ADLI TAKKAL BATAILLE
JACQUES FAVIER

Bitcoin

La monnaie acéphale

Préface de
JEAN-JOSEPH GOUX

CNRS EDITIONS

Présentation de l'éditeur

Voici le guide utile et pratique pour comprendre la méta-monnaie qui pourrait bien redéfinir en profondeur les règles de notre économie globalisée.

Créée en 2009, cette monnaie décrite par les uns comme virtuelle mais considérée par d'autres comme un véritable or numérique s'échange en pair à pair sur Internet en dehors du réseau bancaire traditionnel.

Quelles sont les propriétés spécifiques de cet objet numérique infalsifiable ? Quelles sont les caractéristiques monétaires d'un jeton informatique émis sans autorité centrale, sans banque, sans État ? Que nous dit Bitcoin des nouveaux usages économiques, de la cybercriminalité, de la société de surveillance ainsi que de l'évolution du cyberespace ?

Bitcoin accompagne en effet à la fois Internet dans son évolution et la société dans sa décentralisation, grâce à son architecture et à son registre, la blockchain.

La première grande synthèse en français, claire et accessible, sur la nouvelle monnaie du troisième millénaire.



Jacques Favier, normalien et agrégé d'histoire, a fait carrière dans la banque et l'investissement. Il anime le site « La Voie du Bitcoin ».

Adli Takkal Bataille, diplômé de linguistique, spécialiste du numérique, anime le site « Le Coin Coin. »

ADLI TAKKAL BATAILLE
JACQUES FAVIER

Bitcoin,
la monnaie acéphale

Préface de Jean-Joseph Goux

CNRS ÉDITIONS
15, rue Malebranche – 75005 Paris

© CNRS Éditions, Paris, 2017

ISBN : 978-2-271-11555-3

Ce document numérique a été réalisé par PCA

Sommaire

Préface de Jean-Joseph Goux

Introduction

I. Sidérant bitcoin

1- Une solution inédite pour un désir ancien

2- Un agencement génial, instrument de véritables exploits

3- Une création révolutionnaire cause d'enthousiasme ou de scandale

II. Le bitcoin, sans mystère ni fantasme

1- Esquisse de son ingénieux assemblage

2- Croquis des caractéristiques tant numériques que monétaires du bitcoin

3- Ébauche des usages hétéroclites du bitcoin

III. Histoire passée et présente d'une monnaie jeune, féconde et universelle

1- Une enfance difficile, une adolescence turbulente : le bitcoin dans la zone à risque

2- Bitcoin père de toutes les cryptomonnaies

3- L'entrée dans la vie active

Conclusion

Notes

Remerciements

PRÉFACE

de Jean-Joseph Goux

Dans l'Histoire déjà longue de la monnaie, l'invention du Bitcoin, cette monnaie numérique aujourd'hui encore controversée et expérimentale, apparaîtra très certainement comme un chapitre nouveau à la fois inéluctable, difficile, et chargé de multiples polémiques. Contrairement à la monnaie de compte qui fût sans doute à la base des premières opérations de calcul de type monétaire (pour les impôts par exemple), contrairement à la monnaie métallique circulante, frappée par l'État, dont les Grecs furent les inventeurs – et qui nous a été familière jusqu'à une époque encore très récente – le Bitcoin ou autres monnaies numériques (dites aussi *digitales*, électroniques, cryptographiques, etc.) semblent plus étrangères au sens commun, et en tout cas plus éloignées de l'idée traditionnelle de la « vraie » monnaie qui nous a été léguée jusqu'à ce jour par la culture gréco-romaine. Une véritable rupture, un profond bouleversement, est à l'œuvre, qui nous oblige à une révision complète de nos cadres mentaux. Les résistances à des innovations financières et monétaires ne sont pas nouvelles : la monnaie de papier, le chèque, la carte bancaire, sans parler pour l'instant de l'inconvertibilité des monnaies, ont rencontré de fortes oppositions, suscité des controverses farouches et nourri des angoisses persistantes. Rappelons simplement, parmi mille autres polémiques et réactions négatives, que certains citoyens, aux États-Unis, avaient dénoncé la monnaie de papier comme contraire à la constitution américaine après qu'elle a été perçue, ailleurs, comme un artifice diabolique.

Le Bitcoin ne fait pas exception. D'autant plus que les procédures, les protocoles qui permettent de faire fonctionner cette monnaie décentralisée que certains disent « virtuelle », ne sont pas toujours faciles à saisir du premier coup d'œil et à accepter sans réticences. Cette monnaie récente, qui n'existerait pas sans les possibilités du réseau Internet, ne fonctionne que par une médiation technologique assez complexe qui nous porte bien loin de l'échange direct de pièces de monnaie palpables, ou même de l'écriture bancaire d'un avoir.

Le mérite de l'ouvrage que publient aujourd'hui Jacques Favier et Adli Takkal Bataille est d'être une contribution, claire et détaillée, à une meilleure compréhension de cette monnaie numérique ; une *monnaie acéphale*, insistent les auteurs, car fonctionnant, ce qui n'est pas sa moindre originalité, sur la base d'un réseau sans organe central de contrôle et de gestion, ni la sanction et la garantie d'un tiers de confiance.

Comment cette monnaie, sans autre réalité que celle d'un code numérique chiffrant a-t-elle pu voir le jour ?

On peut dire que l'invention du Bitcoin est le couronnement une évolution historique relativement rapide à l'échelle de l'histoire des monnaies. D'abord, la disparition complète de la matière « précieuse » monétaire circulante au profit du signe monétaire, le billet de banque, qui est censé la représenter ; puis le passage de ce signe monétaire couvert, convertible, à un signe monétaire flottant ou inconvertible. Au lieu d'une conception substantialiste de la chose monétaire (l'or, l'argent), c'est une conception purement sémiotique qui a prévalu. Mais si la monnaie n'est qu'un signe, une sorte de langage, elle peut se communiquer comme un signe, moyennant, bien sûr, un certain nombre de procédures spéciales. Il ne manquait plus que quelques pas pour aboutir à la monnaie numérique. La transmission électronique des signes, par l'invention et la pratique généralisée d'Internet, a été la condition technique ultime qui a rendu possible cette innovation monétaire. À partir de ces deux conditions préalables (inconvertibilité bien acceptée du signe monétaire et transmission électronique de l'information, partout et instantanément) on a pu assister à une cristallisation rapide, conduisant à l'invention d'un protocole d'usage d'un nouveau type de monnaie, une monnaie numérique, qui répond aux caractéristiques traditionnelles de la chose monétaire tout en permettant des opérations que la monnaie traditionnelle ne permet pas. Le Bitcoin est le résultat à la fois scandaleux et inéluctable de cette évolution. À l'âge d'Internet, la mise en place de ce type

surprenant de monnaie n'est pas le moindre bouleversement qu'a apporté, et continue d'apporter, dans tous les domaines des pratiques sociales, ce mode nouveau de communication.

Un point décisif de rupture a donc été l'adoption de l'inconvertibilité du dollar annoncée par Nixon, le 15 août 1971. Il s'agissait de « suspendre temporairement la convertibilité du dollar américain en or », pour mettre fin aux spéculations qui visaient cette monnaie. L'inconvertibilité du dollar devenue permanente, et avec lui de toutes les monnaies, a changé en profondeur l'idée même du signe monétaire. Il fallait accepter l'idée qu'une monnaie peut exister sans être gagée sur quelque chose de « tangible », selon une expression souvent employée. En régime de convertibilité, on pouvait penser que le signe monétaire, le billet de banque, *représentait* une valeur stable, thésaurisée ailleurs, comme l'or, et à laquelle ce signe pouvait toujours renvoyer, tout comme un signe linguistique renvoie à un sens donné et, au-delà de ce sens à une chose stable et bien définie. C'est ce régime ou ce préjugé de la représentation qui est mis en cause par l'inconvertibilité. Ce n'est pas seulement une décision de technique financière et monétaire, mais avec elle un profond bouleversement de la notion de monnaie et de signe. La monnaie numérique naîtra en partie de ce bouleversement, une fois reconnu et bien accepté que la référence à quelque chose de tangible n'est pas nécessaire, ou même davantage encore, n'est qu'une illusion archaïque.

Comment cette acceptation est-elle possible ? Avec la notion d'une monnaie comme signe sans couverture, sans convertibilité, sans gage tangible, s'impose corrélativement l'idée qu'une convention partagée est la seule base de la valeur monétaire. Là encore l'analogie avec le langage est éclairante. De même que l'accord implicite et unanime des locuteurs, à l'intérieur d'une certaine communauté linguistique *fixe* et stabilise le sens des mots de la langue, de la même façon l'accord implicite des échangistes, partenaires économiques et commerciaux, institue une certaine unité comme monnaie, et tend à fixer sa valeur. Elle n'est qu'un signe, mais un signe reconnu, accepté, pratiqué, même si ce signe monétaire n'est pas gagé par une substance matérielle ou garanti par une instance extérieure. Il suffit de l'accord implicite de tous pour lui donner une valeur.

En ce sens on peut dire qu'une unité monétaire (et le signe qui la représente) a de la valeur parce que tout le monde pense qu'elle a de la valeur. On peut parler, de ce point de vue, d'une sorte de fiction. Mais l'acceptation unanime et mutuelle fait de cette fiction une réalité durable, qui ne manque ni de solidité ni d'usage pratique.

Cependant, à l'évidence, la transmission d'une information linguistique dans un réseau électronique, et la transmission d'une valeur monétaire posent des problèmes assez différents.

L'un des plus importants est la garantie qu'une certaine quantité d'unités monétaires électroniques ne pourra pas servir plusieurs fois. Contrairement au langage qui ne se supprime pas par la transmission, mais peut être répété sans dommages ni pour le destinateur ni pour le destinataire, les unités monétaires électroniques sont des signes ou des signaux que la transmission pour paiement doit épuiser, supprimer, car ils ne doivent pas pouvoir être réemployés. Tandis qu'un mot ne perd pas son sens à être transmis une ou plusieurs fois, un signe monétaire fait passer sa valeur à un nouveau détenteur, et il est perdu pour le premier détenteur. La propriété, l'avoir individuel, est une condition essentielle de la communication monétaire, que ne connaît pas la communication du sens par les mots du langage.

La sauvegarde de l'unicité absolue de l'opération doit donc être rigoureusement garantie. Ce problème majeur de la monnaie électronique a été résolu par le fameux dispositif de la *blockchain* de Bitcoin sur lequel les auteurs reviennent à plusieurs reprises. Les blockchains équivalent à des registres, des livres de compte infalsifiables, qui valident, enregistrent et datent rigoureusement chacune des opérations de transmission de pair-à-pair. Dès qu'un bloc de transaction est validé, il est ajouté au registre, accolé au bloc précédent, formant une chaîne ininterrompue de blocs, mémoire immuable et toujours consultable des opérations engagées.

Sans dissimuler les problèmes que peut poser cette monnaie encore jeune (y compris les risques d'usage criminel), sans rien cacher des controverses qu'elle continue d'alimenter, sans ignorer les hauts et les bas de son cours, Jacques Favier et Adli Takkal Bataille retracent, en un langage accessible, les différents procédures ou protocoles qui ont permis de mettre en place – depuis les idées astucieuses et fondatrices de l'énigmatique Satoshi Nakamoto en 2008, jusqu'au plus récents approfondissements – le système du Bitcoin et d'étendre de plus en plus ses usages. *Blockchains, hachage, minage*, ces procédures fondamentales caractéristiques du fonctionnement du Bitcoin, comme système électronique de paiement comptant entre pairs, sont abordées d'une façon éclairante et vivante, même si, bien entendu, toutes les plus difficiles complexités de ces opérations ne peuvent être développées dans ce livre aux dimensions limitées.

En même temps sont évoqués dans cette présentation dense et documentée du Bitcoin les multiples horizons ouverts, dans une dimension méta-économique, par l'exemple extrêmement prometteur de cet étonnant dispositif en réseau, sans organe central dirigeant, qui, pour ainsi dire, s'auto-administre lui-même.

INTRODUCTION

Dans les derniers mois de l'an 2008, le système financier mondial né au début des années 1970 parvenait à retrouver une assise au bord du gouffre par un transfert inouï, vers l'endettement public, des dettes et risques nés de l'activité débridée de la spéculation financière, puis par une politique de création monétaire sans précédent. Le monde reprit sa course effrénée à la croissance, qui malgré les prévisions du Club de Rome et leur bilan accablant quarante ans plus tard, ne cesse d'être prônée par des dirigeants à court d'alternative permettant de conserver leur emprise sur une société sujette à de grandes mutations tout en offrant un monde plus soutenable.

Le 1er novembre 2008, moins de deux mois après la faillite de Lehman Brothers, une note technique décrivait aux quelques centaines d'abonnés d'une obscure publication en ligne consacrée à la cryptographie une invention qu'il n'est pas possible de résumer techniquement en un mot mais qui s'est révélée à maints égards révolutionnaire : un protocole d'échange d'informations sans intermédiaires, un objet numérique non copiable, un livre de compte et d'enregistrement sans fonction centralisatrice et pourtant non-falsifiable, un mécanisme de confiance sans tiers de confiance et sans police, une unité de compte émise indépendamment de toute banque centrale ou commerciale, un possible instrument monétaire sans aucun lien avec une autorité souveraine quelconque.

Cette quasi-simultanéité empêche de considérer le protocole Bitcoin (avec un B majuscule) comme la réponse aux événements. Ceux-ci ont tout au plus précipité la publication de la note signée du nom de Satoshi Nakamoto[1]. Que celui-ci soit un homme ou une femme, américain ou japonais, unique ou collectif, est assez anecdotique. L'essentiel est qu'il avait, en ce 1er novembre, plus d'un coup d'avance sur ce que les événements manifestaient clairement ou suggéraient aux plus critiques des observateurs.

Quatre jours plus tard, alors qu'elle inaugurait le nouveau bâtiment de la *London School of Economics*, il revint à la reine Elizabeth de poser, avec l'élégance ingénue qui n'appartient qu'à elle, la grande question : pourquoi personne n'avait-il rien vu venir ? Le petit aréopage savant qui entourait Sa Gracieuse Majesté ne put sceller un embarras hébété. En France, le président Sarkozy affirmait que personne ne pouvait voir venir la crise. Bien des gouvernants, bien des financiers répétèrent ce genre d'assertions, qui ne donnaient d'indications que sur le spectre étroit de leurs fréquentations et de leurs lectures. En réalité, il est aisé de retrouver tous les avertissements publiés durant des années, et qui furent loin d'être exclusivement le fait des critiques hétérodoxes. Pourtant, pour l'essentiel, la littérature critique visait à dénoncer les « excès » du système, ou ses « dévoiements » : trop de spéculation et pas assez de contrôle, pour faire simple.

Les critiques les plus hardies pointaient deux limites, l'une écologique, l'autre sociale. Si l'on a simultanément trop de gaspillage de ressources non renouvelables et trop d'inégalités, autant dire que les ressources naturelles ne servent plus qu'à payer les frais financiers. Au-delà de cette critique, il reste le choix de prôner l'austérité ou celui de mettre en cause la nature de la « monnaie-dette » et sa création *ex nihilo* par des banques commerciales. L'essentiel de la critique doit donc être une « méta-critique » : c'est le paradigme actuel dont il faut rechercher les ressorts cachés. Seule une réflexion sur les mécanismes du système eux-mêmes peut amener une remise en cause réelle de celui-ci (et non pas des pratiques exercées en son sein et qui en découlent) et une ouverture vers de possibles r-évolutions d'ordre systémique, tel que l'est le sujet de ce livre.

Or le sujet de la monnaie, de sa nature et des conditions de sa création, n'avait pas suscité la publication d'une littérature critique comparable, par sa masse ou sa réception publique, à la production des études sur la crise à venir. Cela permet de comprendre la vacuité ou la naïveté des premières réactions quand il apparut que le

bitcoin, objet non identifié venu d'ailleurs, pouvait peut-être cumuler plusieurs des attributs d'un instrument monétaire. « Le bitcoin, entendit-on alors répéter en boucle, n'a aucun fondement, n'est basé sur rien, n'est régi par aucune autorité et n'est garanti par personne. » Certaines critiques revêtaient un caractère comique, comme celle déniant au bitcoin une valeur fondamentale et ne lui reconnaissant qu'une simple valeur de marché, comme si le dollar ou l'euro avaient valeur intrinsèque et non l'un au regard de l'autre et chacun par sa capacité d'acquérir des biens sur des marchés. On entendit certains parler de ces devises flottantes comme si elles étaient encore grosses d'or. Aussi imprudentes ou impudiques étaient les critiques reprochant au bitcoin de n'être pas émis par une banque centrale, quand il apparaît que 90 % de la création monétaire est aujourd'hui le fait des banques commerciales, qui créent bel et bien *ex nihilo* la monnaie qu'elles prêtent à leurs clients. La distinction entre ce qui est fiduciaire et ce qui est scriptural passait parfois à la trappe dans les raisonnements. Obscènes enfin, les critiques soulignant l'absence de garantie dont bénéficient les détenteurs de bitcoin quand on songe à la modicité des divers « fonds de garantie » constitués pour garantir un système dans lequel, fondamentalement, l'argent des déposants n'est qu'une écriture au passif des banques, et surtout lorsqu'il est apparu en mars 2013 que l'Union européenne pouvait ponctionner directement les comptes en banque (à Chypre pour commencer) sans autre forme de procès.

Comme il arrive souvent, l'irruption d'une nouveauté radicale permet un examen critique non moins radical de ce qui, sans solution alternative adéquate, passait aisément pour naturel.

Le bitcoin est loin d'être la première « nouvelle monnaie » apparue dans (ou contre) le « système » des changes flottants, état de fait instauré de façon toute empirique au début des années 1970. On avait vu les monnaies locales ou complémentaires, monnaies-heures, coupons ou « *miles* », monnaies émises par des sociétés, monnaies électroniques des jeux en ligne théoriquement destinées à demeurer dans les univers virtuels de ces jeux. Aucune de ces monnaies n'avait prétendu à l'universalité, aucune ne pouvait assumer toutes les fonctions d'une monnaie, pour tous et partout. Telles étaient en revanche les ambitions des prédécesseurs du bitcoin : l'e-Gold, le Liberty Reserve, le dollar Linden de Second Life, la WebMoney, le b-money, le bitgold, qu'elles aient existé concrètement ou sur le papier. Certaines étaient nées comme des complots dans le milieu de ceux qui s'intitulèrent les *cypherpunks*, mais d'autres projets fort similaires étaient élaborés dans les bureaux de la Citibank. Aucune ne répondait à la totalité des ambitions d'une monnaie universelle, fluide comme le cash, confidentielle mais sûre, indépendante de tout pouvoir, adaptée au nouveau monde d'Internet. Aucune ne représentait une réalisation aussi parfaite que le bitcoin, même si la question de la soutenabilité de son réseau n'est pas encore élucidée et reste sujet à controverse.

L'invention de novembre 2008 n'a d'abord été reçue que par une toute petite communauté, sur une base largement ludique. Le medium Internet étant encore plus mythologique que le medium télévision, l'essor de l'unité de compte bitcoin (avec un b minuscule) comme une « monnaie » mêla des moments épiques. Entre autres, celui de la fameuse pizza représentant la première transaction avec le monde réel. Ou encore des aventures illicites comme celle de la Route de la Soie où l'anonymat de la monnaie nouvelle, un peu vite jugé total, fit croire à certains qu'elle serait l'instrument idéal de transactions inavouables. Enfin, des désastres classiques comme celui de la faillite de MtGox, que les détracteurs du bitcoin évoquent rituellement bien qu'elle n'illustre pas la faiblesse de la nouvelle monnaie, dont chacun peut et doit garder la clef pour soi, sinon celle du vieux modèle d'établissement qui prétend en prendre soin pour le compte de ses clients.

Soudain, en 2013, la spéculation s'en mêla. On entendit du côté des puissants et des doctes des cris d'orfraie, comme si leur propre système abhorrait la spéculation. Elle retomba. On entendit des prophéties : la farce était jouée. Naturellement, on parla de Ponzi, ce qui, en matière d'argent, est un peu le point Godwin de l'invective. La mort du bitcoin fut annoncée près d'une centaine de fois par diverses autorités, prix Nobel compris, bien sûr.

À l'automne 2015 un nouveau crédo se fit soudain entendre : le bitcoin était une chose sans intérêt que l'on aurait bientôt tué s'il ne mourrait pas tout seul, mais son livre de compte décentralisé, nommée *blockchain*, allait révolutionner la finance. Ce serait bien sûr des blockchains privées, sur lesquelles seules les grandes banques appartenant à un consortium *ad hoc* pourraient échanger leurs monnaies et leurs actifs. D'une chose publique et ouverte (*open source* et *open data*) il suffirait de faire une chose privée et fermée. D'une chose sécurisée par l'intérêt (gagner des bitcoins en entretenant le système) il suffirait de faire un club de connivence pour ôter son venin à l'invention et la rendre bienfaisante, c'est à dire utile au système dont le projet était justement, à l'origine, de se passer. Cette idée enthousiasmait tous les néophytes, rassurés par des analyses de seconde ou troisième main, et qui ne se rendaient pas compte que très peu de développeurs semblaient y accorder la moindre foi.

Quand on eût bien annoncé que le bitcoin était mort, survinrent des attentats qui permirent de dire qu'il en était la cause, et qu'il fallait en finir avec « l'Internet invisible », les messages codés et les monnaies non régulées, coupables de tant de mal.

E pur, si muove… Des centaines de milliers de gens ont une « adresse Bitcoin » (que l'on peut assimiler à un « compte Bitcoin »), des milliers participent activement, comme développeurs ou entrepreneurs, à cette aventure toute récente mais déjà grosse de quelques milliards de dollars. Au-delà de cette somme – relativement légère pour un système monétaire d'envergure mondiale, mais non négligeable si on assimilait l'aventure à celle d'une start-up –, il convient de voir que dans toutes les grandes villes du monde, au travers de *meetups*, se réunissent régulièrement des gens, jeunes, moins jeunes, éduqués et actifs, qui explorent ensemble ce que Bitcoin permet ou promet. Si le cours du bitcoin en dollars et en euros reste volatile (mais moins que jadis), la courbe du nombre de transactions quotidiennes monte inexorablement, et sans grands à-coups.

Par où commencer ?

Le bitcoin, sujet aujourd'hui incontournable, reste le plus souvent abordé naïvement et négativement par ceux qui pourraient y perdre, ou de façon à la fois messianique et trop technique par ceux qui développent son environnement. Or tel qui porte sur lui une carte de crédit peut souhaiter réfléchir sur son usage et ce qu'il implique, même s'il ne sait pas expliquer savamment son fonctionnement ou ne peut pas disserter sur la congruence sur les nombres entiers qui sous-tend la cryptographie de type Rivest, Shamir et Adleman. Les aspects très techniques ont été nécessairement simplifiés, et renvoyés aux notes de fin de volume. Toutefois, en ce qui concerne le bitcoin, deux efforts intellectuels s'imposent, tous deux à la portée de chacun.

Il faut d'abord consentir un effort conceptuel. Voltaire fait quelque part la remarque que les gueux reçoivent les signes monétaires comme les sacrements, sans trop d'examen. Keynes écrivait de son côté qu'on adopte plus facilement une nouvelle idée qu'on ne se débarrasse réellement des « idées anciennes qui ont poussé leurs ramifications dans tous les recoins de l'esprit des personnes ayant reçu la même formation que la plupart d'entre nous[2] ». Le bitcoin, pour qui veut dépasser les critiques prudhommesques, exige une capacité réelle d'abstraction mais aussi et surtout de remise en cause. Sur la nature de l'argent – il n'est ni ce morceau de papier dans les portefeuilles, ni conservé au frais dans le sous-sol des banques pas même à Frankfort – mais aussi la nature de la communauté qui en reconnaît le signe, sur l'espace où il circule, un rhizome géographique et dématérialisé, sur les rapports qu'il entretient avec ce qui tient lieu de souveraineté.

