. Desse modo, após a conferência da conta de saída (endereço público pagador ou remetente), do saldo suficiente, da chave privada ser a correlata e válida, de não se tratar de gasto duplo, não ser uma operação mal formatada, etc., cada nó (cliente) da rede propaga (divulga) a transação válida para conhecimento público. Neste processo de propagação, cada novo nó da rede que receber a transação verificará a transação por si próprio e, em caso de validação, continuará transmitindo para todos os nós com os quais estiver conectado sucessivamente. Para que se possa verificar se quem pretende efetuar um pagamento ou transferência possui saldo suficiente, cada cliente (nó da rede Bitcoin) confere o referido endereço público de saída (*input*) na *Blockchain*. Apesar de que as transações de bitcoins se completarem quase que instantaneamente, elas exigem um determinado número de confirmações para poderem ser finalizadas. De costume, esperam 6 (seis) confirmações. Após verificada a transação, o próximo passo será ela ser incluída em um bloco através de um nó minerador e ser inserida na *Blockchain*. Este é o procedimento de confirmação. Veja *Transação*.

Vírus. Pequeno programa desenvolvido para causar danos em diversos níveis, podendo afetar a integridade de arquivos de dados (removendo partes ou arquivos por completo), prejudicar um computador em particular ou toda a rede de uma empresa

Volatilidade (*volatility*). Volatilidade é a qualidade do que sofre constantes mudanças ou muda frequentemente. Na área financeira, é uma medida de dispersão dos retornos de um título ou índice de mercado. Quanto mais o preço de uma ação varia num curto período de tempo, maior o risco de se ganhar ou perder dinheiro negociando esta ação, e, por isso, a volatilidade é uma medida de risco. Portanto, a volatilidade é uma variável que mostra a intensidade e a frequência das oscilações nas cotações de um ativo financeiro. Esta variável (a volatilidade) é um dos parâmetros mais frequentemente utilizados como forma de mensurar o risco de um ativo considerado. Em resumo, a volatilidade é a medida dos movimentos de preços ao longo do tempo para um ativo financeiro, incluindo a bitcoin.

VPN - *Virtual Private Network* (rede privada virtual). É uma rede de comunicações privada construída sobre uma rede de comunicações pública (como por exemplo, a Internet). No contexto da atividade anônima, a VPN normalmente é um *proxy* que pretende ser anônimo para ocultar a identidade do usuário final. Geralmente é usada para esconder que se está conectado a uma rede anônima como o Tor. A VPN se tornou popular quando decisões judiciais determinaram o bloqueio do WhatsApp (aplicativo de mensagens instantâneas pelo *smartphone*); ou seja, através da VPN os usuários simulavam que estavam em outro país e, assim, continuavam utilizando o serviço temporariamente bloqueado no Brasil.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, **W**, X, Y e Z.

W3C (*World Wide Web Consortium*). É um consórcio mundial fundado em 1994, responsável pela criação das normas que regem a Web. As maiores empresas do mundo na área da Informática pertencem a este consórcio, como por exemplos, Apple, Microsoft, IBM, Google, etc.

Wallet. Ver Carteira.

Wearable User Interface. Qualquer coisa que seja "vestida" (relógios, óculos, roupas, etc.) e esteja conectada, como Smartwatches, pulseiras inteligentes, etc.

Web (*World Wide Web* ou WWW). Área da Internet que contém documentos em formato de hipermídia; uma combinação de hipertexto com multimídia. Os documentos hipermídia da WWW são chamados de páginas Web e podem conter texto, imagens e arquivos de áudio e vídeo; além de ligações com outros documentos na rede. A característica multimídia da Web a tornou a porção mais importante da Internet. Veja WWW.

***Web server* (servidor web)**. O termo é usado tanto para designar o programa que disponibiliza conteúdos na web como o computador que o aloja. Veja Servidor.

Web site. Um servidor de WWW. Contém páginas interligadas conhecidas como documentos de hipertexto (páginas de Web).

Whonix (https://www.whonix.org/ e http://zo7fksnun4b4v4jv.onion) é um sistema operacional baseado no Debian focado em anonimato, privacidade e segurança através do isolamento. Whonix consiste em duas partes: uma exclusivamente corre o Tor e é chamado Gateway. A outra, a Workstation, está em uma rede completamente isolada. Somente conexões através do Tor são possíveis.