Bitcoin, et derrière lui les crypto-monnaies désormais possibles – puisque tout est en « open source » –, vont changer de manière radicale la nature et la circulation de l'argent, mais aussi multiplier les possibilités, bousculer les contraintes et les mœurs des sociétés. Bitcoin ouvre de nombreuses manières nouvelles d'échanger de l'argent mais également des titres, des contrats, des promesses, des informations…

Quelques considérations sur la monnaie seront aussi inévitables, d'autant plus que l'apparition du bitcoin a considérablement soulevé la poussière autour de l'idole !

Il faut ensuite consentir un effort intellectuel : on ne peut éluder un peu de technique ou de science, sachant toutefois que le bitcoin, chef d'œuvre d'agencement de plusieurs idées, n'est pas proprement dit une révolution scientifique. L'essentiel des mathématiques mises en œuvre date de plusieurs décennies, et ceux qui n'y ont pas accès peuvent en percevoir intuitivement l'effet par quelques analogies poétiques : là où le monde nous abreuve d'informations, nous sommes de plus en plus sujets à des réminiscences proches de celles avancées par Platon. Il n'est pas indispensable d'intimider le lecteur avec les détails de la cryptographie à courbes elliptiques ou avec la recherche du logarithme discret.

Le lecteur ne fera donc pas l'économie d'un peu de technique et de vocabulaire nécessaire. Juste ce qu'il faut pour comprendre avant de réfléchir ou de critiquer. Et seulement après avoir saisi, dans les premiers chapitres, ce qui rend cette chose inconnue tellement désirable à ceux qui l'ont déjà comprise.

Nous avons donc choisi de ne pas présenter ces explications techniques en première partie, comme d'autres auteurs l'ont fait à l'étranger, ou comme les conférenciers le font trop souvent. Rien n'empêche le lecteur technophile de commencer notre livre par sa deuxième partie, mais le lecteur simplement curieux risquerait, à commencer par la technique, de se décourager faute de saisir les raisons de l'effort intellectuel à consentir. Sans

doute nos ancêtres ont-ils été émerveillés de lire l'heure au cadran et de rouler à 100 kilomètres par heure avant (pour certains) de tenter de démonter la montre ou le moteur.

Une fois les bases techniques affermies, le lecteur pourra commencer de se poser de vraies questions financières, et même sociologiques. Le bitcoin est une « monnaie rare », une chose tout à fait opposée aux pratiques actuelles de « Quantitative Easing », mais que ses défenseurs considèrent comme une force. Ont-ils raison de voir dans son extrême divisibilité une réponse suffisante à cette rareté ? Quelle vison du monde reflète ce choix de la rareté monétaire ? Révolution technique et (surtout ?) sociologique, le bitcoin est-il pour autant « révolutionnaire » ? Monnaie potentiellement déflationniste (comme l'or à l'image duquel il a été forgé, conçu pour être rare) le bitcoin est-il pour autant « réactionnaire » ? C'est dans cette alliance de concepts paradoxaux que s'est construit techniquement le bitcoin et qu'il doit être questionné sociologiquement. L'examen de ses paramètres monétaires suggère (comme la mythologie du « minage ») la comparaison avec une sorte d'or numérique, mais cette comparaison classique ne saurait rendre compte du bitcoin dans sa richesse conceptuelle et la multiplicité de ses utilisations possibles.

Or, dans son état actuel, le bitcoin ne pourrait probablement pas se saisir concrètement, dans la « vraie vie », de tous les usages envisageables, et encore moins tous à la fois. Qu'il puisse servir à tout (ce qui est l'objet d'un débat) n'implique pas qu'il puisse trouver sa place comme monnaie universelle bien qu'il ait constitué, avec peut-être plusieurs millions de « bitcoineurs », ce qui est pour l'instant la première communauté monétaire alternative au monde. Plusieurs futurs sont encore possibles.

Nous proposons ensuite, dans notre troisième partie, un parcours de type « historique » traitant, pour commencer, des questions qui se sont posées dans les premières années d'expansion de la sphère Bitcoin. Ainsi, la déroute de MtGox permet d'exposer les questions de sécurité liées à la centralisation, celle de la Silk Road de poser les limites de l'anonymat et les enjeux de la cyber-surveillance, la crise de Chypre de montrer que les fragilités ne sont pas toutes du même côté.

Compte tenu de la richesse de la littérature existante sur ce qui touche à la « décadence sécuritaire » ou à la surveillance de masse, il ne nous a pas semblé utile de nous disperser sur ces thèmes, sans pour autant s'interdire de les aborder avec parcimonie. Tout en sachant que ces mêmes thèmes sont devenus centraux à partir de l'instauration de l'état d'urgence en France. Ils sont implicitement présents quand on traite de Bitcoin à l'heure où les autorités entendent supprimer le cash dans certains pays, interdire le chiffrement et dans d'autres bloquer l'argent en banque. Né dans l'univers de la cryptographie, Bitcoin, même adopté par les *venture capitalistes*, même adopté par les *fintechs*, reste un outil de disruption, si ce n'est de subversion.

La croissance continue des échanges, l'injection importante d'argent par les fonds d'investissement dans l'écosystème du bitcoin, l'imagination des développeurs, le climat un peu messianique qui règne dans leur communauté, multiplient les développements possibles en termes d'échanges directs, sans tiers de confiance. Au-delà des usages monétaires de la « devise » bitcoin, on ne doit donc pas perdre de vue l'ensemble de ce que le protocole Bitcoin peut apporter. La crise des banques chinoises permet d'expliquer le partage de pouvoir entre les « nations » dans le bitcoin, l'introduction d'une *blockchain* dans le NASDAQ permet d'envisager la question de l'utilité du bitcoin dans la finance.

Ainsi, l'entrée (encore timide, souvent masquée) du bitcoin dans « la cour des grands » permet finalement d'envisager différents *scenarii*, entre l'utopie d'une disruption généralisée – y compris des disrupteurs d'aujourd'hui – et l'apparition d'un monde de machines contractant entre elles ou se possédant les unes les autres.

Quelques mots sur les auteurs

Nous avons écrit ce livre, en constant dialogue, à quatre mains et à deux générations. Nous sommes tous les deux des auteurs et conférenciers spécialisés sur le bitcoin, mais nous sommes également actifs dans la communauté du bitcoin francophone, que ce soit comme animateurs de *meetups*, de rencontres diverses ou fondateurs d'une Association originale, le « Cercle du Coin » qui regroupe près de 70 acteurs francophones dans une demi-douzaine de pays. Surtout, nous partageons la conviction que si la mathématique et la technique changent le monde, la réflexion assise sur les sciences humaines, l'histoire et la philosophie ont vocation à le rendre intelligible.

Ce livre, dont la rédaction a été achevée au tout début de l'année 2017, dans de fortes turbulences du cours, ne cherche pas à convaincre le lecteur d'adopter le bitcoin au-delà d'un usage pédagogique, et moins encore à lui vanter les mérites d'une plateforme particulière pour en acheter, d'un *wallet* pour en conserver l'adresse, d'une carte pour s'en servir. Notre but est de permettre au lecteur d'en cerner et d'en comprendre les enjeux, techniques ou politiques.

Pour l'inciter à poursuivre la découverte, quelques vignettes de type QR (pour *quick response*) sont disséminées dans le corps de l'ouvrage pour être « flashées » par un téléphone portable ou un ordinateur et emmener le lecteur vers des informations complémentaires, des articles, des conférences, de petits films.



« La Voie du Bitcoin », le site de Jacques Favier



« Le Coin-Coin », le site d'Adli Takkal Bataille

Le site http://bitcoinlamonnaieacephale.fr met en ligne les liens cités dans les notes, ainsi qu'un forum permettant l'échange entre lecteurs et auteurs.

Quelques mots sur le titre de notre livre

Pile ou face, *heads and tails* en langue anglaise. La pièce de monnaie porta, pratiquement depuis sa naissance, l'effigie d'une divinité tutélaire ou d'un souverain dont la puissance garantissait la valeur de « sa » monnaie. Puis il y eu un glissement vers les allégories et les symboles de la Nation et des valeurs dont celle-ci se sentait investie. Chacun reconnaît, fût-ce inconsciemment, la face du Léviathan, le pouvoir des institutions et de leur bureaucratie, sur les pièces et sur les billets de banque.

Le bitcoin, dont la représentation graphique la plus communément admise est un simple ₿ dans un cercle orange, n'a point d'effigie puisqu'il n'a matériellement ni pile, ni face. Ceci le distingue des vieilles monnaies, mais non des devises électroniques comme le sont déjà les « miles » et comme le seront les unités de compte des portefeuilles des géants du Web ou de la téléphonie.

Si le bitcoin n'a point de portrait gravé, c'est aussi parce qu'il n'a pas, non plus, de « chef ». Le mot français, comme le mot latin dont il provient, désigne à la fois la tête d'un corps vivant et la personne qui exerce l'autorité sur un corps social. Or nul ne peut désigner un roi, un propriétaire, un chef de Bitcoin.

En ce sens le bitcoin est une monnaie sans tête, *acéphale* pour le dire en grec. Mais c'est aussi bien plus qu'une monnaie…

I

Sidérant bitcoin

1- UNE SOLUTION INÉDITE POUR UN DÉSIR ANCIEN

Des débuts d'Internet jusqu'au Bitcoin : un chemin monétaire tortueux

Comme l'Amérique, Bitcoin ne fut pas découvert ou inventé en un jour. Le monde était engagé dans une vaste tâche d'exploration, non plus de la vaste mer et de nouveaux continents mais du cyberespace, un territoire à part entière. Celui qui y réfléchit peut reconnaître presque mot à mot la réflexion de Montaigne au XVI^e^ siècle : « Notre monde vient d'en trouver un autre (et qui nous garantit que c'est le dernier de ses frères, puisque les Démons, les Sibylles et nous, avons ignoré celui-ci jusqu'à cette heure ?) non moins grand, plein et fourni de membres que lui, toutefois si nouveau et si enfant qu'on lui apprend encore son a, b, c. »

Qu'est-ce qu'Internet ? C'est non pas un réseau unique sur lequel des milliards d'hommes se connecteraient mais un réseau de millions de réseaux (publics, gouvernementaux ou privés, universitaires, commerciaux). Cet immense flot d'informations circule sans centre postal et sans route unique et constante que suivraient les messages, comme les trains ou les avions peuvent le faire pour transporter des plis, ou comme les fils télégraphiques transmettaient le morse. Les informations, ou plutôt des petits paquets d'informations, circulent entre les nœuds du réseau sur la base de protocoles communs (TCP, IP) pour la publication (HTTP) ou l'échange (SMTP). Ces protocoles, dits « ouverts », sont, comme l'alphabet, devenus des biens communs de l'humanité. Ils assurent l'unité et l'intelligibilité du cyberespace. Par ailleurs, les paquets circulant à l'aide de ces protocoles doivent être traités indistinctement par ceux qui les transportent : c'est la neutralité du net.

L'apparition de l'Internet ne fut pas un simple progrès technique. Comme l'écriture qui nous fit sortir de la préhistoire, l'imprimerie entrer dans le monde moderne, ou encore les télécommunications qui l'unifièrent à l'époque contemporaine, l'Internet change non seulement le monde mais aussi l'être humain lui-même dans sa façon de se représenter le monde. Aussi l'opposition déjà ancienne entre le *réel* et le *virtuel* est-elle de moins en moins pertinente. Lorsqu'un individu s'écrie que telle ou telle chose se fait ou ne se fait pas *dans le vrai monde*, c'est souvent qu'il est simplement mal informé[3], mal à l'aise (et donc un peu malheureux) dans ce monde nouveau. Définir le bitcoin comme une monnaie *virtuelle* s'inscrit dans ce malentendu. Il ne faut pas confondre le réel et le tangible, le virtuel et l'intangible.

Le cyberespace n'est pas un simple prolongement de l'espace physique. On peut bien sûr y acheter des chaussures dont on fera usage dans la rue, mais aussi des accessoires de jeux qui ne serviront qu'à jouer dans le cyberespace. On peut y échanger sur des réseaux sociaux avec des proches ou pour susciter des rencontres réelles, mais on peut aussi échanger avec des gens qu'on ne connaîtra jamais réellement, par exemple dans le cadre d'une communauté ludique. Certains univers ludiques, notons-le, eurent leur propre monnaie avant Bitcoin.

Le cyberespace tend à s'autonomiser. Certes le *cloud* n'existe que métaphoriquement et l'information à laquelle on accède, la trace des échanges que l'on entretient, tout cela se trouve physiquement dans les serveurs géants de firmes géantes, serveurs localisés sur le territoire d'un État. Certes le fournisseur d'accès à l'Internet est sur le territoire d'un État donné et soumis à sa juridiction. Mais l'expérience de l'internaute est toute autre, faite

d'avatars à pseudonymes et d'absence de frontières. Elle donne un grand sentiment de fluidité, d'autonomie – parfois d'impunité.

Pourtant une chose demeurait bien peu fluide sur Internet : l'argent. Plusieurs années avant Internet apparaissait la carte à puce, qui connut un succès mondial. Dans un monde où 90 % de notre argent est conservé dans les banques, non sous forme de billets dans des coffres mais sous forme d'écritures dans leurs livres, la carte à puce rendait son usage électronique presque aussi fluide que celui du cash pour payer, du moins dans les magasins.

En revanche, en ligne et, pire encore, en situation de mobilité, malgré quelques améliorations, la carte à puce reste d'un usage peu pratique et très peu sûr. Le développement du e-commerce puis du m-commerce ne pouvait rester sans conséquence sur les moyens de paiement. L'idéal serait que le téléphone mobile contienne du cash plutôt qu'une borne d'appel. Ce serait en quelque sorte se réapproprier localement le *cloud*.

Certains avaient perçu de longue date ces mutations au sein même du système bancaire. On doit notamment un grand nombre d'éléments constitutifs du génial assemblage du bitcoin à David Chaum, un cryptologue universitaire américain particulièrement fécond. Avant Internet et les *cypherpunks,* celui-ci avait déjà publié la description d'un *cryptographic system for untraceable payments*. En 1990, il créa son e-cash. Visionnaire mais convaincu qu'il fallait traiter avec les institutions existantes, il fonda sa société Digicash pour promouvoir son système de monnaie cryptographique permettant au payeur de maintenir son anonymat tout en identifiant clairement celui auquel il envoyait un paiement sans passer par une institution intermédiaire. Quand David Chaum exposait son système, en particulier aux autorités et aux banques centrales, il insistait sur ce qu'il présentait comme un facteur de transparence. Il commença à se faire entendre, signa des accords avec le gouvernement néerlandais pour le paiement des péages routiers et avec de grandes banques comme la Deutsche Bank, le Crédit Suisse ou Sumitomo. Il engagea avec Microsoft et Visa des discussions qui n'aboutirent pas. Le château de cartes s'effondra et Chaum se retrouva éjecté de sa société peu avant d'ailleurs qu'elle ne finisse en faillite vers la fin de la décennie 1990. Quelles qu'aient pu être ses fautes de management, il apparaît clairement que les idées de Chaum (transactions directes, anonymat, absence d'intermédiaires de paiement) étaient bien trop en avance sur l'époque, qui était celle du premier développement du e-commerce.

Pourtant, tout en maintenant son contrôle sur les paiements en ligne, le monde bancaire cherchait la monnaie du nouvel âge numérique. Dès les années 1990, bien avant que l'on puisse acquérir en ligne des objets numériques, certains imaginaient la monnaie numérique pour les acheter. C'est là qu'intervient une aventure menée au sein de Citibank. Sholom Rosen y développa au début des années 1990 le *Electronic Monetary System* qui visait à doter les États-Unis d'une nouvelle monnaie. Citibank lui en donnait les moyens : des chercheurs du MIT, de Stanford et de Berkeley furent consultés. Les unités de compte autonomes de cet e-cash étaient déjà des instruments de paiements sans intermédiaires nécessaires alors que Rosen lui-même n'imaginait pas vraiment déconnecter une monnaie du système bancaire. En fait, Rosen inventa une forme de cash électronique que les banques commerciales pourraient émettre comme elles créaient de la monnaie scripturale en consentant des crédits. En 1997, le Département du Trésor américain accepta de tester son système sur une assez grande échelle. Et puis un jour, avec la fusion de Citibank et de *Travellers*, l'expérience fut arrêtée. Trop innovante, elle ne s'inscrivait plus, sans doute, dans la nouvelle stratégie de concentration et de maximalisation de la rente des paiements par carte. Comme souvent, le succès d'un produit ingénieux dépend avant tout de son contexte.

Que la fusion à l'origine de Citigroup soit la cause d'un désastre sans précédent (il fallut pour la rendre possible revenir en novembre 1999 sur le Glass-Steagall Act et permettre ainsi la constitution de monstres *too big to fail*) révèle le parallélisme des calendriers.

Dans les mêmes années, les banques recrutèrent massivement des mathématiciens pour faire du trading algorithmique et élaborer des produits « miraculeux » à partir de collectes de données personnelles et d'analyses quantitatives de plus en plus opaques, menant à une évaluation béate de produits dont nul ne connaissait plus le risque. Mais en ce qui concerne le commerce en ligne, l'effort des banques consista essentiellement à adapter le système de paiement par cartes au nouvel eldorado, au prix d'un coût croissant de la fraude en ligne. D'autre part, de nouvelles solutions allaient apparaître, notamment PayPal, en 1998, qui convenait très bien au commerce en ligne de type eBay, tout en ne remettant guère en cause le système bancaire et l'oligopole Visa-Mastercard. La gestion de la confiance en ligne sur les plateformes de type eBay s'appuyait sur la notation par les acheteurs et les vendeurs. Et le tiers de confiance que devenait PayPal se présentait comme une double assurance pour les acheteurs et les vendeurs débutants souffrant d'une réputation inexistante. Il faut rappeler qu'aux débuts d'eBay les vendeurs choisissaient autant leurs acheteurs que les acheteurs leurs vendeurs.

Revenons au sentiment d'autonomie développé par l'internaute. Le moins que l'on puisse dire est qu'il s'accommodait mal de ces options, et notamment de l'archivage bancaire des données tant pour des raisons de principe que de sécurité. Pour ces deux raisons, Internet cherchait aussi son cash en dehors du système bancaire : quelque chose que l'on aurait dans la poche et que l'on transfèrerait en le posant sur le comptoir, sans jeu d'écriture ou intervention d'un tiers.

À partir du début des années 1990, des propositions et des expériences firent surface. Celles-ci s'appuyaient sur des travaux de cryptographie datant parfois des années 1970, sur lesquels nous reviendrons, et sur un ensemble d'innovations plus récentes liées à l'essor des échanges sur Internet. Les premières notions d'horodatage d'un document numérique par inscription dans une chaîne cryptographique furent proposées en 1991 et 1993 par Haber et Stornetta. En 1997, Adam Back proposa, en réalité pour gêner les spammeurs d'e-mails, le Hashcash, aujourd'hui connu comme le principe de la « preuve de travail » dans le système bitcoin : à défaut de prouver son identité ou son innocence, un participant d'un réseau peut fournir la preuve que sa participation est d'un coût suffisant pour être jugée sérieuse.

En novembre 1998, le chercheur en informatique et *cypherpunk* américain Wei-Dai publia un papier décrivant son système de monnaie électronique anonyme « b-money », permettant des transactions directes (dites pair-à-pair ou P2P, c'est à dire sans intermédiaire de type bancaire). Y est formulée l'idée d'émettre de la monnaie pour compenser le coût supporté par les participants au système afin de fournir leur « preuve de travail ».

Nick Szabo, sorte de génie touche à tout, proposa dans un article de blog vers 2005 un système, le bit-gold, de création de « preuves de travail », difficiles à produire et donc rares, échangeables comme des unités monétaires. La sécurité de son système fut ultérieurement jugée moindre que celle du Bitcoin, dont il est suspecté par plusieurs bons connaisseurs d'être le mystérieux inventeur.

La même année, le développeur canadien Ryan Fugger lançait Ripplepay (prédécesseur du protocole de paiement Ripple, toujours considéré comme un rival sérieux de Bitcoin, au moins pour le monde bancaire). Son intention était de créer un système monétaire décentralisé permettant aux individus et aux communautés de créer leur propre monnaie de façon efficace.

Le mystérieux Satoshi Nakamoto affirma avoir travaillé à partir de 2007 à son projet. Parlant de sa découverte, Marc Andreessen (l'un des fondateurs de Netscape) déclara : « je me suis toujours demandé ce qui se serait passé si l'on avait fourni dès le début une solution de paiement en un seul clic intégré au navigateur. Avec Bitcoin, on a enfin trouvé cet Internet de la Monnaie[4] »

Bitcoin, un projet sociétal autant que technique : se passer d'intermédiaires et d'autorité

Nous avons déjà évoqué plusieurs fois le terme de *cypherpunks*. En dehors d'un tout petit monde, il n'est guère d'emploi courant. Le mot, bricolé en 1992 pour quelques personnes se réunissant à San Francisco, alliait une allusion au chiffrement avec le terme de *cyberpunk* qui désignait au début des années 1980 un genre (romans, mangas, BD, musique, jeux vidéo…) mêlant des éléments de science-fiction à base d'informatique et de génétique dans une atmosphère de dystopie où il n'y a *no future*. Des films comme *Blade runner* ou *Matrix* permettront de situer le mouvement auprès du plus large public.

Quant aux premiers *cypherpunks*, ils étaient surtout intéressés par la cryptographie, tant d'un point de vue scientifique que pour assurer concrètement, et non par de simples démarches juridiques, le respect de la vie privée. De quelques centaines au début des années 1990, leur nombre aurait atteint 2000 en quelques années. Sans faire une présentation détaillée du mouvement, deux de ses figures les plus connues donnent une idée des voies que prit ce mouvement.

Philip Zimmermann publia, quelques mois avant l'apparition du mot *cypherpunk*, sa première version de *Pretty Good Privacy*, un logiciel gratuit de cryptographie. Du point de vue de son créateur, « si l'intimité est mise hors la loi, seuls les hors-la-loi auront une intimité. Les agences de renseignement ont accès à une bonne technologie cryptographique. De même les trafiquants d'armes et de drogues. Mais les gens ordinaires et les

organisations politiques de base n'avaient pour la plupart pas eu accès à ces technologies cryptographiques de « qualité militaire » abordable[5]. »

PGP avait la réputation d'être la solution la plus sûre au monde. Le gouvernement américain réagit avec beaucoup de suspicion, assimila sa commercialisation à l'étranger à une exportation d'armes et ouvrit une enquête. Bien avant le 11 septembre qui servit de prétexte au *Patriot Act*, l'idée que des citoyens protègent leurs messages était déjà suspecte. Zimmermann formula une comparaison assez triviale, mais utile pour recadrer les choses : « Que se passerait-il si tout le monde estimait que les citoyens honnêtes devraient utiliser des cartes postales pour leur courrier ? Si un non-conformiste s'avisait alors d'imposer le respect de son intimité en utilisant une enveloppe, cela attirerait la suspicion. Peut-être que les autorités ouvriraient son courrier pour voir ce que cette personne cache… »

Julien Assange allait, lui, se rendre célèbre non en œuvrant à la protection des secrets du citoyen, mais en entreprenant de diffuser ceux des gouvernants pour corriger l'asymétrie d'information entre les uns et les autres. Il avait, à la fin des années 1990, développé des systèmes de cryptographie. En 2006 il fondait l'ONG WikiLeaks qui diffusa des millions de documents secrets tant iraniens ou chinois qu'occidentaux.

En parlant d'*asymétrie d'information*, Julien Assange reprenait un terme qui, en finance, constitue une inefficience grave que les institutions ont à cœur de combattre. Il ne s'agissait pourtant pas pour lui de corriger un système économique paré de toutes les vertus mais de combattre un état de fait politique qu'il jugeait détestable. « L'organisation de fuites » déclara-t-il, « constitue une action intrinsèquement anti-autoritaire ». La diffusion de plusieurs vagues de secrets, y compris des mensonges des dirigeants, sensibilisa plutôt l'opinion. Mais du point de vue de ces dirigeants, c'était un acte d'espionnage qui arrachait des cris indignés à des politiciens de tous bords. Le blocage des comptes bancaires de WikiLeaks fut une première mesure d'asphyxie.

Or le combat des *cypherpunks* n'ignorait pas la réalité du contrôle (au double sens de surveillance et de possibilité d'interrompre) exercé sur la monnaie et les paiements.

À vrai dire, dès 1982, David Chaum, déjà évoqué au chapitre précédent, écrivit un texte proposant un système pour des paiements impossibles à tracer. Il citait la liste des paiements dont il entendait assurer la confidentialité : transports, hôtels et restaurants, spectacles, nourriture, médicaments, alcools, livres, revues et journaux, dons aux œuvres politiques ou religieuses. Soit l'inventaire complet de tout ce qui est aujourd'hui susceptible d'être espionné.

Dix ans plus tard, Tim May, un ingénieur et scientifique de la société Intel, publiait son *Manifeste Crypto-Anarchiste*[6], un texte jusque-là semi-confidentiel d'abord distribué lors de la conférence « Crypto 88 » et présenté comme une adresse aux anarchistes traditionnels, suggérant les possibilités d'action immédiate offertes par la cryptographie : anonymisation des échanges, contournement des lois sur la propriété intellectuelle, piratage des systèmes de contrôle autoritaire. Un an plus tard, en 1993, le *Manifeste d'un Cypherpunk* du mathématicien Eric Hughes[7] reprenait les mêmes thèmes.

Mais alors que la plupart des dirigeants (pour ne rien dire des opinions) n'avaient encore qu'une faible conscience de ce qu'Internet, puis le *big data*, allaient changer à l'horizon du siècle suivant, les idéaux libertaires restaient confinés dans un tout petit monde, circonscrit et marginal d'un point de vue psychologique autant que politique. D'ailleurs, en 1997, le *Cyberpunk Manifesto*[8] de Christian As. Kirtchev, texte non dénué de qualités littéraires, insistait dès ses premières phrases sur cet aspect humain : « Nous sommes l'être différent. Rats technologiques, nageant dans l'océan de l'information. Nous sommes l'effacé, le petit garçon qui s'asseyait à la dernière table dans un coin de la classe, nous sommes l'adolescent considéré comme bizarre par tout le monde, nous sommes l'étudiant qui hacke des systèmes informatiques et en explore les tréfonds, nous sommes l'adulte assit sur le banc d'un parc, le portable sur les genoux, programmant la dernière réalité virtuelle… »



« Le « Cyberpunk Manifesto » de Kirtchev (lecture)

Une présentation historique de la genèse du bitcoin ne peut éluder le choc de la crise de 2008. Celle-ci jeta une lumière crue sur un système bancaire prédateur, donneur de leçon et irresponsable, comme sur les liens incestueux que cet oligopole entretient avec des dirigeants, qui prônent par ailleurs libre échange et libre concurrence comme religion d'État. Mais cette présentation historique ne doit pas non plus ignorer le choc consécutif au *Patriot Act* d'octobre 2001. Non que cette étape ait été la première dans la déconstruction de l'État de droit. Pour donner des repères plus familiers au lecteur français, l'historique du plan Vigipirate suffira. Activé en 1995 (attentat du métro Saint-Michel) et jamais levé depuis décembre 1996, doté à partir de 2003 d'une liturgie de couleurs variées, auxquelles nul n'attache plus d'importance sinon quelques comiques, le rouge étant de toute façon la norme depuis 2005, puis assorti de niveaux d'alertes toujours plus élevés tandis que le nombre de textes de lois de plus en plus sécuritaires se compte par dizaines.

Or, de manière croissante, mais assez nettement depuis 2001 (*Patriot Act* aux USA, loi LSQ en France) ces lois allaient, dans un contexte de généralisation de l'Internet, cibler les nouvelles technologies au motif de leur utilisation potentiellement criminelle. Ainsi, en France, la loi LSQ permettait au juge de demander un déchiffrement d'informations chiffrées, et imposait aux personnes proposant un service de cryptographie de fournir aux autorités les algorithmes de chiffrement, toutes choses contre-intuitives pour un fournisseur de services cryptographiques, quand encore elles seraient seulement possibles d'un point de vue technique…

D'autre part, à partir des événements de 2001 apparut un souci croissant de lutte contre le financement du terrorisme. À chaque nouvel attentat (quand bien même ils n'avaient pas tous, loin de là, mobilisé des moyens humains, technologiques et financiers comparables à ceux du 11 septembre) un nouveau tour de vis fut donné dans le sens de la surveillance financière, avec un texte voté quelques jours après, nul ne se souciant de cacher qu'il était prêt d'avance.

Cette lutte fit bon ménage avec la lutte anti-blanchiment ou contre la (petite) fraude fiscale, car toutes convergent sur deux axes : l'obligation pour tout banquier ou intermédiaire, et finalement pour tout commerçant, d'identifier de façon de plus en plus précise son client (K*now Your Customer)* et la promotion par tous les moyens (y compris répressifs) d'une société sans cash. Que la première obligation fasse l'affaire du marketing et la seconde celle des banques assure l'efficacité de cette politique, du moins si l'on veut bien ne pas mesurer ce pour quoi elle a été mise en place : le blanchiment se porte très bien et les citoyens sont toujours exposés à la menace terroriste.

Quand le bitcoin sortit progressivement de son ghetto, divers néophytes s'interrogèrent plus ou moins sincèrement sur les raisons de l'anonymat (au demeurant mal compris) des transactions. Et pas seulement des inspecteurs de police ou des impôts, comme en témoigne l'étonnant rapport[9] émis en avril 2015 par une Commission du CESE, une assemblée essentiellement composée de représentants sociaux (patronat, syndicats, associations). Au-delà d'une certaine naïveté (« dès lors que les systèmes se définissent comme totalement anonymes, la transparence est remise en cause ») on perçoit une réelle incompréhension : *Pourquoi se cacher ? Comment créer de la confiance sans relations humaines ? Comment faire confiance lorsque l'on ne sait pas à qui bénéficie le système ? Pourquoi considérer que sans anonymat, un système équivalent au Bitcoin ne serait pas efficient ?*

Le rêve initial d'Internet a engendré une surveillance plus puissante que ce qu'Orwell avait imaginé. Gouvernements, fournisseurs d'accès (à Internet ou au téléphone), marchands de systèmes d'exploitation, de logiciels et d'objets connectés, réseaux sociaux, sites et plateformes de vente en ligne, banques et promoteurs de points de fidélité : tous accumulent, conservent, croisent et vendent des milliards de données personnelles.

On peut s'en accommoder. Mais on ne peut rien comprendre à Bitcoin (ni même à la « technologie *blockchain* », forme édulcorée sur laquelle on reviendra) si l'on oublie, ou veut faire oublier, qu'il fut conçu par et pour des gens opposés à l'autoritarisme des gouvernements, refusant la censure et la possibilité de la censure, refusant la surveillance de masse, souhaitant conserver la propriété de leurs données personnelles, pensant que pour cela l'anonymisation de leurs correspondances, de leurs données et de leurs transactions est un droit, que les logiciels libres sont plus sûrs que les logiciels propriétaires, aux sources fermées, et qu'une monnaie libre par rapport aux États et aux banques est une chose désirable et utile. Depuis 2011, il est possible de financer Wikileaks en bitcoin. Bitcoin participe ainsi concrètement de la possible instauration d'une société de *sousveillance*, société où seront inversés la surveillance, désormais possible depuis la base de la pyramide, et le contrôle panoptique, désormais décentralisé. On ne peut s'empêcher de songer à la définition du panoptique par Michel Foucault en admirant la virtuosité architecturale de Bitcoin : « le *Panopticon* ne doit pas être compris comme un édifice onirique : c'est le diagramme d'un mécanisme de pouvoir ramené à sa forme idéale ; son fonctionnement, abstrait de tout obstacle, résistance ou frottement, peut bien être représenté comme un pur système architectural et

optique : c'est en fait une figure de technologie politique qu'on peut et qu'on doit détacher de tout usage spécifique. » [10]

Une prouesse technique de filiation crypto-anarchiste adoptée par des publics différents

Le contexte de la naissance de Bitcoin maintenant exposé, il convient désormais de comprendre l'idéologie de ses créateurs et *early adopters*. En effet la majorité des expériences ou articles dédiés au sujet de la monnaie numérique proviennent (sans surprise) de personnes aux valeurs crypto-anarchistes et libertaires affichées.

Comment définir le crypto-anarchisme ? À la différence du vocable « crypto-communisme », « crypto » n'est pas un préfixe qui viendrait modaliser le mot qui suit, mais possède bien une valeur propre. Les protagonistes n'ont ici pas forcément pour objectif de se dissimuler – ce ne sont pas des anarchistes se cachant ou cachant leurs opinions – mais d'instaurer une anarchie pourvue d'un droit certain à l'anonymat à l'aide de la cryptographie. Ce désir découle naturellement de leurs connaissances en cryptographie, qui les amènent à penser que, sans un usage démocratisé des outils cryptographiques, le glissement vers un État sans liberté serait très rapide.

Pour les crypto-anarchistes en effet, si un système d'anonymisation ne concerne pas tout le monde, il est forcément moins efficace, voire inefficace. Ainsi réalisent-ils l'alliance de deux principes porteurs, selon eux, de liberté, à savoir de la décentralisation, chère à l'anarchie, et du droit au chiffrement généralisé et à l'anonymat, cher aux cryptographes.

Dès lors on comprend mieux pourquoi Bitcoin utilise des concepts de cryptographie asymétrique, pourquoi Bitcoin possède en son sein des systèmes permettant d'être le plus discret possible sur le réseau, et enfin pourquoi Bitcoin est un protocole conçu de sorte à réunir tous les utilisateurs sous une même enseigne. Mais nous reparlerons de la question de l'anonymat du Bitcoin plus en détail plus tard dans l'ouvrage.

À noter que, dans le cas de Bitcoin, on ne saurait proclamer la neutralité de la technologie comme nous l'entendons régulièrement. Ici, le code est, à sa genèse même, déjà puissamment idéologique. On serait tenté de dire *Code is Law* et de poursuivre l'adage en rappelant que ceux qui font la loi sont rarement dépourvus d'idéologie.

Ce désir d'émancipation a conquis de nombreuses personnes soucieuses de se réapproprier certaines libertés, considérées comme pratiquement confisquées par ce que l'on nomme encore pourtant l'État de droit. Notamment celle du droit à l'anonymat, de plus en plus mis en cause tant par des lois liberticides, votées sans réflexion sérieuse en réaction aux attentats, que du fait d'un usage débridé et généralisé de plateformes captant nos données personnelles privées. Dans une certaine mesure on peut dire que le *Patriot Act* et toutes les révélations qui suivirent avec Snowden et Assange, comme cela a été dit plus haut, ont influencé le Bitcoin en ce sens. Encore une fois, tout est question de contexte.



Le paiement anonyme est-il un crime ? (article de Benoit Huguet)

L'hostilité envers les institutions, sous ce rapport de la protection de notre vie privée, rallie désormais des publics forts différents, allant des communautés scientifiques aux militants politiques radicaux, en passant par les développeurs ou aficionados des Internets libertaires et libres. De là est né un mélange en soi intéressant entre des personnes d'obédiences et de milieux différents, ce qui est malgré tout assez rare, car les communautés sont souvent assez homogènes par définition.

Là encore, ce sont des principes universels qui guident les membres de cette communauté : le respect dû à la vie privée, inscrit dans l'article 12 de la Déclaration Universelle des Droits de l'Homme (« Nul ne sera l'objet

d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteinte ») mais aussi le droit à la propriété inscrit dans son article 17 (« 1. Toute personne, aussi bien seule qu'en collectivité, a droit à la propriété. 2. Nul ne peut être arbitrairement privé de sa propriété ») et enfin le refus de toute censure, qu'elle affecte la liberté d'expression ou la circulation des capitaux.

Les valeurs que sont le droit à la propriété et l'absence de censure seront par la suite très appréciées des libertariens. À tort ou à raison, ce courant politique vise la réduction de l'État à ses fonctions minimales et promeut une forme de société extrêmement permissive, régie par un capitalisme poussé à ses dernières conséquences. Le libertarianisme, bien que vivement critiqué pour ses relations avec le *Tea Party* et son idéologie extrême, est pourtant un des premiers publics et promoteurs des monnaies décentralisées – dont l'existence même évoque les théories de l'école autrichienne et notamment l'ouvrage de Friedrich Hayek, *Pour une vraie concurrence des monnaies*, théories auxquelles ils sont généralement sensibles. Les libertariens craignent principalement l'ingérence de l'État ou l'expropriation. Dès lors Bitcoin apparait absolument approprié à leur cadre conceptuel.

Le bitcoin est avant tout une monnaie que l'on possède comme de l'or. Aucune autorité ne peut décider de saisir des bitcoins ou de les dévaluer. Du moment que l'on a sa clef privée (ce concept sera approfondi plus loin dans le livre), personne n'est en capacité de s'emparer des fonds. C'est là une des forces de Bitcoin face au pouvoir. Le bitcoin est souvent appelé monnaie virtuelle, mais, comme nous le verrons à maintes occasions, c'est tout au contraire une monnaie certes intangible mais la plus réelle qui soit parmi les monnaies d'échange et d'épargne, avec les métaux précieux qui ne sont cependant pas aussi pratiques à échanger que Bitcoin.

Pourquoi cela ? Parce que les billets de banques n'existant que par une garantie (et une coercition) de l'État envers le citoyen, la banque centrale peut manipuler à loisir ses émissions, ou démonétiser à tout instant ses billets, comme dans le célèbre *Cave se rebiffe*… ou plus récemment en Inde. Quant au compte bancaire du client, leur montant ne représente rien d'autre qu'une dette de la banque envers lui, ce qui l'expose au risque de défaillance de celle-ci, d'autant que les fonds de garantie sont d'une manière générale bien peu élevés.



Démonétisation, une scène culte (film)

En revanche, dans le cas de la cryptomonnaie, le détenteur est pleinement propriétaire de ses bitcoins, et seule la main invisible, prônée par les admirateurs de Smith desquels font partie les libertariens, peut changer le cours de ses biens intangibles mais en aucun cas les lui confisquer.

Autre paramètre important dans l'adoption de Bitcoin auprès de ces publics : son caractère théoriquement non-censurable. On peut certes penser à de possibles changements dans le protocole qui pourraient éventuellement démentir cela, mais il y a tout de même de grandes chances qu'une chaîne régie par une version sans censure du protocole soit entretenue *ad vitam aeternam* en cas de changement et d'externalités non prévisibles visant à la censure du réseau. Or qu'est-ce que l'absence de censure, sinon la liberté pour tous ceux qui rejettent en bloc Rousseau et son *Contrat Social*, l'État-providence et son administration, trop contraignants selon eux ? Ici, nulle limite dans l'exercice concret de la liberté, surtout dans celle de commercer. D'où, il faut l'avouer, la profusion des plateformes de vente sur le Darknet suite à la création du Bitcoin…

Les libertariens furent les premiers à vanter les mérites de ces plateformes qui fonctionnaient sans aucune régulation, tant en terme de stock que de description, de prix ou de services après-vente. Bref, une paradoxale illustration de la force de l'intelligence collective ! De là à considérer ce genre de site comme le Pinacle de la civilisation, c'est évidemment discutable moralement ou politiquement, mais il importe d'en considérer le fonctionnement et les implications.

Dans ce monde sans confiance (*trustless)* tout dépend de la réputation que chacun peut acquérir derrière un pseudonyme. Il en va de même dans le monde de la cryptomonnaie en général. Des développeurs ont pu lever

2 millions d'euros très rapidement sur des projets complexes et spécialisés car ils avaient un nom connu du public visé [11]. Ce règne de la « e-réputation » dans les rapports humains séduit un certain public qui se fonde sur l'axiome discutable : « on n'a que ce que l'on mérite. ». Ainsi, quelqu'un d'honnête ne rencontrera aucune barrière pour exercer n'importe quelle activité commerciale, mais une erreur de parcours pourra coûter très cher.

Revenons à Bitcoin, qui participe à échafauder, petit à petit, un modèle de société assez mouvant sur un spectre social et intellectuel large, ce qui implique une adhésion de publics hétérogènes. Même si les racines de ce public sont, comme nous l'avons dit, les cryptographes, les anarchistes, les libertaires et les libertariens, la nature monétaire de Bitcoin a rapidement attiré des mordus d'innovation financière, et son aspect informatique inédit a mené à lui de nombreux *geeks*. Encore ne sont-ils pas les seuls publics de Bitcoin, car cet objet monétaire non identifié attise la curiosité chez tous ceux qui chérissent les défis paradigmatiques et les concepts intellectuellement riches.

Ainsi, dès sa genèse, même si l'écosystème de Bitcoin reste limité, il regroupe des individus dissemblables. Et les amateurs de ces concepts novateurs ont conservé et accentué leur diversité à travers les années. Lors des évènements consacrés aux monnaies numériques, il n'est pas rare de voir un magistrat converser avec un matheux, ou bien un développeur discuter avec un diplômé de sciences humaines. Les barrières sociales sont quasiment invisibles tant la passion idéologique ou intellectuelle et la défense de valeurs universelles sont au cœur de l'intérêt pour Bitcoin.

Ce caractère hétéroclite et communautaire de Bitcoin est capital. Il y a très souvent dans cette communauté un désir d'alternatives sérieuses, autres que celles qui sont proposées, en grossissant le trait, par les altermondialistes « classiques ». Aussi retrouve-t-on assez peu de promoteurs des MLC (monnaies locales complémentaires) dans le monde Bitcoin, bien que celui-ci soit, avec plusieurs millions d'usagers, de loin la première monnaie « communautaire » à être aussi universelle et à avoir des caractéristiques aussi innovantes et variées. Bitcoin est souvent considéré comme amoral aux yeux de nombreuses personnes combattant le capitalisme et l'argent de manière très générale, et parfois un peu vague : Bitcoin n'avait certes pas pour but de permettre la réduction des inégalités de revenus mais il entendait les rendre plus justes puisque sa création monétaire n'était distribuée qu'en échange d'un réel effort. D'autre part, il a aussi pour propriété de rendre l'accès à la monnaie plus facile, on y reviendra ; sa résistance à la censure fait que, par définition, n'importe qui peut utiliser Bitcoin du moment qu'il possède un accès à Internet, ce qui n'est pas encore le cas tout autour du globe mais qui tend à le devenir.

La valeur communautaire de Bitcoin est tellement forte que, tout autour du monde, différentes personnes se mettent à créer des lieux de rencontre où l'on peut payer en bitcoin. Tout autour du monde des profils différents se réunissent dans des *meetups* pour partager cette passion de l'alternative décentralisée. Ainsi naissent rapidement des « *evangelists* » semblables aux missionnaires d'une religion. Ces gens, comme le grec-américain Andreas Antonopoulos, vont sillonner le monde pour apporter la bonne nouvelle qu'est Bitcoin. Parce qu'un tel changement de paradigme induit un travail d'éducation gigantesque. Et parce que Bitcoin est avant tout de par sa nature une expérience communautaire : c'est un protocole de réseau décentralisé. Les jetons que sont les bitcoins sont faits pour être transférés et échangés. On revient dès lors à la nature première de la valeur monétaire, celle d'un moyen et non d'une fin, bien que la thésaurisation reste encore forte du fait des perspectives telles que les perçoivent les gens qui travaillent concrètement au développement de l'écosystème.

Enfin, il faut noter, au chapitre des sentiments communautaires, qu'une sorte d'union dans l'adversité s'est formée au sein des communautés Bitcoin face au traitement médiatique réservé à celui-ci. Comme on y reviendra dans l'historique (cf. III, 1) Bitcoin a subi un véritable « délit de sale gueule » et il est encore décrié comme une monnaie de criminels, une monnaie louche, une monnaie « sulfureuse ». La communauté des *bitcoineurs* a su se défendre face à ce traitement en innovant et en montrant que les possibilités sont toujours plus nombreuses et révolutionnaires. Bitcoin est un projet agile qui devient plus fort à mesure qu'on le frappe ; un projet « antifragile » selon la définition de Nassim Taleb dans son livre éponyme : « L'antifragilité est au-delà de la résilience ou de la robustesse. Ce qui est résilient résiste aux chocs et demeure intact ; ce qui est antifragile en sort meilleur. » [12]

C'est aussi l'ampleur des accusations portées contre Bitcoin, devenu « infréquentable », qui amena le fameux *buzz* autour de la *Blockchain* en 2015 (cf. III, 1). Cette agitation médiatique visait à laver l'image du protocole d'échanges décentralisés, mais de manière assez ridicule, à l'image de Monsieur Trichet qui expliquait en octobre 2016 que la *blockchain* était une « invention géniale » mais laissait penser, en ajoutant qu'il pouvait « détacher la *blockchain* de Bitcoin » qu'il ne maîtrisait guère son sujet. Au fur et à mesure que le discours sur la *blockchain*

s'autonomisait, une sorte de scission communautaire s'est opérée entre des personnes avant tout passionnées par Bitcoin (et par le paiement en monnaie non légale) et ceux qui souhaitaient surtout profiter de la folie médiatique et marketing autour d'une « technologie *blockchain* » présentée, non sans approximation technique, comme une promesse de renouveau de l'industrie bancaire traditionnelle.

Les divergences idéologiques entre ces deux communautés passent très clairement par les idées qui viennent d'être présentées : une remise en cause des convictions et des paradigmes existants.

2- Un agencement génial, instrument de véritables exploits

Un exploit conceptuel à l'origine du bitcoin : une confiance sans police ni garant

Nous allons maintenant tenter de montrer en quoi Bitcoin est un objet conceptuel génial. En effet, le protocole Bitcoin a réussi – et c'est une première – à créer un bien numérique non reproductible. Ce que nous entendons par là, c'est qu'en informatique rien n'est unique et que tout est ordinairement copiable. Par exemple, lors de l'envoi d'un mail, la pièce jointe envoyée par l'un à l'autre n'est pas perdue par l'expéditeur, elle est simplement copiée. Rien ne distingue l'original (d'un fichier texte, image, musique…) de sa copie. Et cette transmission par copies non distinguables de l'original se reproduit à l'identique pour toutes les opérations informatiques, fussent-elles décentralisées en pair-à-pair comme le partage d'un fichier « torrent », pour citer une référence que les téléchargeurs de films comprendront et qui pointe vers la difficulté de « vendre » un produit numérique sans évaporation…

Le seul moyen de rendre un objet numérique cessible de manière exclusive, et dans des conditions juridiques satisfaisantes, était donc de passer par un tiers : une banque, par exemple, ne manque pas de retirer la monnaie électronique d'un compte lorsqu'un virement est effectué, quand bien même cette monnaie n'a pas encore été versée sur le compte du récipient. Il en va de même pour le retrait progressif des euros dépensés sur un site où un utilisateur a préalablement entré les références d'une carte cadeaux. Tous ces actes passent par une vérification centralisée des opérations.

Passer par un tiers comporte deux risques désormais contournables : d'une part il n'est plus obligatoire de faire confiance à un tiers faillible, corruptible et particulièrement exposé aux attaques du fait même de sa centralisation ; d'autre part il n'est plus nécessaire de faire confiance à un tiers qui pourrait être malintentionné ou malhonnête. Ces deux cas de figure, souvent minimisés par le système, doivent pourtant être mentionnés, car l'un montre la faiblesse d'un système centralisé et l'autre la faiblesse d'un système où l'on doit faire confiance à un acteur.