***Whistleblowing* (denúncias)**. Divulgação por uma pessoa, geralmente um empregado em uma agência do governo ou empresa privada, para o público ou para os que exercem autoridade, de má gestão, corrupção, ilegalidade ou algum outro delito.

***Workstation* (estação de trabalho)**. Pode significar um computador que faz parte de uma rede interna de uma empresa ou se refere a um tipo específico de computador, com altíssima capacidade de resolução gráfica, usado para projetos de engenharia ou tarefas de *design* (estética) e publicidade. A palavra estação possui o sentido do local onde se encontra.

Worm. Tipo de código malicioso. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores.

WWW - *World Wide Web* (teia em todo o mundo). Significa rede de alcance mundial. Consiste num sistema online em hipermídia (reunião de várias mídias interligadas por sistemas eletrônicos de comunicação e executadas na Internet), onde é possível acessar qualquer site para consulta na Internet. A Web usa, basicamente, três parâmetros: a URL, que especifica o endereço exclusivo de cada página; HTTP, que é um protocolo de transferência de dados; e, HTML, um método de codificação de como as informações devem ser exibidas aos usuários ou visitantes do site. Veja Internet e Web.

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, **X**, Y e Z.

XBT. Código ISO 4217 não oficial para representar a unidade monetária da bitcoin. Código da moeda informal para 1 bitcoin (definida como 100.000.000 satoshis). Algumas pessoas propuseram usá-lo para 0,01 bitcoin para evitar confusão com BTC.

XML - *eXtensible Markup Language*. Linguagem de marcação recomendada pela W3C - *World Wide Web Consortium* (principal organização de padronização da World Wide Web) para a criação de documentos com dados organizados hierarquicamente, tais como textos, banco de dados ou desenhos vetoriais. A marcação de um documento é como se define a estrutura, o significado e a aparência das informações no documento. Linguagem de marcação é um agregado de códigos que podem ser aplicados a dados ou textos para serem lidos por computadores ou pessoas. Alguns dos propósitos do XML são: auxiliar os sistemas de informação no compartilhamento de dados (especialmente via Internet),

codificar documentos e inserir seriais nos dados comparando o texto com o de outras linguagens baseadas em serialização. O princípio do XML é que ele pode ser lido por diversos tipo de software assim como se integra com inúmeras linguagens de programação, o que facilita sua leitura e escrita. O XML surgiu para suprir as deficiências e limitações do HTML (mas sem o substituir, apenas o complementar) no desenvolvimento de aplicações avançadas para a Internet; principalmente no que tange àquelas aplicações que precisam manipular um grande volume de dados. O XML e o HTML têm propósitos diferentes: o HTML é projetado para exibir dados e é focalizado em como os dados são apresentados, ao passo que o XML é projetado para descrever dados e é focalizado em o que os dados são. O arquivo XML é a versão digital da nota fiscal, sendo o formato utilizado para registro das informações relativas à NF-e (Nota Fiscal Eletrônica). Para que sejam lidos de forma apropriada os arquivos XML necessitam de leitores específicos (exemplos: Leitor XML, FreeNFE, XML Viewer, etc.).

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y e **Z**.

Zipar. Compactar arquivo de dados, para que possa ser mais facilmente transmitido pela Internet ou gravado em alguma mídia portátil (pendrive, HD portátil, CD, etc.). A palavra vem da extensão .zip de um dos programas de compactação mais usados (populares); o Winzip (http://www.winzip.com/win/bp/index.htm).

Zombie computer. Veja Computador zumbi.

ZULU Time. Trata-se do fuso horário europeu (UTC-0 Ocidental).

Confira outros dicionários em:

- Dicionário de Informática e Negócios: http://www.dicweb.com/;
- Definição de termos do mercado financeiro - http://www.infomoney.com.br/educacao/glossario/a;

- Dicionário Técnico de Informática: http://fasam.edu.br/wp-content/uploads/2016/06/Dicion%C3%A1rio-T%C3%A9cnico-de-Inform%C3%A1tica.pdf;

- Dicionário de Informática e Internet: http://comp.ist.utl.pt/aaa/Prog/Dicion%E1rio%20De%20Inform%E1tica%20&%20Internet%20Ingl%EAs-Portugu%EAs.pdf.

Gamer over (fim do jogo)!