Bitcoin résout ces deux problèmes. On décrit souvent ce système comme *trustless* (sans acte de confiance obligatoire) et décentralisé. Qu'est-ce que cela signifie ? Dans un premier temps Bitcoin est un système sans confiance dans le sens où il n'est nullement nécessaire de faire confiance à quelqu'un dans l'environnement proche ou lointain d'une transaction, puisque celle-ci est exclusivement garantie par le réseau et le protocole eux-mêmes, sans intervention humaine. Ainsi, lorsque l'on reçoit des bitcoins, nul besoin de se soucier de leur validité, le système ayant déjà effectué automatiquement toutes les opérations de vérification. En ce sens, le système est absolument autonome. Disons que la seule confiance accordée est celle qui est accordée au réseau, tout en sachant bien sûr que des humains sont à l'origine de la rédaction du code et que, par conséquent, des erreurs de codage sont possibles. Cependant, l'utilisateur peut se fonder sur la pérennité et la résilience d'un réseau qui, au bout de 8 ans, n'a jamais été compromis, y compris depuis qu'il a pris une valeur de nature à attirer d'incessantes attaques[13].

On distingue ici l'essence des mots grecs *autos*, « même », et de *nomos*, la « loi ». En définitive, qu'est-ce que l'autonomie dans Bitcoin ? Cela semble être le principe *code is law* ; le protocole obéit uniquement à son code et n'a pas besoin d'intervention extérieure et autoritaire. La notion d'autonomie du système est primordiale en ce sens que Bitcoin se distingue, pour continuer de parler grec, de la *polis* qui, elle, est corruptible. Ainsi les lois de la cité peuvent-elles être changées ou enfreintes (les tyrans se servent fort bien des lois démocratiques antérieures,

les États de droit peuvent suspendre certaines garanties) et l'ordre public même n'est essentiellement garanti que par un pouvoir central et non par les citoyens eux-mêmes, leur implication n'étant que symbolique.

À la différence des systèmes que font fonctionner les banques, tout le code de Bitcoin est totalement consultable et donc audité chaque jour par des milliers de personnes. Aussi, du fait que Bitcoin est un système ouvert, et même (de façon contre-intuitive pour les non-informaticiens) du fait des pirates qui tentent de le casser, le système bénéficie de davantage de tests que des infrastructures privées qui paient pour ce genre d'audits mais ne peuvent en faire constamment. Le réseau possède une résistance supplémentaire certaine étant données ses caractéristiques décentralisées : il n'offre pas de point individuel de défaillance (SPOF, pour *single point of failure*). Andreas Antonopoulos compare la résistance de Bitcoin à celle d'un rat d'égout !



Bitcoin, le rat d'égout ? (conférence d'Andréas Antonopoulos)

La résultante de toutes ces caractéristiques est la disparition du « tiers de confiance », jadis obligatoire, dans les opérations numériques de cession de titres ou de valeurs. Habituellement, quasiment toutes nos opérations numériques passent par un tiers de confiance. L'envoi d'argent est effectué par des banques ou divers organismes financiers qui prennent des commissions non négligeables pour des services qui sont souvent loin d'être à l'avant-garde technologique, bien que certaines alternatives décentes et en adéquation avec leur temps voient parfois le jour. On peut imaginer raisonnablement que cette « décentralisation » pourrait s'étendre dans le futur à d'autres services qui requièrent des tiers de confiance, l'économie collaborative par exemple.

Il ne s'agit pas forcément de faire totalement disparaître le tiers de confiance. En effet, dans le cas d'un paiement en bitcoin, il est impossible de se retourner vers qui que ce soit et d'effectuer une requête pour être remboursé. La seule possibilité est la plainte légale qui pourra être reçue si une fraude est constatée. Cependant, suivant le type de fraude, il pourra être compliqué de retrouver ou de qualifier celui qui aura nui au plaignant. En ce qui concerne les règlements d'échange de biens par exemple, il serait possible de ne faire appel à un tiers de confiance indépendant et reconnu que dans le cas où l'acquéreur n'aurait pas confiance dans le vendeur et uniquement dans ce cas, alors qu'un vendeur identifié et réputé comme certaines grandes enseignes bénéficierait toujours d'une réputation ne rendant plus nécessaire le tiers de confiance.

L'avantage compétitif de Bitcoin sous l'angle de l'absence du tiers de confiance se situe au niveau des opérations en pair-à-pair et dans les opérations vers le vendeur. Le vendeur peut être assuré qu'il n'a pas été floué, par exemple avec de la fausse monnaie, ou victime d'une malversation, comme certaines annulations de transaction a posteriori, tout comme un ami à qui l'on transfère de l'argent peut être assuré qu'il a bien reçu l'argent en question et n'aura pas besoin de douter de sa quantité ou fiabilité.

La présence d'un tiers est requise pour tout échange non effectué dans le cyberespace et donc non programmable. Les problèmes de sécurité proviennent toujours, en effet, d'un point de contact avec le monde tangible. D'où le fait que Bitcoin est souvent surnommé « la monnaie d'Internet », parce qu'au fond, comme cela a été dit au point I, 1, il a été conçu pour cela.

Les supporters de Bitcoin ajoutent que ce n'est pas tout. Car la libéralisation, ou la disparition pure et simple, de l'activité de tiers de confiance ne leur paraît guère dommageable dans la mesure où elle devrait permettre de tirer les prix vers le bas grâce à une concurrence accrue parmi les tiers. Les tiers ne seraient dès lors rémunérés que sur la plus-value apportée lors d'un service, et non à cause d'un monopole historique ou corporatiste, comme les notaires ou l'INPI par exemple.

Mais tous ces nouveaux avantages n'auraient pas vu le jour si deux problèmes de taille n'avaient pas été surmontés : il s'agit des réseaux décentralisés et des systèmes de pair-à-pair, qui incluent des problématiques inédites.

Le premier réside dans le problème dit des « généraux byzantins ». Un drôle de nom, peut-être dû à son aspect métaphorique envers les systèmes d'informations, et sans doute inspiré à trois matheux par un péplum. En effet, le problème est théorisé sous ce nom en 1982 par Leslie Lamport, Robert Shostak et Marshall Pease[14] : différents généraux byzantins doivent envahir un camp ennemi mais ne peuvent communiquer qu'à l'aide de messagers. Cependant, parmi les généraux, certains peuvent être des traitres, et des messagers peuvent être corrompus ; le problème réside donc dans la faculté d'établir malgré cela un plan de bataille commun : un consensus décentralisé.

De ce problème, théoriquement fort difficile à résoudre, Satoshi Nakamoto a présenté une solution pratique élégante, une combinaison ingénieuse de plusieurs trouvailles qui seront abordées successivement : un réseau pair-à-pair, le minage par la « preuve de travail » (sur laquelle nous reviendrons plus d'une fois), la cryptographie asymétrique, et enfin la *blockchain*.

La transaction de pair-à-pair permet à la fois la décentralisation et la transmission des données, en évitant les problèmes de montée en charge et de censure. En effet, l'avantage d'un réseau pair-à-pair réside dans le fait que le réseau gagne en efficacité quand le nombre d'utilisateurs augmente, contrairement aux serveurs centralisés qui se trouvent en difficulté lorsque trop de personnes y font simultanément des requêtes. C'est par exemple le cas du réseau téléphonique lors du Nouvel An. Si ce réseau était décentralisé, aucun problème ne se produirait.

En ce qui concerne Bitcoin, c'est un petit peu différent pour le moment, en raison d'un paramètre fixé dans le protocole et limitant le nombre de données incluses dans le livre de compte toutes les dix minutes. De surcroît la tâche du minage étant décentralisée (accomplie par certains) et non distribuée (accomplie par tous), la répartition des tâches sur le réseau n'est pas totale. Nous aurons l'occasion de revenir sur cela dans quelques chapitres.

D'autre part, le pair-à-pair est résistant à la censure, comme le montre très bien le réseau Freenet datant de 2000, premier réseau web totalement distribué, qui fonctionne toujours actuellement même si la navigation n'y est pas très rapide ; mais aussi avec le téléchargement illégal en « torrent », déjà mentionné, qui part du même principe et qui, lui non plus, n'a toujours pas été « arrêté », quand bien même de puissants moyens sont mis en œuvre à son encontre.

Il faut enfin mentionner les bienfaits, insuffisamment vantés, de tels espaces décentralisés et sans censure. Nous en voyons bien plus souvent, parce qu'on nous les donne complaisamment à voir, les côtés négatifs qui parfois ne peuvent concerner que des populations très minoritaires. Ainsi des pédophiles ou de tous les adeptes de pratiques amorales et condamnées par la société, mais qui sont bien antérieures aux techniques que l'on met en cause : ces personnes se serviront toujours d'outils pour commettre des actes illégaux dans le secret, que ce secret soit lui-même légal ou non.

En revanche, les outils du secret peuvent aussi servir aux dissidents politiques au sein de régimes autoritaires, ou même dans des régimes démocratiques, aux journalistes en quête de témoignages difficilement partageables publiquement sans risque. N'oublions pas la puissante contribution à la défense de la liberté de ces réseaux, qui ne peuvent être arrêtés ou censurés. À noter que les interdire ne ferait que permettre aux seuls criminels et imbéciles de les utiliser, au lieu d'une utilisation massive et bénéfique pour tous les citoyens.

Bitcoin, en s'inscrivant dans cette lignée, offre déjà un horizon conceptuel où la liberté est reine, et cela suffit amplement à le trouver génial et opportun dans les temps que nous vivons. À l'aune des velléités d'interdiction brandies aujourd'hui chaque matin, nos arrière-grands-parents auraient interdit la traction-avant parce qu'elle favorisait les entreprises condamnables du gang qui en 1946 lui dut son nom[15] !

La seconde trouvaille est donc le « minage ». Expression métaphorique : il ne s'agit pas ici de donner de harassants coups de pioche pour trouver de l'or dans une mine, mais de produire un gros travail informatique dont la récompense (attribuée de façon semi-aléatoire) est l'extraction et l'obtention de nouveaux bitcoins.

Satoshi Nakamoto propose la solution du minage pour répondre tant au problème des « généraux byzantins » qu'à un second problème majeur, inhérent aux réseaux décentralisés, qui porte le nom, non moins curieux, de « l'attaque de Sybil » – en référence au livre du même nom (publié en 1973 par Flora Rheta Schreiber) qui décrivait de façon d'ailleurs romancée une schizophrène troublée de multiples dédoublements d'identité. Sur les réseaux décentralisés, il est normalement possible de changer assez facilement d'identité ou de multiplier ses identités. Par exemple, sur Internet, l'adresse IP, censée représenter la personne derrière la machine, peut aisément être modifiée à l'aide d'un réseau privé virtuel ou d'autres services comme le célèbre Tor (cf. III, 1), de

même qu'il est possible d'avoir plusieurs identités en utilisant des « machines virtuelles », sortes d'ordinateurs au sein de l'ordinateur, ou bien tout simplement en utilisant d'autres machines, par exemple de grands parcs informatiques piratés dans leur ensemble. Toutes ces techniques permettent d'avoir de multiples identités, et donc de tricher dans un réseau où l'identité aurait un poids et où le consensus reposerait sur un vote par identité : de nombreuses personnes pourraient alors en abuser à l'aide des moyens que nous venons de décrire.

Pour enrayer cette « attaque de Sibyl », Bitcoin recourt donc au minage, parce qu'il oblige à consommer de l'énergie, prouvant par-là que l'on est une seule personne ou rendant la multiplication d'identité excessivement onéreuse, l'énergie étant régie par les lois incorruptibles de la physique. Ce système nommé Hashcash a été inventé en réalité en 1997 par le cryptographe et crypto-hackeur Adam Back [16]. C'est le principe que Bitcoin utilise dans le minage. Tous les mineurs essaient de résoudre un problème informatique lié à une fonction mathématique dite de « hashage » (que l'on va présenter un peu plus loin) en étant placés en situation de concurrence, et seuls ces concurrents peuvent valider les blocs de transactions. Il n'y a qu'un validateur pour chaque bloc, toutes les 10 minutes (à peu près) dans le réseau Bitcoin. Mais ces mineurs sont aussi en concurrence, la récompense étant attribuée au gré du hasard parmi ceux qui produisent la solution du problème de hashage. Le système fonctionne car il est impossible de consommer de l'énergie à l'infini. Cet élément permet alors la résolution du problème d'identité.

Finalement, grâce à un consensus décentralisé fondé sur la concurrence du minage par résolution du problème cryptographique, tous les acteurs du réseau se mettent au diapason. Cette technique de validation est nécessaire pour permettre à tout le système (à tous ceux qui participent au réseau, à tous ceux qui ont téléchargé le registre) de s'harmoniser avec une seule et même base de donnée. Bitcoin réussit avec brio à obtenir un consensus de manière décentralisée et permet ainsi de conserver la fiabilité de sa base de données et l'immuabilité des écritures de ses transactions.

S'il n'était pas possible de se mettre d'accord, rien de tout cela ne le serait non plus car personne ne pourrait jamais savoir s'il est bien synchronisé avec le reste du réseau ou s'il détient bien la bonne copie du registre mis à jour. Il faut véritablement prendre la mesure de cette prouesse qui est de trouver un accord sans avoir préalablement désigné un chef ou une autorité centrale. On peut donc voir Bitcoin comme une révolution, au sens premier du terme, celui du renversement, dans notre cas le renversement de l'autorité. Il s'agit, de fait, de la première monnaie horizontale dans sa conception même.

Inauguration du concept de *blockchain* : un rouage indispensable du protocole Bitcoin

Le consensus résulte donc de la validation des mineurs et celle-ci s'effectue sur un gigantesque registre partagé qui garde en son sein toutes les transactions réalisées sur le réseau. Ce registre s'appelle la *blockchain* (*chaîne de blocs* en français). On voit dès lors que ce n'est là qu'un rouage des systèmes d'échange décentralisé et non pas un élément précurseur au protocole, en ce sens que la *blockchain* est une production du protocole et du réseau, et non l'inverse. Ce n'est qu'une base de données structurante et non une entité pouvant servir toute seule.

Le père du Bitcoin est l'inventeur du concept de *blockchain*. Il est assez amusant de remarquer que ce nom n'est même pas mentionné dans le papier original de Satoshi Nakamoto *Bitcoin : A peer-to-peer electronic cash system* [17]. Ce détail historique montre à nouveau à quel point l'objet *blockchain* n'était qu'un élément du système, et n'était pas considéré comme l'invention principale. L'innovation technologique est avant tout le protocole Bitcoin dans son ensemble et ce chainage de bloc n'en était qu'un engrenage.

C'est cependant ce registre qui est soudain devenu célèbre indépendamment du protocole Bitcoin en raison des fantasmes qu'il procure à certains. On parle souvent dans les médias de « la technologie *blockchain*. »

Il ne faut pas penser cet objet au singulier comme quelque chose de similaire à chacune de ses utilisations. Il n'y a pas une technologie *blockchain* mais des blockchains, chacune conditionnée par différentes technologies, différents protocoles avec leurs paramètres et leurs intentions sous-jacentes.

Cet incroyable procédé qui permet d'avoir une base de données fiable et infalsifiable dans le temps a donc également pour inventeur Satoshi Nakamoto. Que son invention se soit presque dédoublée préfigure bien l'aspect extra-monétaire du Bitcoin (nous y reviendrons). Mais pour autant il faut bien comprendre que Bitcoin est

inséparable de sa *blockchain*, composante qui permet son fonctionnement. C'est en effet dans ce registre que sont gravées toutes les transactions.

L'intérêt d'une base de données distribuée de type *blockchain* réside dans sa sécurité. Et pour que celle-ci soit sécurisée elle doit être accompagnée d'un fort effet de réseau. C'est-à-dire qu'une *blockchain* utilisée par trois personnes en circuit fermé n'a que très peu de valeur en raison de sa fragilité face à des attaques. N'oublions pas que, dans la décentralisation, le nombre fait la force. Bitcoin, qui possède autour de 6 000 « nœuds »[18] que l'on pourrait assimiler à des relais, demeure le réseau le plus solide de toutes les blockchains créées depuis 2009 puisque cela signifie que sa *blockchain* est répliquée dans chacun de ses nœuds et que l'on a donc au minimum 6 000 copies de ce grand livre de compte.

Le nombre de mineurs et la puissance de calcul dédiée au réseau Bitcoin, et par conséquent à la *blockchain* Bitcoin, sont absolument hors-de-portée de n'importe quel supercalculateur, le réseau étant 10 000 fois plus puissant que les 500 plus gros supercalculateurs au monde[19]. Cette puissance s'explique par la motivation monétaire, qui rend le minage rentable et incite les mineurs à perfectionner sans cesse leur équipement pour rester compétitifs. Le jeton monétaire de la *blockchain*, sa distribution et sa valeur sont des éléments majeurs dans la sécurisation de la *blockchain* Bitcoin. Le mathématicien Ricardo Perez-Marco affirme publiquement[20] qu'il ne connaît pas d'autre moyen d'éliminer le risque des généraux byzantins que par la rémunération de la preuve de travail par une crypto-monnaie. Un autre mathématicien, Jean-Paul Delahaye, partage son scepticisme, par exemple, sur la volonté de la *blockchain* alternative (celle d'Ethereum) de se passer un jour de la « preuve de travail »[21].

Il faut également comprendre que ce registre permet de tracer l'histoire de chacun des bitcoins émis depuis le début de l'expérience en 2009. Chaque bout de bitcoin a son histoire et elle est théoriquement immuable. Les blockchains fonctionnent à l'inverse des manuscrits palimpsestes de jadis : on ne peut jamais modifier, supprimer ou réécrire des portions de texte. L'écriture est uniquement linéaire dans le temps et se doit de l'être pour demeurer un médium non censurable. Cette donnée est importante : l'irréversibilité des transactions en bitcoin demeure possible grâce à l'écriture uniquement linéaire dans le livre de compte. Ce système autonome, qui génère son propre temps, a créé le premier « temps universel » intrinsèque qui faisait défaut à Internet, temps assez imprécis (l'intervalle de 10 minutes[22] n'est pas exactement constant) mais totalement autonome.

La *blockchain*, publique et publiquement exploitée par divers sites, est réellement accessible à tous (même ceux qui ne l'ont pas téléchargée) et permet de consulter ainsi toutes les actions passées et présentes. Elle est transparente et permet à tout le monde d'utiliser le réseau Bitcoin sans limitation.

Ce qui est fascinant, c'est que rien ne se déplace dans la *blockchain*. Tout demeure immobile. Les bitcoins changent de propriétaires sans pour autant bouger, comme dans un livre de compte…

On dit d'ailleurs souvent de la *blockchain* qu'elle s'inspire de l'ancienne méthode de comptabilité en partie double inventée au XV^{e} siècle par Luca Pacioli qui consistait à séparer les comptes en deux, le débit d'un côté et le crédit de l'autre. De fait, sur les blockchains, et typiquement sur la mère de toutes les blockchains, on s'échange d'abord et essentiellement des jetons (*tokens* en anglais). Dans le protocole Bitcoin, ceux-ci sont nommés des bitcoins ; dans le protocole Ethereum, des ethers. Le fait que les bitcoins possèdent le même nom que le protocole est un hasard linguistique, sans doute dû à un maigre intérêt de l'inventeur pour ce genre de choses.

Mais la *blockchain* de Bitcoin, comme toutes les autres, est avant tout transactionnelle. Elle a pour fonction l'enregistrement de la transmission d'une unité de compte nommée « bitcoin » qui, subdivisée au cent-millionième, s'appelle le Satoshi, en honneur de son créateur. Si on considère ces jetons (qui étaient l'objet principal du *white paper* de 2008) on voit bien que la *blockchain* est seconde au protocole : elle vient après.

Sans vouloir s'embourber dans un débat digne de celui de l'œuf et de la poule, il faut absolument intégrer que c'est l'action de générer des jetons qui a provoqué l'apparition du *genesis block*, le premier de la *blockchain* (3 janvier 2009), mais que le protocole et le code exécuté existaient avant même la première écriture. Cela permet de comprendre que la *blockchain* est une production du protocole Bitcoin, et qu'après seulement ce dernier s'en est aussi servi de support à ses unités de compte, les bitcoins. Nous apercevons alors clairement une relation insécable entre Bitcoin et sa *blockchain*.

Sur ces bases, posons-nous les questions suivantes : qu'est-ce qu'un « bloc » contient ? Qu'est-ce vraiment que la *blockchain* de Bitcoin ? En quoi celle-ci apporte-t-elle une sécurité ?

Tout d'abord, un bloc contient un en-tête avec tous les éléments (nous y reviendrons) permettant de créer l'identificateur numérique, c'est-à-dire l'empreinte cryptographique de ce bloc, de le lier cryptographiquement au bloc précédent et au bloc suivant. Puis s'en suivent l'heure, la mesure de la difficulté du travail qui a été effectué ainsi que la création de bitcoin générée par sa validation, les différentes transactions bitcoins validées et représentant environ 10 minutes de transactions au niveau mondial et enfin ce qu'on appelle, soit le « nonce » (pour *number used once*), soit parfois le « sel », bref, les signes aléatoires dont l'adjonction ont permis la résolution du problème dit de « hashage », déjà mentionné, et qui sera détaillé au point II, 1.

Tous les blocs dûment validés sont donc enchaînés les uns aux autres grâce à leurs empreintes et au scellage final des blocs par les mineurs.

La *blockchain* de Bitcoin n'est que l'enchaînement de blocs le plus long que nous connaissons et qui répond aux exigences du protocole. Pourquoi le plus long ? Parce qu'il arrive parfois que des mineurs différents trouvent simultanément le résultat du problème de minage permettant de valider et sceller un bloc. Pour s'abstraire de cette difficulté pratique, Bitcoin contient un mécanisme permettant de considérer que seule la plus longue chaîne est la chaîne viable. Comme il est hautement improbable qu'une seule personne arrive à maintenir toute seule le consensus pendant plusieurs blocs, il y aura forcément un moment où la chaîne privilégiée par l'ensemble des mineurs demeurera plus grande et sera dès lors la seule à perdurer.

Pour tenter une analogie, ce sont comme les rails d'un train avec des aiguillages. Si l'aiguillage mène d'un côté vers une voie abandonné, le train ira de l'autre côté, celui où la voie continue. Dans le cas du Bitcoin, c'est la même chose, le but est en quelque sorte la survie, et la plus longue chaîne sera toujours considérée comme la chaîne véridique. Cela apporte une sécurité accrue puisqu'à part pour des moments d'une dizaine de minutes (et pour les transactions au cours desdites minutes), l'intégralité des utilisateurs du réseau peut être absolument sûre de la fiabilité des données qu'ils obtiennent.

Sans sa *blockchain*, Bitcoin ne pourrait donc pas fonctionner. Nous espérons que le lecteur a compris qu'il est impossible de modifier les boulons de cette belle mécanique, de cet assemblage génial, comme bon semble à chacun ou selon les intérêts commerciaux de chaque institution. Chaque élément est imbriqué dans un autre et ne peut être modifié sans risquer de perdre l'équilibre du système. Les tentatives de certains de disséquer Bitcoin, en ne gardant que les concepts qui leur plaisent, sont ridicules. Le protocole Bitcoin est un savant mélange permettant un équilibre technologique élégant, pas un catalogue de gadgets informatiques.

On pourrait assimiler la *blockchain* de Bitcoin à ce que l'on peut appeler les « communs », en ce sens que n'importe qui peut en disposer et la consulter. Elle n'appartient à personne et chacun peut l'utiliser en respectant ses règles. Une de ces règles est la nécessité de posséder des bitcoins pour écrire dedans. Car, comme nous l'avons vu plus haut, toute écriture dans la *blockchain* est transactionnelle. Les bitcoins, ces jetons monétaires, sont ainsi autant de droits d'entrée et d'utilisation du réseau.

Dès lors, l'idée que la *blockchain* est une base de données classique doit être écartée. Ce n'est pas un stockage dans le *cloud* (comme ce que propose *Dropbox*) où chacun peut déposer des fichiers ou quoi que ce soit. La *blockchain* stocke uniquement les données de transactions Bitcoin. Ces données transactionnelles ont plusieurs formes différentes : les données permettant le changement de propriétaire des bitcoins, les données de programmation pour effectuer des actions auto-exécutables et enfin 80 caractères de texte (plus précisément 80 bytes (640 bits) équivalent à 80 caractères encodés en ASCII). Ainsi, le seul espace de stockage libre de la *blockchain* réside dans ces 80 caractères, et nous savons tous à quel point les 140 caractères de Twitter sont contraignants. Même si cela permet de faire déjà beaucoup de choses, comme nous le verrons un peu plus tard, cela ne supporte pas l'idée (techniquement fausse au demeurant) que l'on va faire de la *blockchain* Bitcoin les « Archives de l'Humanité ».

Cessons de (faire) croire que la *blockchain* de Bitcoin héberge des données classiques. Celle-ci a un rôle bien défini : permettre la cession d'un bien intangible et numérique, son jeton. Avec ce rapide tour d'horizon, qui sera approfondi au point II, 1, nous pouvons tirer quelques enseignements sur la *blockchain* de Bitcoin que nous synthétisons de cette manière.

Elle n'est qu'un rouage d'un système bien plus complexe : le protocole Bitcoin. Elle est destinée à stocker des données transactionnelles et non pas des données classiques. Elle est unidirectionnelle car il est impossible de réécrire quelque chose dans celle-ci. Elle est fiable car elle résulte d'un consensus décentralisé : une seule version ne peut être considérée comme vraie. Et enfin, elle est inaliénable et éternelle car répliquée sur des milliers d'ordinateurs différents.

Mathématique et admirablement fluide, les étonnantes propriétés « physiques » du bitcoin

Nous venons, en somme, de voir les exploits du protocole Bitcoin : permettre une transaction numérique sans qu'un tiers de confiance n'autorise, valide, enregistre ou surveille la transaction, permettre une validation collective sans avoir à se soucier de l'honnêteté ou de la loyauté de tiers qui restent étrangers à la relation (les généraux byzantins) ou de la possibilité qu'existent des leurres d'identité (Sybil), permettre enfin la tenue collective, grâce à ce protocole ouvert, d'un registre qui devient une sorte de bien commun, éternel et infalsifiable.

Comment, maintenant, parler des propriétés « physiques » du bitcoin, si celui-ci n'est finalement qu'un objet mathématique, une unité de compte du registre ? Il y a une compréhensible inhibition à cela, qu'exploite et renforce l'appellation maladroite ou malintentionnée de monnaie « virtuelle ». Une analogie peut aider à lever cette inhibition : malgré le scandale logique que cela a longtemps représenté, il faut bien admettre que la lumière, phénomène ondulatoire pour Huygens, corpusculaire pour Newton, est à la fois l'un et l'autre. Pour le dire de façon plus métaphysique, elle peut être décrite efficacement comme l'un ou comme l'autre. Ou pour donner une image plus simple : l'ombre d'un cylindre sera selon un certain angle un rond, selon un autre angle un carré ! Eh bien le bitcoin semble susceptible d'être décrit à la fois comme une unité de compte et comme un jeton.

À ce point du livre, le lecteur a sans doute admis que le bitcoin était l'unité de compte d'un registre particulier (le *ledger*) qui est non pas un livre de compte en partie double, comme celui d'une banque, mais un inventaire tenu en bitcoin. Attardons-nous un instant sur cet acquis. Un inventaire peut être défini comme un recensement exhaustif et daté d'entités matérielles ou immatérielles destinées à en faciliter l'évaluation ou la gestion. On ne devrait donc pas confondre l'unité de compte (euro, bitcoin) avec les entités inventoriées, fussent-elles justement des euros ou des bitcoins. Pour expliciter cette distinction, qui peut paraître inutilement compliquée, disons que l'inventaire de la caisse du supermarché est établi en unité de compte « euro » (comme ses comptes) mais qu'un braqueur ne part jamais avec des unités de comptes mais bien avec des entités physiques.

Un paiement, « l'envoi » d'un bout de bitcoin d'un portefeuille (*wallet*) à un autre, n'est que la radiation/soustraction d'une entité numérique inventoriée en bitcoin de l'adresse de l'émetteur et son inscription/addition à l'adresse du receveur sur le même registre. Si la transaction se fait aussi vite, c'est parce qu'elle se fait sur un seul et même registre quand une transaction bancaire implique un grand nombre de livres de comptes successifs à valider.

Mais le lecteur est-il déjà disposé à admettre qu'au-delà de cette unité de compte, l'entité numérique est bien un « jeton » (*token* en anglais) ; est-il même simplement disposé à admettre que ce soit une « chose » ?

Pour le philosophe, une chose est tout ce qui peut exister, être pensé, tout ce à partir de quoi on peut affirmer ou nier quelque chose. De ce point de vue, le bitcoin est bien une chose. Mais pour le sens commun, une chose matérielle se définit en ce qu'elle occupe physiquement une certaine portion de l'espace à un instant donné, et qu'en pratique on peut l'appréhender par les sens, notamment la vue et le toucher.

Il est douteux que l'information, qu'on l'appelle registre, *ledger* ou *blockchain*, soit à ce compte « une chose » : elle est inscrite sur mon ordinateur où cette information occupe une certaine place sur mon disque dur, mais la même information peut être inscrite sur n'importe quel ordinateur. De même que tel exemplaire de *l'Éthique à Nicomaque* d'Aristote est une chose en tant que livre occupant une certaine place sur telle étagère, mais que le texte lui-même peut en être indéfiniment reproduit partout grâce au protocole ouvert qu'est l'alphabet, et qu'à la limite il peut même être mémorisé mentalement par plusieurs esprits différents.

Mais si l'on parle du bitcoin en tant qu'il est inscrit dans son registre désormais considéré comme un univers propre (au sens où l'on parlera, par exemple, d'un « personnage de roman »), la somme en bitcoin inscrite à mon adresse *16aSqT2bw…* ou bien si l'on veut la somme des entités numériques valorisées en bitcoin et inscrites à cette

adresse, possède des caractéristiques similaires à celles d'une chose physique : elle peut être appréhendée de manière sensible par la vue sur écran autant que de manière numérique avec une fonction de recherche ; les entités inscrites à cette adresse ne peuvent être inventoriées qu'à cette adresse et elles peuvent être mues vers une autre adresse du même univers pour y demeurer, ce qui est une caractéristique physique (selon Aristote, est dit physique ce qui contient en lui-même un principe de mouvement et de repos).

Le fait que les objets ne puissent (du moins à l'échelle macroscopique) être à deux endroits à la fois résout physiquement le problème moral de la double dépense : si une pièce d'or n'a pas d'odeur, elle a une couleur, on peut la prendre entre les doigts, et, surtout, elle ne peut être à deux endroits à la fois, dans la poche du débiteur et dans celle du créditeur. Son transfert fait paiement.

L'entité bitcoin, sur sa *blockchain*, quoique de nature entièrement numérique et sans support matériel unique, a pourtant exactement la même caractéristique. Cette entité ayant les propriétés physiques d'une chose est répertoriée, exprimée, libellée dans une unité de compte propre à l'univers où elle existe : à défaut d'être une monnaie (ce que l'on verra plus loin) c'est au minimum un jeton monétaire dont la substance est non pas une matière précieuse ou vile mais une (grande) quantité d'information vérifiable, qui joue en quelque sorte le rôle d'un minerai précieux.

C'est de ce jeton monétaire à la substance informatique-mathématique que nous souhaitons ici souligner quelques étonnantes propriétés physiques.

Une pièce d'or n'a pas de mémoire. Dans l'Evangile, quand Jésus examine le denier qu'on lui montre, il ne peut en identifier que l'origine, l'effigie de l'empereur[23]. Le bitcoin, qui est de l'information frappée, représente une forme de mémoire.

Un bout de bitcoin est d'abord (mais on verra qu'il ne l'est pas seulement) ce que les historiens appellent un objet épigraphique, c'est-à-dire qui porte des inscriptions permettant d'en retracer l'histoire. Autrefois, quand il était possible d'endosser un chèque au profit d'un tiers, on pouvait voir un chèque portant deux ou trois endos, et reconstituer son trajet, son histoire. Sur la *blockchain*, chaque fraction d'entité bitcoin peut être historiquement tracée depuis le bloc à l'occasion duquel ces bitcoins ont été créés en récompense du processus de validation. Certains de ces endos sont facilement reconnaissables (si ces bitcoins sont passés par des sites illégaux dont la police connaît l'adresse, par exemple) mais la plupart sont protégés par le caractère pseudonyme des transactions. L'histoire claire de ces endos ne peut être reconstituée que par des algorithmes puissants, l'analyse complète d'un *wallet*, fût-ce sur un nombre assez restreint de transactions précédentes, ne peut être que statistique : elle va s'exprimer comme un tableau coloré représentant une sorte de nébuleuse de transactions, sauf évidemment si l'on cherche à tracer une transaction précise.

Mais ce qui est fondamental, c'est que cet historique est certain (chaque étape a été vérifiée en son temps), irréversible (on ne peut valider une étape ultérieure visant à modifier frauduleusement et a posteriori une étape antérieure, c'est ce que sous-entend l'expression « *chaîne* de blocs »), autonome (la succession linéaire des blocs suscite le premier temps universel propre au cyberespace, sa première chronologie) et enfin indissociable de la « chose ». Une analogie possible avec le monde physique serait par exemple celle de la cristallisation d'une roche. La cristallographie est (en ce qui concerne les changements du climat, ou la position du pôle magnétique) un livre d'histoire infalsifiable, car on peut détruire un cristal plus facilement que d'en modifier les plans de clivage…

Puisque nous en sommes à l'histoire, il faut noter que c'est par une réflexion proprement « historique », que Bayer, Haber et Stornetta en sont arrivés en 1993 à construire un horodatage numérique intrinsèque : « pour établir qu'un document a été créé après un moment donné, il est nécessaire de rapporter des événements qui n'auraient pu être prédits avant qu'ils ne soient arrivés. Pour établir qu'un document a été créé après un moment donné, il est nécessaire de provoquer un événement suscité par ce document et qui puisse être constaté par des tiers[24]. » Le vieux sophisme *post hoc ergo propter hoc* trouve enfin ici un fondement technique.

La flèche du temps règne aussi en maîtresse sur la thermodynamique. Et, techniquement, pour citer l'un des plus éminents connaisseurs français, le polytechnicien Pierre Noizat, « la seconde loi de la thermodynamique et la limite de Landauer imposent une consommation d'énergie minimale pour un processus de calcul irréversible comme l'ajout d'un bloc à une chaîne de blocs : chaque confirmation d'une transaction précédente correspond à une diminution de l'entropie du système. Plus il y a de blocs qui confirment une transaction, plus cette transaction est froide, gelée dans l'historique global des transactions à l'intérieur du système, et moins elle est susceptible d'être invalidée dans le futur par une réécriture partielle de la chaîne des blocs[25]. »

Il est tentant de garder cette métaphore cristalline pour aborder une autre caractéristique « physique » de bitcoin : sa transparence. Les transactions, dont la mémoire est figée au moment de la validation, ne sont pas enregistrées une à une et seulement ordonnées par un ordre chronologique pauvre en informations. Les transactions sont regroupées par blocs, un bloc toute les dix minutes environ. Au commencement, les blocs regroupaient seulement quelques transactions, ou quelques dizaines tout au plus ; c'est en mai 2012 que le seuil de 100 transactions (en dix minutes, au niveau mondial) a été franchi, le seuil des 1 000 mettra trois ans de plus à être atteint. En 2016, ce chiffre s'élevait autour de 1500 pour atteindre en fin d'année le seuil des 2 000[26].

Comme cela a été dit, les données des transactions font l'objet d'un traitement consistant à calculer à l'aide d'une fonction dite de « hashage » une empreinte numérique hexadécimale (64 lettres de a à f ou chiffres de 0 à 9) qui sera unique (si on fait deux fois la même opération sur le même fichier on obtient aisément, et en un instant, à chaque fois le même résultat : on dit que la fonction est déterministe) et irréversible (de ces 64 signes, on ne remontera jamais aux données « en clair »). Mais ce hashage n'est pas fait dans le désordre ou à la queue-leu-leu : on réunit les données des transactions par paires, puis on hashe de nouveau par paires les résultats des hash des transactions, puis de nouveau par paires les résultats précédents, etc. Chaque niveau supérieur intègre donc les données d'un nombre croissant hyperboliquement de transactions, et au sommet on obtient un hash de tête intégrant les données de centaines ou de milliers de transactions, ainsi que le hash de tête du bloc précédent. Cette structure en « arbre » porte le nom d'arbre de Merkle, du nom de son inventeur l'informaticien et cryptographe américain Ralph Merkle en 1979[27]. Le hashage de tête de chaque bloc s'appelle la « racine de Merkle » ou parfois la « somme de contrôle ».

Cette racine de Merkle, qui permet d'authentifier un bloc gigantesque d'information en une seule opération, peut s'appliquer non seulement à la vérification d'un bloc de milliers de transactions, mais elle pourrait aussi, par exemple, permettre aux clients d'une future « banque bitcoin » pratiquant le « full reserve banking », c'est-à-dire ne prêtant que l'argent qu'elle a vraiment, de s'assurer en une seule opération de la véracité des bilans (total des dépôts), rendant possible un changement de paradigme dans la relation.

Ces propriétés « physiques » garantissent des transactions d'une étonnante fluidité. La « vérification simple du paiement » (SPV selon l'acronyme en anglais) permet une connexion très rapide au réseau de *wallets* fonctionnant sur un mode dit « léger ». L'opérateur de chaque nœud du réseau peut en effet décider d'installer un nœud complet qui construit et tient à jour un exemplaire local de la *blockchain*, ou se contenter d'un nœud léger qui fait appel aux nœuds complets pour valider les transactions en utilisant le protocole SPV, c'est-à-dire en ne téléchargeant que les empreintes de tête des blocs, ce qui permet une mise à jour presqu'instantanée, même en cas de connexions très espacées.

Bitcoin possède à la fois (c'est le propre des métaphores cohérentes) la structure et la transparence du cristal. À ce niveau on peut avancer qu'un bout de bitcoin n'est pas un simple « objet épigraphique ». Sa matière même est l'écriture, l'information, non point dans un état de nature (comme le minerai pour le métal) ou amorphe, mais travaillée pour la rendre transparente et sûre, par de l'énergie dont le coût est aussi cristallisé dans le jeton.

Satoshi Nakamoto l'annonçait déjà dans sa définition donnée en octobre 2008, définition qu'il nous a paru plus judicieux de ne citer qu'en conclusion pour que le lecteur puisse maintenant en goûter pleinement la portée : « Nous définissons une pièce électronique comme une chaîne de signatures numériques. Tout propriétaire transfère cette pièce à un autre en signant numériquement une empreinte de la précédente transaction ainsi que la clef publique du nouveau propriétaire et les ajoute à la fin de la pièce. Tout bénéficiaire peut examiner les signatures pour vérifier la chaîne de propriété.[28] »

3- Une création révolutionnaire cause d'enthousiasme ou de scandale

La genèse du Bitcoin : un renversement des idées reçues sur la monnaie

La monnaie, chose subtile, se donne pourtant à voir de façon triviale, en témoigne le nombre incroyable d'expressions imagées ou argotiques qui la désignent.

Profitons de cette richesse linguistique pour commencer l'exploration des idées qui, comme les espèces elles-mêmes, ont cours en société. Certains mots en appellent à l'archéologie de la monnaie (*le blé*, *un sac, une barre*), évoquent des espèces révolues (*la maille*, *le sou*, *la thune*) ou ne font parfois allusion qu'à la couleur du métal noble (du *jaunet*) ou vil (du *grisbi*). Dans la langue, elle est toujours *liquide* et circule sous une forme (le *pognon* que l'on tient à pleine poignée) ou sous une autre (le *bifton* que les plus jeunes nomment *bif*) sans qu'aucun terme ne fasse encore allusion à sa numérisation qui fait échapper la monnaie à l'empire des sens.

Certains noms d'origine ancienne (*balle* a déjà cours en 1655 et se recycle aujourd'hui en *boule*) ou plus récente (*brouzouf* dans une BD de SF en 1967) ont une étymologie obscure. Qu'importe : pour l'argent on se comprend toujours, et parfois à demi-mot tant il est symboliquement fort et n'utilise les mots que comme un support interchangeable, conformément à l'idée de Saussure qui les définit comme des pièces de monnaie fiduciaire, sans valeur significative intrinsèque.

Mais quand on présente Bitcoin, on ne se comprend pas si bien. Il est difficile de dire de but en blanc que c'est une monnaie : n'est pas Aristote qui veut et la plupart des gens appréhendent davantage la monnaie par ses apparences et ses représentations que par l'analyse de ses fonctions.

La monnaie fait partie des choses essentielles sur lesquelles la grande majorité des bacheliers ne se sont pas penchés une heure. Son fonctionnement, comme celui des banques, reste un mystère insoupçonné. D'autre part nos compatriotes vivent depuis la fin de la dernière guerre avec une monnaie (franc puis euro) unique et en outre (relativement) stable depuis un quart de siècle. Cette situation confortable rend la monnaie comme transparente. Des gens moins instruits, dans des pays où le gouvernement et sa monnaie peuvent changer deux fois dans l'année, savent parfaitement faire des arbitrages sur deux ou trois monnaies. C'est parfois une question de survie.

Les nombreuses présentations effectuées par les membres du « Cercle du Coin » auprès des publics les plus divers fournissent autant d'occasions de mesurer les incompréhensions et les scandales que suscite le bitcoin, le plus souvent parce qu'il renverse des idées reçues sur la monnaie que nous allons ici tenter de passer en revue.

D'abord, le bitcoin n'est pas « accroché » à l'euro comme le sont les monnaies locales complémentaires dont le fonctionnement est complaisamment décrit par la télévision et qui, pour chaque billet émis, conservent un billet en euro dans le tiroir-caisse. De son côté, le bitcoin semble manquer de contrepartie sérieuse. D'où peut lui venir une quelconque valeur ?

Par ailleurs le bitcoin n'est pas « garanti ». La nature et la portée de la garantie que les gens ont à l'esprit sont souvent assez floues. Plus précisément, le bitcoin n'a pas, comme l'euro ou le dollar, « la garantie d'un État ». Il y a là une confusion entre la garantie qu'une monnaie officielle conserve son usage pratique, pour payer et rembourser, et la garantie toute différente que cette monnaie garde sa valeur.

La première ne tient pas à la « confiance en notre monnaie » si souvent invoquée, mais au cours forcé de la monnaie officielle. Ce qui donne son efficacité à la monnaie officielle, ce n'est pas la confiance du citoyen ou celle de l'épicier, comme le dit la bibliothèque rose de l'économie, c'est le fait que le percepteur exige cette monnaie. Le fisc est, comme le savait Jésus, la raison d'être et le vrai fondement de la monnaie de César. Un euro permet de payer un euro d'impôt, l'une des plus universelles dépenses. *In tax we trust*. Encore faut-il noter qu'un billet de 5 euros peut être démonétisé et ne vaudra plus rien, tandis qu'un bitcoin vaudra toujours un bitcoin.

La seconde garantie, celle qui porterait sur la valeur, n'existe simplement pas. D'abord parce qu'il n'est pas du ressort de l'État mais bien de la Banque Centrale d'assurer la stabilité des prix. Ensuite, parce que si globalement le pouvoir d'achat du billet en euro se maintient au supermarché, peut-on en dire autant chez l'agent immobilier ? Et puis la valeur de notre argent doit aussi s'apprécier internationalement. Au cours de l'année 2015, l'euro a perdu de la valeur pour celui qui était amené à le dépenser en Suisse, en 2016 il en a gagné pour celui qui se rendait à Londres. Les autorités parlent toujours de l'argent comme si le leur était le seul sur terre, éludant tant la possibilité pratique de stocker du cash en devise que le débat théorique que la base monétaire[29]. Et enfin il y a l'or, certes démonétisé mais qui joue toujours un rôle important dans les échanges… entre les banques centrales elles-mêmes. Et, en pratique, pièces et lingots existent toujours. Quoi qu'il en soit, le même euro qui permet d'acquérir trois fois moins de mètres carrés parisiens qu'à sa naissance ne permet plus d'acquérir que le quart du poids d'or d'alors. Quelle valeur conserve-t-il réellement dans le temps ?

Mais, nous-dit-on, la valeur non garantie du bitcoin « fluctue » et est forcément « spéculative ». Rappelons que dans un monde où les devises, le blé, le pétrole et le prix du billet de train, varient de minute en minute, et où

la valeur de marché est cependant censée en tout et pour tout donner la vraie valeur des choses (en dépit parfois de l'évidence, mais telles sont les normes comptables désormais), le fait que la valeur du bitcoin soit donnée, comme celle de l'or par exemple, par le rapprochement des cours constatés sur les principales plateformes d'échange n'est pas un scandale inouï. D'autant plus que le bitcoin subit déjà nombre d'opérations d'arbitrage qui maintiennent son cours quasi-égal entre les principales plateformes.

Le bitcoin n'est pas émis par une Banque Centrale qui en contrôlerait le volume. C'est exact, mais c'est tout autant le cas pour 90 % de la masse monétaire de l'Euroland.[30] La conscience de la création monétaire *ex nihilo* par les établissements de crédit est encore peu répandue et progresse lentement. Ceux-là même qui ont compris que l'argent n'est pas de l'or (le dollar flotte dans le vide depuis 1971, il arrive d'avoir à le rappeler) pensent parfois qu'il y a quand même quelque chose en banque, au moins des billets dans le coffre, comme dans les albums de *Lucky Luke*. Et même parmi ceux qui se sont libérés des représentations sensibles, ils sont loin d'être rares ceux qui pensent que l'argent que la banque leur prête vient de l'épargne de leurs parents et voisins. Il est pourtant loin, le temps de la banque de dépôt !

Tout est fait en vérité pour encourager cette croyance qui exonère le système bancaire en en faisant un simple intermédiaire, rémunéré pour sa prudence. On a vu un patron de banque déclarer devant une commission parlementaire : « Nous ne pouvons créer de l'argent. Il nous faut le collecter à travers les dépôts des particuliers et des entreprises ainsi que par des émissions sur les marchés.[31] ». Même si toutes les personnes qui se donnent la peine de chercher le savent, même si des analystes[32] de la Banque d'Angleterre (la mère des banques centrales !) ont enfin publié en mai 2015 une note affirmant que les banques ne sont pas des intermédiaires transformant ou multipliant les dépôts pour créer des crédits, cela reste la représentation dominante. Que les crédits soient consentis en monnaie créée *ex nihilo*, que l'activité industrielle et commerciale transforme ensuite en dépôts dans d'autres banques, que ce soit cet argent créé *ex nihilo* qui nous serve à tous de monnaie reste une connaissance ésotérique.

Le bitcoin n'est ni créé ni conservé par ou chez une banque régulée. Ce reproche va de pair avec le précédent ; il est cependant plus aisé de mettre en lumière l'avantage de la chose. Certes conserver l'argent en banque est plus commode, et généralement plus sûr, que de l'avoir sous le matelas, nul n'en disconvient. Mais au fil des ans la porte blindée de la banque semble être devenue celle d'une prison : impossible de recevoir un salaire ou un paiement ailleurs qu'en banque, impossible de retirer en liquide au-delà de sommes de plus en plus limitées, voire en se justifiant, incertitude sur les garanties, délais dans les transferts. Nous vivons une véritable dépossession de l'argent. L'argent des Français doit être et rester dans des banques qui, à l'exception notable de la Banque Postale, ont toutes des activités de marché. Sous prétexte de libre concurrence, on a fermé les comptes de particuliers jadis gérés par la Banque de France, le Trésor ou le Crédit Municipal. Et l'argent déposé sur un compte Nickel était au Crédit Mutuel avant d'être vendu à BNP Paribas.

On abordera plus loin les problèmes que cela pose en termes de vie privée. Quelle est la valeur de la garantie offerte en contrepartie de cette servitude bancaire ? Faible. Celle-ci n'est pas vraiment accordée par l'État mais par un Fonds de Garantie capitalisé de 3 milliards, soit une vingtaine d'euros pour chacun des 140 millions de comptes de particulier. La littérature officielle à ce sujet est lénifiante, et celle des chercheurs universitaires (mais prudents) tout autant. La possibilité d'une ruée vers les guichets est parfois ramenée à celle du film *Mary Poppins* et donc « purement psychologique ». Au fait, revoyez bien le film… et songez aux agitations médiatiques suscitées il y a quelques années par les appels d'Éric Cantona à retirer massivement aux distributeurs et aux guichets des banques.

Qui prend la peine de lire les flyers en petits caractères joints à l'extrait de compte mensuel ? Combien ont compris les modifications des règles du Fonds de Garantie ou les conséquences de la transposition par ordonnance en 2015 de la *directive relative au redressement des banques et à la résolution de leurs défaillances* ? Combien de Français croient posséder les euros qui apparaissent en bas de page de leur relevé, alors qu'ils n'ont qu'une créance de ce montant sur cette banque ?

Revenons au bitcoin. Il n'est pas « tangible ». On ne le tient pas entre ses doigts. Du coup, n'étant ni dans la poche, ni dans la banque, il ne serait probablement nulle part. Derrière cette notion d'argent tangible (le petit geste du pouce frottant l'index !) se cachent bien des enjeux.

Nos ancêtres, à trois ou quatre générations de nous, guère plus, ont vécu avec une forme de monnaie tangible, qui paraissait naturelle et saine depuis des siècles : des morceaux de métal précieux, dont l'État garantissait le poids et l'aloi en leur imprimant ses symboles. Quels qu'aient pu être les limites, les contraintes et

les défauts de ce système, il faut revenir sur une évidence oubliée : qui possède une pièce d'or la possède vraiment tant qu'il ne l'a pas aliénée ou qu'on ne lui a pas volée. Les banques émirent des billets, payables ou remboursables en métal. Ceux que le système inquiétait (pour de bonnes ou de mauvaises raisons) dénoncèrent surtout la multiplication de billets que permettait la tolérance légale accordée aux banques de n'avoir que des réserves fractionnaires pour émettre une sorte de fausse monnaie[33] seulement assise sur la confiance naïve des citoyens. Mais il y a autre chose : celui qui a en main un billet même remboursable (ce qu'ils ne sont plus depuis bien longtemps !) ne possède déjà plus de l'or mais une créance (en or) sur la banque. Aujourd'hui on dirait qu'il ne possède qu'un IOU (*I owe you*, « je vous dois » en anglais).

Toute l'astuce du système consiste, en laissant circuler quelques billets (fiduciaires), à laisser croire que l'énorme amas de monnaie scripturale, qui n'est plus elle-même que très marginalement convertible en cette monnaie émise par la Banque centrale, a la même nature, et qu'il est lui-aussi « tangible ». Mais tangible ou pas, même le billet de banque n'est jamais qu'un bout de dette et de papier inconvertible.

Le bitcoin n'est pas tangible avec les doigts. Mais avec un protocole informatique, celui qui le contrôle en fait lui-même ce qui lui plait (virement, paiement, transfert ou don) sans avoir à demander à un tiers de le faire, ou la permission de le faire. Dans le cyberespace, le bitcoin est tangible. Et surtout, il est indépendant de toute relation débitrice. C'est une monnaie-valeur. Bien heureux aurait sans doute été Platon de cette « monnaie-idée », valeur intrinsèque qui n'existe que par essence sans jamais être une représentation plus ou moins fiduciaire d'une valeur extrinsèque.

À la fin d'une présentation théorique, quand l'auditoire est encore plein de doutes, rien ne vaut d'installer quelques « portefeuilles » virtuels sur les téléphones de deux ou trois volontaires. Cela prend trois minutes. Puis, en moins d'une minute, d'envoyer pour un euro de bitcoin au premier d'entre eux, et de lui demander de l'envoyer au second et ainsi de suite. À voir ainsi cette étrange monnaie passer d'un téléphone à l'autre en si peu de temps, les plus sceptiques comprennent que, électroniquement tangible, elle est bien réelle. Sans doute ont-ils, un jour, dû rappeler leur banque trois jours durant pour s'assurer qu'un virement avait bien été crédité ?

Un instrument de transaction à l'anonymat relatif et à la transparence incontestable

Pourquoi se cacher ? Le bitcoin n'est-il, avec ses transactions sous pseudonymes, qu'une monnaie pour faire de sales coups ? Difficile d'évoquer le bitcoin sans avoir à se défendre d'une impressionnante série de méfaits. Il faut sans cesse rappeler que, si la totalité des bitcoins ne servaient qu'au trafic de stupéfiants, ils n'en représenteraient guère plus de 3 %, et que ce trafic doit bien être fait en grosses coupures (les seuls billets de 500 euros représentent 30 fois la valeur de tous les bitcoins) et par le système bancaire mondial. Ensuite, il faut rappeler que si tant de politiciens en quête de bouc émissaire dénoncent le bitcoin comme monnaie des organisations terroristes, les spécialistes d'Europol se montrent bien plus nuancés[34].

Nous reviendrons au point III, 1 sur les mauvaises fréquentations qu'il ne s'agit évidemment pas d'éluder et sur quelques crapuleries qui ont aussi valeur d'enseignement. Mais commencer par-là est une démarche polémique et surtout stérile car elle ne permet ni de comprendre la valeur du mode pseudonyme des transactions en bitcoin du point de vue politique, comme du point de vue du légitime secret des affaires voire des mœurs, ni sa raison d'être à l'aune de la solidité du système de transactions lui-même.

La dimension politique est aisée à présenter. En tant qu'être politique, chacun a le droit de publier ce qu'il pense (dans le respect des lois), mais en tant qu'être humain doté d'une intimité, d'une vie affective ou sociale, il a aussi le droit de garder pour lui ou de contrôler la diffusion de certaines choses, pudiques ou intimes. Chacun a aussi à gérer des relations asymétriques avec des partenaires dont il peut ne pas souhaiter qu'ils disposent de trop d'informations sur lui, comme son employeur. S'il est loisible à un tiers (État, patron, grandes compagnies et leur marketing) de tout savoir de chacun, quel reproche pourra-t-on faire à celui qui choisit de se promener nu dans la rue ?

Or dans un monde où il n'y a pas de repas gratuit, les factures sont des archives complètes de nos vies. Que la banque conserve des archives détaillées de nos repas au restaurant, de nos déplacements, de nos abonnements et de toutes nos dépenses est une forme de viol de notre intimité. Mais rien ne justifie que nous perdions pour autant les services numériques de la monnaie tels que l'historique de nos transactions, tant qu'il est pour nous

seuls. La confidentialité des transactions est indissociable de la vie privée. Elle était totale et naturelle du temps des espèces et finalement assez grande du temps du chèque. Cela n'a pas empêché le monde libre de survivre alors à bien des menaces, et l'économie de connaître une croissance plus forte qu'aujourd'hui !

Mais cette défense politique est aussi aisée à mettre entre parenthèses. L'État n'a aucun mal à plaider l'importance qu'il y a pour notre sécurité à surveiller certains, dont la liste est secrète, pour un temps dont le terme n'est jamais clairement fixé, et sous le contrôle d'un juge qui est peut-être débordé ou en campagne électorale. L'État clamant qu'il défend nos valeurs – sans jamais en donner une liste explicite – le plus grand nombre admet le procédé, oublieux du fait avéré que tout pouvoir tend à l'abus de pouvoir, et qu'en matière de surveillance l'abus de pouvoir tend à supprimer les contre-pouvoirs. Quant aux grandes sociétés et aux réseaux sociaux, ils accumulent une information pléthorique en nous entretenant dans une forme de bétaillère ludique. Les tyrans de la Boétie deviennent non pas les souverains, mais les empires numériques auxquels nous offrons notre *servitude volontaire*[35].

Donc si l'affaire était uniquement politique le combat serait perdu d'avance, parce que la liberté est la seconde victime des attentats, que la technologie se déploie plus rapidement que la réflexion sur ses conséquences et que la surveillance est aussi mutuelle et horizontale, participative, en réseau.

Seulement le secret est aussi le talon d'Achille des affaires et même, si l'on peut filer la métaphore, ses deux talons : les sociétés qui s'engraissent de nos propres secrets n'ont aucune envie que ni ces données ni les leurs se retrouvent sur la place publique, dans les serveurs de leurs concurrents ou ceux d'un pirate. Le scandale *Ashley Madison* peut illustrer ce double aspect. À l'été 2015, des hackers firent main basse sur la quasi-totalité des informations personnelles des 37 millions de membres inscrits sur ce site qui vendait la perspective de rencontres adultères tout en vantant explicitement sa capacité à conserver ces secrets. Quand les pirates mirent en ligne les secrets volés, on vit quelques suicides, des démissions, des déclarations pathétiques (notamment de conservateurs américains dotés peu de temps avant d'une solide image de père-la-vertu) et sans doute une multiplication de chantages en tous ordres. Mais on put aussi voir les secrets de l'entreprise elle-même : sa sécurité très limitée et son recours massif à des robots pour suppléer le nombre trop faible de profils féminins. Pas plus tard qu'en novembre 2016 ce sont plus de 400 millions de comptes qui sont piratés sur *AdultFriendFinder* dont plus de 5 000 adresses en « .gov » et 900 000 mots de passe « 123456 »[36].

Les grands secrets sont-ils mieux gardés ? Inutile de rappeler que le fisc français, le Pentagone, et bien sûr les grandes banques, ont déjà été hackés un très grand nombre de fois. Il est comique de voir les mêmes politiciens dénoncer le cryptage des téléphones et s'indigner des publications sur WikiLeaks. On constate ainsi clairement un énorme manque de sérieux concernant la sécurité informatique, même dans les plus hautes instances de l'État.

Aussi, dans le monde des affaires et de la finance, tout en jetant un discrédit méprisant sur le Bitcoin, on ne tarit pas d'éloge sur « la technologie qui est derrière », la fameuse *blockchain* dont il sera question plus loin. C'est que l'idée de gérer ses bases de données (chacun pour son compte, évidemment) d'une manière plus confidentielle n'est pas forcément pour déplaire, bien que partiellement illusoire.

C'est aussi que les transactions sous pseudonymes, si elles sont un droit politique et une précaution dans les affaires, sont un élément de l'architecture décentralisée qui fait le vrai « blindage » du système de bitcoin. C'est, de loin, le point le plus subtil à saisir.

Revenons aux transactions : pourquoi a-t-on besoin d'intermédiaires ? Parce que nous n'avons pas sur nous de valeur tangible à remettre comptant, ou bien parce que nous souhaitons envoyer de l'argent au loin sans avoir à nous déplacer. L'intermédiaire qui fait le paiement est nécessaire car le type de monnaie dont nous disposons n'est ni tangible ni téléportable. Or, dans le cyberespace, le bitcoin est, comme nous le verrons, tangible et transférable en quelques secondes. En effet, ce n'est pas le bitcoin qui est déplacé mais uniquement son propriétaire qui change.

Pourquoi les données conservées chez un intermédiaire ne sont-elles jamais en sécurité ? Parce qu'elles sont conservées dans des bases de données uniques, sur des serveurs identifiables, et souvent en clair ou avec un niveau de chiffrement dérisoire, la clef étant elle-même conservée sur un site ou dans un fichier identifiable. Or, sans anticiper sur les explications techniques qui seront données au point II, 1, le fonctionnement de la base de données du bitcoin est radicalement différente à de nombreux égards, dont deux qui font ici une différence essentielle : la clef des données est chez l'utilisateur (non dans la base) et la base n'est pas dans un coffre-fort informatique mais en accès libre et dupliquée dans des milliers d'ordinateurs.

Imaginez un compte bitcoin comme une boite aux lettres physique ou électronique dont tout le monde connaitrait l'adresse (*Monsieur Tintin, 26 rue du Labrador* ou *dupont@dupondt.be*), à laquelle tout le monde pourrait adresser un chèque, mais dont bien sûr seul celui qui a la clef ou le mot de passe pourrait récupérer et dépenser l'argent reçu.

Ce compte bitcoin est en fait une ligne dans un livre de millions de lignes. Tant qu'il demeure inactif, il n'apparaît pas publiquement dans le livre. Mais dès qu'une transaction a lieu l'adresse bitcoin est inscrite dans le livre. Elle ressemble en fait à une série de 34 lettres ou chiffres, comme cela : 3Jb8QpPh5BickgUGvXLfTY58wn2jXoj9sh.



À vot' bon cœur ! (expérience)

Si le téléphone du lecteur lit le flash-code ci-contre, il ira vérifier que cette adresse existe et, s'il est doté d'un portefeuille bitcoin, il pourra lui envoyer ce qu'il veut en signe d'amitié. Ne vous inquiétez pas, cette adresse est partagée par les deux auteurs qui devront s'entendre pour évacuer les fonds !

En fait, ni celui qui envoie du bitcoin à cette adresse ni celui qui en reçoit ne savent s'ils traitent vraiment avec Tintin. Cela pourrait être les Dupondt (car il peut y avoir des comptes-joints à double signature, comme le nôtre) ou Tchang à l'autre bout du monde. En fait, cela pourrait même être une machine (connectée) inventée par Tournesol, car une machine dénuée de personnalité juridique mais dotée d'une capacité de calcul et d'une connexion peut parfaitement mener une transaction.

En revanche, tous ceux qui connaissent l'adresse 3Jb8QpPh5BickgUGvXLfTY58wn2jXoj9sh peuvent, très aisément, en un clic, savoir depuis quand cette adresse existe en tant qu'écriture, combien elle a reçu ou envoyé de fonds. Mais on ne connaîtra que des transactions entre adresses chiffrées : on saura que telle adresse a envoyé 0,06 bitcoin à l'adresse *1EEevW3…* non que son détenteur a dépensé 60 euros pour acheter une bouteille de Loch Lomond (sans doute pour un vieil ami) parce que cela ne regarde personne.

Mais même si l'on découvre sur une adresse plusieurs milliers de bitcoin, seul le détenteur de l'adresse connaît la clef lui permettant de débiter cette adresse. En un milliard d'années et avec une énorme machine, nul ne pourrait deviner ou calculer cette clef. Elle ressemble à une série longue de 51 ou 52 lettres ou chiffres[37]. Il existe des millions de fois plus de solutions que de molécules d'eau sur terre.[38] Entre cette série longue et la série plus courte, il y a plusieurs fonctions mathématiques à sens unique. Celui qui connaît la cinquantaine de signes peut obtenir la trentaine en un clic. Celui qui n'a que les 34 signes ne connaîtra jamais la cinquantaine. Si le détenteur de la clef (la série de 51 ou 52 signes) la conserve en dehors de son ordinateur (en marge de la planche 24 de *Vol 714 pour Sydney…* ou sur une clef USB) aucun espion, pirate ou gouvernement ne pourra ni connaître cette clef, ni manœuvrer des sommes sur l'adresse correspondante.

Revenons sur la seconde différence radicale citée plus-haut. Le livre qui recense les euros du lecteur dans sa banque est à l'abri dans les serveurs de ladite banque, avec toutes les sécurités au dernier cri, attendant le prochain pirate. En attendant, le banquier, le fisc, l'Urssaf, Pôle emploi, la police, les douanes, l'AMF, les agrégateurs bancaires… peuvent lire ces écritures (en clair) tout à loisir. Le livre qui recense les bitcoins est téléchargeable par quiconque, et quoi qu'il soit assez lourd (100 milliards d'octets à la fin de 2016, à peu près 100 Go[39]) des milliers d'ordinateurs en ont la copie, mise à jour automatiquement toutes les dix minutes. Nous expliquerons au point II, 1 ce qui le rend inviolable, ou plutôt comment sa falsification serait d'un coût incommensurable. À défaut de télécharger tout le livre, il est possible sur certaines plateformes d'explorer l'adresse de son choix (avec toutes les transactions enregistrées), suivre toute la vie d'une partie de bitcoin depuis son origine, retrouver les transactions de l'avant-veille à 17 heures ou celles portant sur une somme de 0,23 bitcoin, etc. Tout est en clair et public parce que tout est pseudonyme.

Quelles sont les conséquences en terme de vie privée (ou de criminalité, pour nos lecteurs ministres) de ce caractère pseudonymes des écritures ? Il est difficile de donner un point de vue unique et définitif. L'expérience Bitcoin est loin d'être figée. Tel que nous l'avons décrit ici, en son état natif, le bitcoin nous semble pouvoir être décrit comme un moyen de paiement discret, apte à protéger la vie privée, plus que secret.[40] Ceux qui ont fait le pari qu'il assurerait le secret à leurs entreprises illégales ou criminelles dorment en prison.

À un moment ou à un autre, l'une des adresses peut être identifiée par recoupement et triangulation (si quelqu'un verse l'argent de poche en bitcoin à son fils et que tous deux jouent au poker en ligne sur le même site, chacun des deux aura du mal à le nier…). Chaque poussière de bitcoin a une histoire, qui peut être retracée depuis son origine.

A lieu une course parallèle au sujet de l'anonymisation des transactions entre des développeurs qui mettent au point des logiciels automatisant le traçage, dans l'espoir de rendre le bitcoin compatible avec la politique de KYC (*know your customer*) des banques, et d'autres qui inventent des procédés pour rendre les transactions plus difficiles à tracer, notamment en associant non pas une adresse unique mais plusieurs adresses publiques à chaque clef privée. Mais, encore une fois, comme le disent en souriant les vrais responsables de la traque des criminels : rien ne vaut l'anonymat des grosses coupures, honorablement émises par les banques centrales. Il reste qu'elles ne sont pas, comme le bitcoin, programmables et que leur nombre n'est pas, comme celui du bitcoin, précisément fixé.

Les enjeux d'une monnaie sans État et sans banque : une confiance inédite

Le bitcoin est, dans sa construction, une monnaie sans État et sans banque. Scandale pour certains, progrès pour d'autres, il faut dans tous les cas en analyser les conséquences.

Comment, demandent ses détracteurs, pourrait-il inspirer la confiance sans le prestige de l'autorité régalienne ? Comment, suggèrent les banques, pourrait-on faire confiance à un système sans guichets, sans conseillers, mais aussi sans régulation ni responsabilités établies ?

À ces objections nous répondons en commençant par une réflexion sur ce qu'est la confiance et sur ce qu'elle n'est pas, et revenons donc sur la présentation de la confiance comme naturellement suscitée et entretenue par une institution tierce et centralisée bénéficiant de l'onction de la puissance publique. Ce paradigme, largement inspiré par les institutions elles-mêmes, élude superbement l'ancestrale méfiance de l'épargnant vis-à-vis des pouvoirs publics ou l'animosité que suscite la position exceptionnelle des banques.

Les hommes se font d'abord confiance l'un à l'autre. On ne recompte pas une liasse de billets remise par un ami. Quand on ne partage pas une addition on dit « je te revaudrai ça ! ». *Confiance* a la même racine latine que *confidence* : elle est de nature intime. Au-delà du premier cercle, elle est historiquement de nature ethnique ou religieuse, ce qui explique les liens familiaux et religieux dans certaines communautés de marchands (lombards, juifs, ismaéliens, gujaratis).

Or la puissance publique n'est pas de nature intime, ethnique ou religieuse. L'idée selon laquelle l'autorité publique serait le fondement de la confiance dans la monnaie est un mythe enjolivant le cours forcé. À plus forte raison, un groupe bancaire, inextricable réseau de sociétés *anonymes*, ne saurait créer autre chose que des liens de clientèle, quels que soit les efforts pour maquiller cette relation commerciale en *communauté*. Payer avec une carte de fidélité plutôt qu'en cash ne crée pas de *relations humaines*. Le tiers de confiance n'est jamais qu'un intermédiaire, qui comme tel prélève sa part sur le labeur, les biens et désormais les secrets d'autrui. Court-circuiter les intermédiaires quand c'est possible est de bonne guerre.

Utiliser le bitcoin suppose deux formes de confiance différentes pour remplacer respectivement la banque et l'État.

D'abord une confiance rationnelle dans la validité d'une transaction, c'est-à-dire dans sa loyauté et son irréversibilité. Cette confiance repose elle-même sur la compréhension de deux choses qui seront expliquées plus tard : la nature spécifiquement mathématique du processus de validation et la cohérence intrinsèque de chaque écriture avec l'ensemble du registre (la *blockchain*). Les *bitcoineurs* se reconnaissent dans une devise latine, *Vires in numeris,* que l'on pourrait traduire par « la force est dans les chiffres », non sans un débat de grammairien sur

l'opportunité discutable du pluriel, certains sous-entendant que *vires* au lieu de *vis* désigne ici les forces militaires. En somme, une réponse à la question « Bitcoin, combien de bataillons » *?*

La force des chiffres, c'est la résistance des objets mathématiques (le logarithme discret dans la cryptographie sur courbes elliptiques) mais aussi la puissance de calcul du réseau, supérieure de plusieurs centaines de fois à la puissance combinée des 500 plus gros ordinateurs connus[41], et utilisant une puissance qui est peut-être de l'ordre de 423 MW en fin 2016[42]. Et c'est encore l'ancienneté de son registre, la *blockchain*, qui a dépassé en juillet 2016 son 420.000ème « bloc » de transactions validées, chacun lié au précédent par un chainage cryptographique : truquer une écriture demanderait de réécrire toutes les écritures jusqu'au trucage, plus de 150 millions à l'été 2016, et ceci en un temps très court tout en luttant contre 423 MW de puissance.

Au-delà de cette confiance rationnelle dans la solidité des mathématiques, il faut aussi une confiance politique dans la communauté complexe des gens qui utilisent le bitcoin, de ceux qui valident les écritures et de ceux qui spéculent sur son ascension dans le ciel des grandes devises comme instrument de transaction mais aussi comme réserve de valeur. Ce pari est-il rationnel ? Les adversaires de bitcoin aiment à brandir la courbe de son cours, beaucoup plus volatile que celle des devises classiques, même si cette volatilité, similaire à celle du cours d'une start-up, tend à s'atténuer. Les partisans répondent volontiers avec la courbe du nombre de transactions, beaucoup moins heurtée, largement insensible aux « scandales » et en progression constante selon une sage hyperbole. Car la courbe du prix s'ajuste assez bien, sur le temps long, à celle du nombre de transaction et mieux encore au carré du nombre de transactions quotidiennes, illustrant de façon assez imagée la loi de Metcalfe[43].

Fondée sur les mathématiques et sur un sentiment de puissance communautaire, la confiance dans Bitcoin est confortée par l'expérience. Nombre de détracteurs n'ont simplement pas cette expérience. On a vu des conférenciers avouer qu'ils n'avaient jamais téléchargé d'application ni ouvert de portefeuille en bitcoin. On retrouve ici cette forme de « différence communautaire » que nous avons déjà présentée.

Or chacun peut faire l'expérience entre amis, et voir ensuite les fonds passer de l'un à l'autre presqu'instantanément. Nul besoin d'avoir le même appareil en main, nul besoin d'avoir le même système d'exploitation ni la même application. « Bitcoin reconnaitra les siens » : tous les clients (tous les logiciels) sont interopérables. Puisque Bitcoin est un protocole, on ne peut construire que sur lui et uniquement de manière ouverte aux différents usages. En comparaison, les systèmes offerts par les banques, dont l'ambition est toujours d'imposer des systèmes propriétaires à des clientèles captives, apparaissent toujours restrictifs, limités, lents. Quant aux transferts internationaux, en particulier ce que l'on appelle la *remittance* des sommes envoyées par les expatriés à leurs familles, leurs coûts s'avèrent particulièrement choquant au regard des populations qui les supportent. On verra au point II, 3 le boulevard qui s'ouvre pour le bitcoin en matière de transfert d'argent des populations émigrées.

Cependant, une fois établies les raisons de faire confiance à une monnaie sans banque, il convient de comprendre les conséquences de cette absence. L'un des enjeux des entreprises de son écosystème consiste d'ailleurs à doter cette devise de services nouveaux, dont il faut inventer l'architecture radicalement différente, pour offrir à ses utilisateurs certaines fonctionnalités dont pourraient les priver l'absence de système bancaire propre et le refus du système bancaire classique d'assurer ces services pour le bitcoin. Ainsi certains travaillent sur des systèmes d'authentification des identités, de réconciliation et d'audit des écritures, d'automatisation de certains paiements (tout ce qui tourne autour des *smart contracts* ou contrats auto-exécutables).

Reste qu'une monnaie sans banque est une monnaie beaucoup plus difficile à emprunter. Il faut assumer la chose. On ne peut reprocher aux banques de créer l'argent *ex nihilo* et regretter qu'un système sans banque ne puisse connaître que du prêt sur fonds propres : celui qui prête des bitcoins (par exemple dans une opération de *crowdlending*) doit les posséder. Nos ancêtres connaissaient bien cela avec les paiements en or et les crédits que l'on se procurait non sans peine chez le notaire. Le bitcoin ne sera donc pas la monnaie du crédit immobilier ou du crédit à la consommation, si ce n'est peut-être, un jour, par l'intermédiaire de *sidechains* (évoquées au point III, 2) spécialisées sur des opérations de crédit… Si certains supporters imaginent le bitcoin comme une devise à tout faire, il est clair qu'il est une devise davantage tournée que les autres vers ce cyberespace que les banques classiques appréhendent par ailleurs bien mal.

Impossible d'aborder ici le problème de la dette autrement que par allusions… Elle apparaît naturelle aux banquiers puisque sans dette privée et publique, plus de (leur) monnaie et plus de banque commerciale. C'est par elle que les banquiers sont, comme l'écrivait Gilles Châtelet, « les Maîtres du crédit qui peuvent *se payer sur le*

futur, y imposer leurs dettes comme *moyens de règlement* et donc s'assurer la maîtrise des *horizons économiques* »[44].

La dette tourmente davantage les philosophes qui, comme Maurizio Lazzarato[45], réfléchissent sur *la fabrique de l'homme endetté*, et se demandent comment le système s'y entend à *gouverner par la dette*.

Enfin, la dette constitue aussi une source d'inquiétude fondamentale pour ceux qui s'inquiètent du devenir de la planète. La croissance est toujours présentée comme indispensable à l'emploi ; elle l'est en réalité au paiement en monnaie « gagnée » d'un prêt consenti en monnaie créée *ex nihilo*. À cet égard, la valeur en pourcentages des taux d'intérêts des crédits consentis, celle de la croissance et celle de la capacité de reconstitution des milieux naturels forment un triangle du danger. Sans doute, ceux qui s'alarment haut et fort du coût environnemental du minage (inférieur à celui des seuls distributeurs de banque, soit dit en passant…) mesurent-ils mal le lien de cause à effet entre la monnaie de la dette et la fonte des glaces.

Cette monnaie sans banque est aussi, on l'a dit, une monnaie sans État, ce qui veut dire notamment sans fisc, sans frontière, sans influence politique.

Les ministres suspectent que le bitcoin soit conçu pour échapper à l'impôt. Sur ce point, on ne leur donnera pas totalement tort malgré sa transparence. Il y a un côté « attrape-moi si tu peux » dans le bitcoin. On peut raisonnablement penser que la petite fraude passera sous le radar (quoiqu'avec de puissantes machines retraçant les transactions, ce pourrait être automatisé), que les grands fraudeurs éviteront une devise qui laisse tout de même des traces et que des règles devront être établies, applicables aux particuliers (assujettissement aux impôts sur la fortune, sur les gains en capitaux, etc.) et aux entreprises pour lesquelles l'existence de comptes en plusieurs devises est déjà une réalité bien balisée. La technologie permettra les calculs complexes (prix de revient fiscal, extériorisation des plus-values, etc.) et l'administration finira sans doute par admettre de n'intervenir que lors des passages des monnaies cryptographiques vers l'univers classiques des devises nationales, du moins dans un premier temps. On peut aussi imaginer une simplification de la « taxe Tobin » ou du prélèvement à la source par un mécanisme de *smart-contract*. Quelques affaires serviront d'exemple…

Mais on peut aussi estimer que la déconnexion du bitcoin par rapport à toute pompe fiscale est sa faiblesse : il « circule » (du latin « aller en rond ») encore insuffisamment, et autrement que le sang dans l'organisme.

Cette considération chagrine bien peu dans le milieu du bitcoin. Les libertaires proviennent de mouvements à l'origine de fortes résistances à l'idée d'impôt et sont largement imperméables à la mythologie (récente) qui en ferait un signe du pacte républicain. À l'inverse, le milieu du bitcoin adhère sans trop d'examen au récit libéral sur la monnaie, née pour servir à des échanges entre égaux sur un marché libre d'où la puissance régalienne aurait été miraculeusement absente…

Rappelons que ce qui donne sa valeur à la monnaie de l'État, c'est que l'on doit payer ses impôts avec. « Rendez à César ce qui est à César ». Toute personne qui paye des impôts peut bien accepter d'être payé avec « ça », puisque le percepteur prend « ça ». Quand on pense au poids des prélèvements obligatoires sur le PNB d'un pays, oublier ce détail est une folie. Elle semble cependant étrangement fréquente.

Dire du bitcoin qu'il est une monnaie sans frontière peut laisser indifférent dans la mesure où les archéologues attestent que les monnaies ont toujours franchi de longues distances[46]. Mais justement, les monnaies d'or et les valises de billets franchissent les frontières, et les devises scripturales électroniques restent inscrites dans des livres bancaires situés dans la juridiction d'un État territorial, de sorte qu'en basculant d'un livre de banque français à un livre de banque suisse, elles passent en quelque sorte la frontière.

Le bitcoin ne passe pas les frontières, il les ignore. Il faut ici réfléchir sur l'espace dans lequel il se meut, distinct du plancher des vaches. Le mot latin *limes* qui signifiait la frontière, a donné l'adjectif « limité ». Or notre droit civil et notre fiscalité restent marqués par les savoir-faire du géomètre et du conservateur des hypothèques, dans un espace borné et « limité ».

La douane qui détaille ce qui doit être déclaré reste muette sur le bitcoin. Le voyageur détenteur de bitcoin ne porte jamais sur lui davantage de valeurs que celui qui transporte sa carte de paiement : une adresse et un code pour y accéder. Il ne porte sur lui que des chiffres et des lettres. Mais cette adresse n'est pas unique et localisable. Qu'on l'encaisse ou qu'on le décaisse, le bitcoin demeure dans son registre doté d'ubiquité. Sa vitesse de transfert ne provient d'ailleurs que de ce qu'en fait il ne voyage pas, du moins pas avec nous ou dans le même espace que

nous. Cette réflexion, qui pourrait être approfondie philosophiquement, doit être rétorquée à tous les discours visant à établir une souveraineté nationale sur le bitcoin, comme en général sur le cyberespace.

Inversement, cette monnaie sans État n'est pas faite pour eux. Le bitcoin pourrait certes servir de monnaie complémentaire locale en cas de crise, voire sur de petites îles (Aurigny ou Man en caressent peut-être l'idée), mais il souffre aux yeux des politiques d'un défaut majeur : on ne peut l'emprunter et vivre à découvert avec lui !

Bitcoin n'est pas fait pour un territoire donné ou circonscrit mais pour un Internet global et sans frontière. Il est normalisé et interopérable dans sa conception protocolaire. Sa gestion est décentralisée et apatride.

L'institution monétaire se prévaut généralement de ce que, opérant à la jonction des dettes privées et des dettes sociales, elle assure la cohérence et l'unité sur un territoire donné, national. Mais n'oublions pas qu'une partie de la valeur produite par la société est occultée. Comme le rappelle Bernard Friot, le travail domestique est un vrai travail et produit de la valeur, mais il est oublié. Face à de telle difficultés à déterminer la valeur produite par un ensemble monétaire, y a-t-il une véritable science possible de l'émission monétaire ?

Bitcoin s'inscrit comme une monnaie économique, impartiale, purement instrumentale, face aux monnaies centrales étatiques visant à la représentation de la société comme totalité. Monnaie sans dette, Bitcoin exprime le pouvoir d'achat là où la monnaie-dette des États exprime aussi le pouvoir sur la société. Le bitcoin, monnaie finie s'il en est, s'oppose à la monnaie de crédit qui incarne la logique de la production pour la production, c'est-à-dire l'introduction de l'infini dans l'univers capitaliste.

Tant décrié comme un simple instrument de spéculation, le bitcoin est tout autrement une monnaie de la finitude, dont on découvre peu à peu qu'elle est notre horizon écologique. Ainsi faut-il concevoir une économie axée sur la division du fini (souvenons-nous que Bitcoin pourrait être pratiquement divisible à l'infini) au contraire de l'expansion infinie qu'on justifie par l'idée de conquête spatiale. Nous touchons là aux *limites de la Croissance* si bien décrites et pressenties par le Club de Rome[47].

II

Le bitcoin, sans mystère ni fantasme

1- Esquisse de son ingénieux assemblage

Un protocole au fondement de son aspect monétaire

Le lecteur qui tourne les pages de ce livre dans l'ordre et aura apprécié notre présentation de Bitcoin contournant, tant bien que mal, ses aspects techniques devra, dans cette seconde partie, y faire face dans une mesure raisonnable pour comprendre en profondeur Bitcoin.

Ceux qui auraient choisi de commencer par ici ne devront donc pas se décourager devant l'aspect, peut-être rugueux par moments, des lignes qui vont suivre : elles ne sont pas représentatives de l'intégralité du livre !

Commençons par expliquer ce qu'est un protocole. Il est toujours utile de regarder vers nos amis les Grecs lorsque l'on cherche à comprendre un mot. « Protocole » vient du grec πρωτόκολλον (« protókollon », où « proto » signifie « avant, premier » et « kolla », « gomme, colle ») qui fait référence à la première page d'un rouleau de papyrus. C'est là qu'étaient inscrits le nom de l'auteur, la date et le lieu de manufacture dudit papyrus, ce qui est amusant à mettre en regard des fonctions de signature et d'horodatage de Bitcoin. Les Grecs, les Romains et les Byzantins avaient pour habitude de couper ce protocole avant la lecture. Mais pour certains documents officiels il était interdit de le faire. Ce qui prouve que l'importance de la date, du lieu et de l'auteur ne date pas d'hier. On voit ici une fonction encadrante qui a évolué sémantiquement au fil des âges.

En français, si l'on se réfère au mot orthographié à l'époque « protocolle » dans le délicieux dictionnaire de 1690 d'Antoine Furetière[48], on trouve une fois encore des données fort intéressantes. Voici en effet les différentes définitions qu'on y lit dans une langue modernisée par nos soins :

> Formulaire de plusieurs actes de justice pour instruire les novices en la pratique. Il y a des livres imprimés, des protocoles de notaires, des protocoles des Sergents, où sont les formulaires des actes qui se font en ces professions. [1] Protocole est aussi un registre des notaires où ils doivent écrire toutes les minutes de leurs actes les unes à la suite des autres, afin qu'elles ne soient point perdues, changées ni altérées. Cet usage serait avantageux au public, mais il ne s'observe qu'en quelques lieux de la Province, nonobstant la disposition expresse de l'Ordonnance d'Orléans, Art. 83. [2] Protocole s'est dit autrefois de celui qu'on appelle maintenant Souffleur, qui est derrière celui qui parle en public, pour lui suggérer ce qu'il doit dire, au cas où la mémoire lui manque. Cela vient de ce qu'on appelait aussi Protocoles chez les Romains, certains Nomenclateurs qui savaient tous les noms des citoyens, et qui les suggéraient à leurs Maîtres, afin qu'ils puissent saluer chacun par son nom en l'abordant. [3] Protocole, originairement était la première feuille d'un livre, où était la marque du papier ; et même il signifiait quelquefois cette marque, qui était tantôt à coté, tantôt au haut de la page. La Nouvelle XLIV de Justinien défend d'ôter et de couper les protocoles des chartes, qui faisait connaître l'année où le papier ou le parchemin avaient été faits, et l'Officier qui les avait délivrés à ce commis : ce qui servait à découvrir plusieurs faussetés. On a suppléé à cette formalité par le paraphe des Juges, qu'on a fait apposer à tous les feuillets des registres de certains Officiers publics, comme

> Banquiers, Geôliers, etc. D'autres disent que protocole est une première minute ou brouillon et sommaire d'un acte qu'on doit passer, que les Notaires mettaient en abrégé dans de petits livrets, et qu'ils étendaient après à loisir : ce qui a le plus d'apparence.

Ces définitions sont absolument époustouflantes en regard de ce qu'est Bitcoin. On y trouve presque tout : l'aspect normatif du protocole, son aspect de registre atemporel, inaliénable, inaltérable, tout y est. On a là presque une définition de Bitcoin et il est fabuleux de trouver cela dans un dictionnaire de 1690.

Mais le sens du mot va changer au fil du temps pour aboutir à cette première définition générale dans le Larousse: « Ensemble de règles établies en matière d'étiquette, d'honneurs, de préséances dans les cérémonies officielles ; services chargés de les appliquer. » On a là encore des données intéressantes, en ce sens que même si l'on est dans le sens commun du mot on retrouve « l'ensemble de règles » et surtout l'idée que le protocole est la règle et en même temps ce qui fait appliquer la règle. Et dans Bitcoin cela fonctionne remarquablement bien dans la mesure où *code is law,* maxime que l'on devrait étendre de la sorte : *code is law and police*, même si cela sonne moins bien. En effet, dans Bitcoin la norme est autonome, le protocole se suffit à lui-même et à ses utilisateurs pour conserver son intégrité. On se rapproche dès lors du sous-titre de notre livre : Bitcoin est bien une *monnaie acéphale*, du fait qu'il n'admet pas de police, ses principes intrinsèques étant censés empêcher toute malversation (par rapport à ses règles) dans ses fondements-mêmes.

Enfin, regardons la définition particulière de l'informatique que donne le Larousse : « Ensemble de règles définissant le mode de communication entre deux ordinateurs. » Nous arrivons ici au dernier point important de l'aspect protocolaire de Bitcoin. Il est le liant entre différents interlocuteurs, en l'occurrence des machines derrières lesquelles se cachent des êtres humains ou non. Et dans Bitcoin la communication est extrêmement importante : son usage est pensé avant tout pour des actions transactionnelles, c'est-à-dire des actions de communication, car, du point de vue d'un ordinateur, tout n'est que langage.

Et justement c'est une des forces de Bitcoin que d'être un protocole. Il diffère du langage informatique qui vise à programmer ou structurer des données informatiques. Son rôle est vraiment centré sur la définition de la manière dont les données seront échangées. En revanche, comme le langage, c'est plus ou moins une norme. Le protocole va permettre à un ensemble de machines suivant la même norme pour communiquer de se connecter et d'interagir entre elles.

Le lecteur aura forcément entendu parler des protocoles TCP (Transmission Control Protocol) et IP (Internet Protocol), à l'origine de la suite Internet TCP/IP, soit l'organisation des couches de protocoles permettant de faire fonctionner Internet. Le lecteur aura croisé ces termes pendant ses cours de technologie au collège ou bien dans les médias quand Internet est arrivé. Bien qu'ils soient loin d'être les seuls impliqués, ils en sont plus ou moins le cœur du réseau mondial d'Internet. Comme Bitcoin est avant tout un réseau, il est donc naturel qu'il soit également un protocole.

Comme n'importe quel protocole, il permet d'établir un réseau et une communication entre des machines. Ce point est capital : le fait que Bitcoin soit un protocole permet son interopérabilité. Les logiciels qui utiliseront le protocole Bitcoin n'auront ainsi pas de problème de compatibilité entre eux. Nous verrons ce point quand nous parlerons des *wallets* dans quelques paragraphes. Une analogie simple en aide la compréhension. Lorsque que l'on tape une adresse web, elle est toujours précédée de « http » (HyperText Transfer Protocol) : c'est le protocole qui permet d'effectuer les requêtes pour obtenir des pages web. Les protocoles ont ce qu'on appelle des *clients*, des logiciels qui vont appeler d'autres logiciels serveurs où sont situées les données. On appelle cela l'architecture *client/serveur*. Les logiciels clients HTTP les plus répandus sont les navigateurs web. Et comme le lecteur surfeur l'aura remarqué, qu'importe le navigateur, il accède toujours au web. C'est justement grâce à ce protocole standardisé, que tous les navigateurs adoptent au sein de leur code, que les machines peuvent communiquer entre elles et ainsi envoyer des requêtes à des serveurs.

Pour Bitcoin, c'est un peu différent en raison de sa nature pair-à-pair (P2P). En effet, l'architecture des protocoles pair-à-pair se distingue de celle client/serveur, en ce sens qu'il n'y a pas de séparation entre les logiciels clients et les logiciels serveurs, même si certains logiciels sont amputés de leur aspect serveur et nous verrons très vite pourquoi. Ce qu'il faut retenir, c'est que, pour son bon fonctionnement, Bitcoin nécessite cette architecture pair-à-pair qui fait que son logiciel est hybride.

La nature pair-à-pair de Bitcoin est une des notions clefs : c'est ce qui lui donne son architecture distribuée. On parle d'architecture distribuée quand tous les nœuds (logiciels clients/serveurs en marche) sont interconnectés et qu'il n'y a pas d'autorité centrale. Nous retrouvons là, de nouveau, le sous-titre de notre livre. Le Bitcoin est acéphale, c'est-à-dire sans aucune tête, en ce sens qu'il n'est sous la domination d'aucune autorité. Le réseau est uniquement constitué de pairs. C'est ce qui fait de Bitcoin un réseau horizontal tranchant nettement avec tous les systèmes monétaires existants qui, eux, sont verticaux.

L'horizontalité est aussi un gage d'une liberté que nul ne pourra contredire, celle défendue par les crypto-anarchistes créateurs et promoteurs de Bitcoin. Nous rappelons ici que l'anarchie n'est pas ce que l'on entend dans le sens courant et péjoratif, une absence d'organisation et de règles. L'anarchie est une organisation horizontale ou tendant vers l'horizontalité, mais avec des règles. Ces règles, dans le cadre de Bitcoin, consistent en son protocole complètement transparent et donc lisible par tous, libre et donc modifiable par tous. Cependant, le réseau devant trouver un consensus décentralisé, une seule version de Bitcoin pourra fonctionner à la fois (deux dans des cas spécifiques très rares) ; mais l'information importante, c'est que cette version pourra être mise à jour, tout comme n'importe quel protocole. Ceci dit, il faudra tenir compte du fait qu'un protocole est bien plus difficile à modifier dès lors qu'il est lourdement implanté. Nous verrons ces problématiques liées à Bitcoin dans le point III, 2. Pour l'exemple, peu l'auront remarqué, mais le protocole HTTP, qui était en version 1.1, a été mis à jour en HTTP 2.0 en mai 2015 : il a fallu près de 10 ans pour publier une mise à jour du protocole. La majorité des sites n'a pas encore été mise à jour pour utiliser HTTP 2.0 et beaucoup ne feront jamais cette mise à jour. On comprend que les mises à jour de protocoles ne sont pas une mince affaire dès lors que ceux-ci sont répandus.

Nous avons vu que le protocole Bitcoin était un protocole pair-à-pair. Il est également un ingénieux assemblage d'autres technologies. Il importe de souligner que Bitcoin n'est pas une technologie, mais bien un protocole qui utilise différentes technologies. Parmi celles-ci se trouve tout d'abord la fonction de hashage, que l'on peut désormais présenter par son nom, SHA-256, créée par la NSA et publiée en 2001[49]. Les fonctions de hashage sont souvent présentées comme le « couteau suisse » de la cryptographie. L'algorithme SHA-256 peut être résumé ainsi : il va prendre une portion de fichier (par exemple un message), faire en sorte qu'elle puisse être subdivisée en bloc de 512 bits (unité binaire informatique), pour ensuite découper le message en suivant certaines itérations, d'où ce qu'on appelle le hashage (de l'anglais *hash* : pagaille, désordre), et enfin renvoyer une empreinte unique du message d'origine. Par exemple, si l'on prend notre titre *Bitcoin, la monnaie acéphale* cela donnera, après un moulinage en SHA-256, la suite :

623cd261b06460c9d000d6486af866857494b9848dcb9a66dd354c3f8de8b411



Apprenez à hasher ! (expérience)

Cette empreinte « unique » (ce hash) du message est le résultat du traitement du texte cité par la fonction SHA-256. Cette fonction est à sens unique et il sera impossible de retrouver le message original à partir de l'empreinte. En revanche, il sera toujours très facile de vérifier que notre message initial est bien le bon car la fonction SHA-256 est déterministe et son résultat sur un message donné sera toujours le même. La fonction est chaotique : le résultat d'un texte à peine modifié (*Bitcoin: la monnaie acéphale*, deux points au lieu de la virgule) sera entièrement différent :

cceb8c70cc27fba54f2cf3f3f8d3704c21d94bac0d147190f466995b0428e1f0

Deux textes peuvent-ils avoir la même empreinte ? Ce risque (appelé risque de collision) est théoriquement possible mais sa probabilité est de l'ordre de l'inimaginable, comme celle de puiser une molécule d'eau précise dans l'océan. On considère donc (même si c'est mathématiquement faux en toute rigueur) qu'un hash est unique.

Bitcoin utilise le fonctionnement SHA-256 pour générer des arbres de Merkle, comme ce sera expliqué plus loin, mais il utilise aussi les courbes dites elliptiques (des courbes de type $y^2 = x^3 + ax + b$), dans les détails[50] desquels nous n'entrerons évidemment pas ici, afin de générer les paires de clefs des utilisateurs, pour la signature des transactions. C'est donc l'une des clefs de voûte du fonctionnement de Bitcoin.

Dans cet ingénieux assemblage, nous trouvons aussi la cryptographie asymétrique. Il s'agit du système qui permet d'envoyer un message secret à quelqu'un tout en faisant en sorte qu'il puisse nous livrer publiquement une clef (dite « publique ») pour le chiffrement du message que lui seul ensuite (avec sa clef dite « privée ») pourra déchiffrer. De cette manière, on peut communiquer à distance de manière chiffrée. En effet, pendant très longtemps, le problème du chiffrement avait été la transmission de la clef unique, qui était capitale mais qui pouvait être interceptée. Cette contrainte n'existe plus dans le cadre de la cryptographie asymétrique. C'est une technologie bien plus ancienne que Bitcoin, datant de 1978 avec le chiffrement RSA. Notons que c'est ce chiffrement qui a notamment permis l'invention de la carte de paiement. C'est aussi l'un des piliers du fonctionnement de Bitcoin. Tous les utilisateurs de Bitcoin sont dotés d'un compte avec une clef privée et une clef publique, ainsi qu'une adresse. Ce sont ces trois éléments qui leur permettent de faire et de signer des transactions. Il faut toujours garder en tête que Bitcoin a été intégralement pensé comme un système de transfert de propriété (dé)matérialisée sous forme de jetons numériques.

Enfin, le dernier élément de ce protocole est le registre distribué qu'est la *blockchain*. C'est elle qui structure les données de Bitcoin. En gardant la trace de toutes les actions effectuées sur le réseau, la *blockchain* assure la cohérence du système dans le temps. Elle est fiable et infalsifiable grâce aux autres mécanismes de Bitcoin que l'on vient d'évoquer. Le protocole contient aussi de nombreuses autres fonctions que nous détaillerons quand nous parlerons des contrats auto-exécutables.

L'inventeur anonyme du Bitcoin, Satoshi Nakamoto, a ainsi eu recours à toutes ces différentes technologies. Cela ne doit jamais être omis, Bitcoin est un assemblage technique et non une technologie. Il est absurde de parler de « technologie *blockchain* », qui n'est qu'une pierre de l'édifice Bitcoin et de tous les autres protocoles d'échanges décentralisés créés à partir de Bitcoin. Cet abus de langage était excusable durant les années passées ; persister à le faire en 2017 témoignerait d'un retard regrettable dans la compréhension de la chose.

Le bitcoin est également une unité de compte. On notera l'utilisation d'un b minuscule pour cette dénomination, à la différence du B majuscule du protocole. C'est une distinction importante à faire, qui permet de bien savoir de quoi on parle. Il est aussi d'usage de ne pas mettre d'article devant Bitcoin pour l'identifier à l'oral. Toutes ces normes se sont établies assez naturellement dès les premiers échanges sur celui-ci en 2008 et ont perduré pour finalement trouver leur place dans l'Oxford Online Dictionnary en 2013, tout du moins pour la forme avec le b minuscule.

Le mot bitcoin est cependant équivoque car, avec ce b minuscule, il ne désigne pas seulement l'unité de compte mais aussi la monnaie au sens de devise. Or il serait possible d'avoir une devise et des unités de comptes dotées de noms différents. Il faudra donc faire attention à ce dont on parle lorsque l'on lit bitcoin avec un b minuscule. Mais de manière générale cela ne crée pas vraiment d'ambiguïté, y étant nous-mêmes habitués avec nos monnaies classiques qui ont ce même « problème ».

L'unité de compte qu'est bitcoin est aussi définie au sein même du protocole Bitcoin de manière extrêmement précise. On détaillera dans le prochain chapitre son fonctionnement plus en profondeur, mais on peut déjà noter que la quantité de bitcoins est limitée à 21 millions d'unités subdivisibles au cent-millionième. Ce qui fait qu'un bitcoin peut s'écrire sous cette forme un peu absurde 1,00000000 BTC. La plus petite unité est communément nommée le Satoshi en hommage à son créateur et elle est égale à 0,00000001 BTC. Un milliBitcoin vaut 0,001 BTC et un bit vaut 0,00000100 BTC. Certains parlent en multiples du Satoshi, ainsi un kiloSatoshi vaudra-t-il 0,00001000 BTC. Il faut savoir que la divisibilité est aussi régie par le protocole qui sera donc potentiellement mis à jour s'il advient que la valeur du bitcoin soit trop élevée et nécessite une plus grande division. Il sera toujours possible de diviser davantage le bitcoin sans pour autant avoir à modifier sa rareté et le rythme de sa création monétaire.

Nous avons vu dans ce chapitre la subtilité du mélange qu'est le protocole Bitcoin et comment les racines des mots peuvent être d'un grand secours, d'une pertinence parfois étonnante pour plonger dans des concepts nouveaux. En partant du mot protocole, nous avions presque déjà la définition du protocole Bitcoin et de ses particularités. Nous allons maintenant faire un zoom sur le fonctionnement des données dans Bitcoin, en regardant la *blockchain* et les mécanismes qui l'entourent. Nous espérons que le lecteur aura surmonté les difficultés potentielles de ce sous-chapitre et sera encore d'attaque pour continuer son périple dans les sous-chapitres suivants.

La blockchain, un livre de compte avant tout

Le mot *blockchain* est devenu le roi de tous les mots-fantasmes. Il fut le *buzzword* de 2016 dans la « tech » et la finance. Qu'en est-il vraiment ?

Tout d'abord il faut préciser qu'on ne peut parler de *blockchain* avec un article défini singulier type « la » sans spécifier le protocole auquel elle est associée. Lorsque l'on voudra, dès lors, parler du concept, il faudra parler des blockchains au pluriel et prendre en compte que cela sera toujours légèrement imprécis en raison des différences pouvant exister entre celles-ci suivant le protocole utilisé et l'amplitude de son utilisation. Dans notre cas nous allons bien sûr parler de la *blockchain* de Bitcoin, même si toutes les blockchains ont des structures plus ou moins similaires.

Nous l'avons vu, la blockchain sert à structurer les données de Bitcoin ; elle permet donc la mise par écrit de toutes les opérations effectuées sur le réseau Bitcoin. Une de ses particularités est d'être linéaire et unidirectionnelle dans le temps, car il ne peut y avoir qu'une accumulation de blocs et non une soustraction. Par analogie mathématique on peut dire que la Blockchain est une suite arithmétique $s = 0 + n.r$ très simple de raison $+1$. Ainsi elle s'étend à l'infini en rajoutant des blocs un à un, à un intervalle à peu près régulier.

Cet intervalle est d'environ dix minutes, cela a déjà été mentionné sans plus de détails sur ce qu'il faut entendre par « environ ». L'intervalle ne suit pas ce que les mathématiciens appellent une loi *normale* mais une loi *exponentielle*, comme celle qui régit les passages du bus. C'est une loi qui modélise la durée de vie d'un phénomène sans mémoire, sans vieillissement et sans usure, pour lequel le fait qu'il ait déjà duré un certain temps jusqu'au temps t ne change rien à son espérance de durée à partir du temps t. Ce n'est pas un point de détail : le fait que SHA-256 soit une bonne fonction de hashage, sans défaut, entraine le fait que le temps de hashage soit exponentiel. Une notion que l'on retrouvera lorsque l'on examinera les chances d'un attaquant.

Le maintien de cet intervalle est rendu possible automatiquement par le calcul de la difficulté du réseau établi tous les 2 016 blocs[51], soit à peu près toutes les deux semaines. On introduit là un nouveau concept : la difficulté. Il s'agit de la difficulté du problème que doivent résoudre les mineurs pour avoir le droit d'écrire dans la blockchain. Comme le problème auquel ils sont confrontés est probabiliste, il est possible de régler sa difficulté en fonction de l'équipement dont sont dotés les mineurs, en l'occurrence de leur puissance de calcul, déduite à partir de leur temps de résolution.

Ainsi, bien qu'avec le temps et les avancées techniques, mais aussi avec l'intérêt financier du minage, la puissance de calcul des mineurs ait augmenté de façon spectaculaire, le problème prend toujours à peu près dix minutes pour être résolu. L'ajustement de la difficulté est effectué grâce à l'allongement ou au raccourcissement du nombre de zéro qu'il faut produire au début de l'empreinte cryptographique du bloc grâce à l'adjonction dans les données dudit bloc d'une série de signes supplémentaires, le « nonce ». Ainsi plus le nombre de zéro est conséquent, plus il sera difficile de produire une telle empreinte. On nomme le nombre qui va déterminer le nombre de cette suite de 0 la « *target* » ou difficulté. Il est inclus dans l'en-tête des blocs.

La lourde tâche qui consiste à valider les blocs Bitcoin est confiée aux mineurs. Ceux-ci vont effectuer l'écriture de données dans la blockchain. Ce sont donc eux les écrivains façonniers de la blockchain. On les appelle mineurs car l'étape de validation est récompensée par une nombre fixe de bitcoins versés au mineur ayant résolu le problème cryptographique, le hash. C'est donc uniquement l'aspect monétaire qui est désigné par cette appellation. On voit ici encore une fois dans la sémantique, l'omniprésence de l'idée monétaire de Bitcoin. L'analogie choisie par l'ensemble des utilisateurs est purement monétaire, même si elle permet également d'identifier le travail effectué par le mineur. Mais on pourrait donner d'autres sobriquets aux mineurs, qui sont aussi les surveillants, les validateurs du réseau et les écrivains de la blockchain.

Ce sont eux qui font que l'on appelle les monnaies comme Bitcoin des monnaies *décentralisées* et non des monnaies *distribuées*. La décentralisation sur le réseau opère au niveau des mineurs, car tout le monde ne mine pas sur le réseau. On peut très bien utiliser Bitcoin sans pour autant miner. Le fait que seuls quelques pairs participent à cette opération en a fait un processus de consensus seulement décentralisé et non réellement distribué. Ce résultat inévitable d'une « course aux armements » entre mineurs a cependant permis que le réseau Bitcoin puisse fonctionner correctement, bien qu'il y ait perdu un peu d'horizontalité par rapport à la vision d'origine.

Comme nous l'avons vu auparavant, le réseau nécessite un consensus décentralisé pour que tout le monde puisse statuer sur une version de la blockchain. Ceci implique qu'un pair ait le droit de valider un bloc parce qu'il a prouvé qu'il a fourni un travail au sein du réseau. La concurrence entre les mineurs permet, elle, de faire en sorte que les mineurs ne soient pas tous les mêmes et qu'ils combattent en accroissant leur puissance de calcul pour augmenter la sécurité du réseau. Cette preuve de travail est le seul moyen de limiter la tricherie dans le réseau, bien que d'autres algorithmes visant ce but aient fait leur apparition avec d'autres cryptomonnaies dont nous parlerons plus en détails dans le point III, 2. S'il était possible que le consensus permettant de valider la blockchain soit distribué, comme le stockage de la blockchain elle-même, il y aurait de grande chance pour que Bitcoin ait déjà implanté cette solution. Certains chercheurs soutiennent qu'il n'existe pas d'autre moyen de neutraliser la fameuse « attaque de Sybil » que la coûteuse « preuve de travail »[52]. D'autres, comme Silvio Micali, soutiennent le contraire.



Les mineurs égoïstes (article de Pierre Noizat)

Mais contentons-nous ici de comprendre que c'est le seul aspect du réseau qui est décentralisé et donc un peu moins horizontal que le reste. La blockchain, quant à elle, est bel est bien distribuée dans son stockage et dans son usage, car elle est répliquée sur tous les ordinateurs du réseau et tout le monde peut hypothétiquement écrire dedans dans le respect de ses règles. Intéressons-nous désormais à sa structure de données.

La blockchain est constituée d'un ensemble de blocs. Ces blocs sont constitués de deux parties : l'en-tête et le contenu ou le corps. L'en-tête est constitué précisément d'un ensemble de données.

Tout d'abord[53] viennent les données techniques, composées d'un identifiant dit « magique »[54], de la version du protocole utilisé et de la taille du bloc ; ces données sont importantes parce qu'elles déterminent la version du protocole et donc ses particularités. C'est en changeant la version du logiciel utilisé qu'on pourra mettre en œuvre de nouvelles fonctionnalités incluses dans une mise à jour du protocole.

Vient ensuite l'empreinte unique de l'en-tête du précédent bloc, sans son identifiant magique et sa taille. Cette partie de l'en-tête est absolument cruciale pour le fonctionnement de la blockchain, et donc de Bitcoin : c'est grâce à elle qu'on dit que les blocs sont chaînés. De ce fait, on ne pourra pas modifier un bloc de la blockchain sans modifier tous les blocs précédents. Autant dire qu'il est illusoire d'imaginer une telle prouesse en 10 minutes, puisque quelqu'un devrait arriver à battre la puissance de calcul de plus de la moitié des mineurs, lui compris. La liaison indestructible de la blockchain permet d'avoir des comptes absolument fiables, sachant qu'il est possible de remonter jusqu'à l'origine de toute transaction. Pour rendre la chose plus poétique, la blockchain est le fil d'Ariane de Bitcoin, fil unique grâce auquel on peut retrouver le chemin emprunté par le réseau depuis sa genèse.

L'en-tête est également composé d'une racine de Merkle. C'est une empreinte un peu spécifique qui est le condensé de toutes les transactions effectuées dans le bloc. Le nom de racine n'est pas anodin car la racine est le résultat d'une suite de hashage en arbre. Pour faire une analogie, c'est l'arbre généalogique des empreintes des transactions du bloc que l'on marie arbitrairement pour réussir à obtenir un empreinte fille « unique » (ou racine). Ce procédé peut sembler trivial au premier abord mais il est capital et déjà présent dans le papier original de Satoshi Nakamoto. Il permet au protocole d'avoir des logiciels semblables à des logiciels uniquement clients qui sont donc plus légers et plus simples à utiliser car ils n'ont pas à télécharger l'intégralité de la blockchain. Une prouesse de taille dont nous reparlerons dans le prochain sous-chapitre.

Après la racine de Merkle, le bloc comporte aussi un horodatage. C'est un atout immense du Bitcoin que de réussir à effectuer un horodatage cohérent sur le réseau. Nous verrons toutes les possibilités que cela offre au fur et à mesure de l'ouvrage. Bitcoin doit s'appuyer sur ce mécanisme pour conserver la cohérence unidirectionnelle de sa blockchain. C'est aussi l'horodatage qui permet de recalculer la difficulté. En effet, le réseau ne voit pas la puissance de calcul totale du réseau mais s'ajuste par rapport au temps de résolution des 2016 blocs précédents.

On a déjà noté que cet horodatage, temps propre de la blockchain, est aussi le premier « temps universel », la première chronologie intrinsèque sur Internet.

Puis est inscrit le niveau de difficulté, celui qui permettra au mineur d'optimiser sa résolution du problème. La difficulté est modifiée tous les 2016 blocs comme il a été dit plus haut.

Enfin vient le fameux « nonce » dont nous avons parlé auparavant. C'est là que le mineur teste des valeurs aléatoires et dépose sa solution. Si elle est bonne, le hash sera adéquat et correspondra à l'empreinte de l'en-tête voulu.

Il convient de rajouter que ce « nonce » ne suffit généralement pas à trouver un hash correspondant à la difficulté voulue. De ce fait, d'autres facteurs d'ajustement existent comme le *timestamp* ou l'ordre des transactions. Mais au cas où ces facteurs ne conviennent toujours pas, il existe aussi un « extranonce » contenu dans la transaction de génération des nouveaux bitcoins (*coinbase*) [55].

Nous voilà au bout de l'en-tête d'un bloc. Le lecteur constatera que c'est un véritable condensé de mécaniques et de technologies toutes plus ingénieuses les unes que les autres. Encore une fois, tout n'est qu'assemblage.

Entre l'en-tête et le bloc se trouve le nombre de transactions incluses dans le bloc selon le choix du mineur et la taille du bloc. En effet le mineur fait deux opérations avant de valider des transactions. Il va d'abord vérifier qu'aucune transaction n'enfreint les règles du protocole, comme une tentative de dépenser plus que les bitcoins réellement enregistrés à l'adresse de l'émetteur, ou bien de dépenser les bitcoins d'une autre adresse. Puis il va sélectionner parmi les transactions valides celles qu'il va accepter et inscrire dans son bloc suivant leur taille et les frais payés corrélés à cette taille. Car les mineurs ont le choix de refuser des transactions. Au début, les transactions bitcoins étaient intégralement gratuites mais, des personnes mal intentionnées tentaient de bombarder le réseau pour le saturer puisque que cela ne leur coutait absolument rien. Est advenu un deuxième problème : la somme étant toujours trop faible, des individus étaient prêts à payer pour tout de même saturer le réseau. Ainsi la taille des blocs a été limitée à 1 million d'octets, ce dont nous reparlerons plus tard. Mais retenons qu'il y aura un jour sur bitcoin un marché des frais de transaction très développé, ce qui ne veut pas forcément dire qu'elles seront très chères. On distingue encore une fois l'aspect monétaire de la Blockchain, qui obéit à des règles de frais de transaction inclus dans le protocole Bitcoin. Encore une preuve que Bitcoin a été pensé en vue d'une propriété monétaire numérique et non comme un simple échange de jetons sans valeur.

Arrive ensuite le corps ou le contenu du bloc. C'est ici que sont inscrites toutes les transactions. La blockchain est avant tout un registre de comptes destiné à l'échange de valeur. La première transaction inscrite est celle nommée *coinbase*. C'est la transaction initiale du bloc, composée des bitcoins récompenses, résultat de la création monétaire et des bitcoins correspondant aux frais de transaction. Ce sont là les seules transactions sans entrée ni adresse correspondant à l'expéditeur, puisque c'est le réseau même qui créé ces bitcoins. De ce fait, l'espace de l'entrée (*input*) peut être occupé par ce qui a été décrit plus haut comme un « extranonce ».

Procédons désormais à un gros plan sur ce qu'est une transaction classique de la même manière que nous l'avons fait pour l'en-tête du bloc. De quoi se compose une transaction, cette « fonction communicante » de la monnaie ? Eh bien tout d'abord d'un en-tête avec des données techniques tout comme on l'a vu à l'échelle supérieure avec le bloc. Dans ces données techniques, on retrouve encore des mécanismes essentiels à Bitcoin. Il y a bien sûr le numéro de version du protocole pour s'assurer que la transaction est bien compatible avec l'ensemble de règles définies dans l'en-tête du bloc. Il y a encore une fois une donnée temporelle, elles sont chères à Bitcoin. Mais cette fois-ci ce n'est pas vraiment un horodatage mais plutôt un « blocodatage ». On spécifie alors que la transaction ne pourra être délivrée qu'après un certain nombre de blocs passés, équivalent théoriquement à 10 minutes. Ce qui permet ce paramètre s'appelle nLocktime.

Puis, dans ces données techniques, il est indiqué combien d'entrées et combien de sorties la transaction possède. On ne peut trouver une meilleure preuve pour montrer la nature d'unité monétaire de Bitcoin. La blockchain ressemble à un livre de comptes à doubles entrées. La particularité de Bitcoin est que, lorsque l'on envoie une transaction, en réalité on regroupe un certain nombre de sommes que l'on a reçues auparavant, de sorte à avoir assez de bitcoins pour envoyer la somme donnée. C'est de cela que nous parlons lorsque nous avançons qu'il est possible de garder la trace de chaque bitcoin depuis son origine. En effet, les opérations sur le réseau ne cessent de créer des paquets de bitcoins, qui sont gardés comme tels lors des transactions ou ré-agencés. Une transaction Bitcoin aura généralement deux sorties, à moins que l'utilisateur ne dépense l'intégralité de la

somme de son portefeuille d'un coup. Sinon l'utilisateur se rendra en quelque sorte la monnaie à lui-même. Par exemple, s'il possède un lot de 25 bitcoins et qu'il veut en dépenser 12, il enverra un paquet de 12 bitcoins au vendeur et un paquet de 13 à lui-même. Ces paquets sont les sorties de notre transaction, qui seront deux futures entrées quand les bitcoins reçus seront dépensés. On appelle ces entrées de bitcoins non dépensés par une adresse UTXO (Unspend Transaction Output). Ainsi, une somme de bitcoins sur une adresse correspond à la somme de ses UTXO.

Ces entrées sont précisément constituées d'éléments techniques comme la longueur du script, son numéro de séquence, le hash de la précédente transaction, qui permet de lier les transactions entre elles un peu comme les blocs le sont entre eux, et enfin les données du script. Le script classique dans Bitcoin est celui qui permet de dépenser ses bitcoins. On signe avec la clef privée le droit de possession sur les bitcoins appartenant à une adresse publique correspondante. Il faut retenir ici que Bitcoin permet des actions monétaires avec ces scripts. C'est ce que l'on peut nommer des contrats intelligents ou auto-exécutants, mais nous verrons cela plus en détail plus loin. L'essentiel est de garder en mémoire que les scripts sont des actions transactionnelles et que même la plus simple d'entre elles en est une.

Les sorties se composent pratiquement des mêmes éléments. Elles possèdent une donnée technique indiquant la longueur du script, combien de bitcoins sont envoyés et l'adresse du destinataire. Nul besoin de souligner pourquoi ceci est primordial, puisque ce sont des mécanismes basiques d'interactions transactionnelles.

Il peut paraître abrupt de montrer les entrailles de la blockchain Bitcoin de la sorte. Toutefois, il nous semble capital que le lecteur puisse comprendre les mécanismes de base qui assurent le bon fonctionnement de ce bijou d'harmonie. Car nous l'avons vu de nouveau, Bitcoin est avant tout un assemblage et une imbrication d'un grand nombre de mécanismes. Sans oublier le but premier de toute cette fabrication, créer un protocole qui serait à la fois une monnaie, une unité de compte et un instrument de paiement.



Regardez vivre la Blockchain ! (expérience)

Il en va de même pour la blockchain, conçue pour être un livre de transactions à double entrée, car sa mécanique transactionnelle est pensée comme telle. Mais elle est aussi un inventaire infalsifiable en raison de la puissance de calcul requise pour participer au réseau en tant que mineur et de la rude concurrence qui règne au sein de ce groupe. Véritable livre-horloge d'Internet, elle garantit une certaine fiabilité dans le calcul du temps. Les mécanismes du code sont en effet pensés de sorte à ce qu'il ne puisse y avoir de tricheries au sein du réseau. Elle est un livre potentiellement éternel car partagé par tous les participants du réseau qui le souhaitent. Enfin, elle est absolument transparente à chaque instant : c'est la base de tous les échanges Bitcoin qui doivent sans cesse se référer à elle. La blockchain est la mémoire du réseau Bitcoin où l'adage *tempus fugit* se voit subtilement contredit.

Une multitude d'utilisations promise dès sa création

Le lecteur pourrait à présent nous faire quelque reproche : ce que nous racontons de Bitcoin est bien beau, peut-être, mais il n'a pour l'instant aucune idée de comment s'en servir concrètement… Et il aurait raison. Nous avons en effet passé volontairement sous silence cet aspect pour l'amener dans cette partie et dans les suivantes.

Après avoir vu ce qui serait plutôt le côté logiciel serveur de Bitcoin, consacrons-nous à sa phase client. En effet, la « question a mille francs » est bien *comment se sert-on de Bitcoin ?* Pour cela, rien de plus simple. Si le lecteur se souvient de l'analogie du navigateur web utilisant le protocole HTTP, eh bien les logiciels utilisant Bitcoin sont pléthores et l'équivalent du navigateur serait le *wallet* ou communément appelé portefeuille en français.

Il est fort amusant de voir encore une fois un décalage dans le mot choisi. Il est uniquement tourné vers l'usage monétaire, fidèle à la nature première de Bitcoin. En réalité, il serait plus juste de parler de trousseau de clefs. Car, comme le lecteur l'aura compris, on ne possède jamais réellement de bitcoins sur son ordinateur, on a juste une preuve de propriété matérialisée par des jeux de clef privée et clef publique.

Le jeu de clefs est généré comme cela a été abordé plus haut par l'algorithme nommé ECDSA (*Elliptic Curve Digital Signature Algorithm*). Le mécanisme de cryptographie asymétrique permet d'effectuer à l'aide d'une clef privée une signature que tout le monde peut aisément vérifier à l'aide d'une clef publique. Tout est fondé sur le principe *hard to find, easy to check*.

Lors d'une transaction Bitcoin sur un *wallet*, l'utilisateur va en réalité signer la transaction à l'aide de sa clef privée pour prouver qu'il possède bien les bitcoins correspondant à une adresse donnée. Voici un exemple de clef privée :
KzWfvZJeBeqNHWyiT4XMbwJw9RAwNqJ1fMQmDiQnNZrFSRCFb5xC

Voici la clef publique compressée associée à cette clef privée :
0299fc1197699e5a5847c87cdef23a9d6d40c051c4f4659177561f351887216461

Inutile d'insister sur le fait que vous ne vous servirez pas de ces clefs. En effet, si elle est ici publiée, la clef privée est *de facto*… publique et grillée[56].

La clef publique est très longue et s'écrit en base 16. Pour plus de commodité et pour que les clefs publiques restent tout de même discrètes, celles-ci subissent un double hashage en SHA-256 et en RIPEMD-160 pour finalement être encodées en Base58Check, ce qui permet d'enlever les 0, O, 1, l, qui peuvent être confondus facilement suivant la police. Le but est ici de rendre tout simplement la clef publique potentiellement lisible et reproductible sur clavier par un humain, en la transformant en quelque chose d'autre, dérivée d'elle-même et par conséquent liée à celle-ci. L'adresse correspondante sera donc sous cette forme :
12725SMAp62NkkyqEnArHWSDADDpjyxk8i

Soit un hash de 34 (le plus souvent[57]) caractères alphanumériques commençant forcément par 1 (pour une adresse à signature unique) ou par 3 (pour une adresse partagée).

L'adresse peut être tout simplement considérée comme l'emplacement ou le numéro d'un coffre. Elle permet de faire pointer des bitcoins d'un coffre à un autre grâce à la blockchain et au réseau. Ainsi le possesseur de la clef correspondant au coffre sera le seul à pouvoir envoyer ses bitcoins vers d'autres coffres. Le portefeuille est avant tout le lieu où les clefs sont stockées et donc, par extension dans notre esprit, (car même si c'est faux substantiellement parlant, notre esprit est trompeur !) le lieu où les bitcoins sont stockés.

Tout déplacement de bitcoins sera instantanément relayé sur le réseau. Comme dit plus haut, les transactions sur la blockchain sont intégralement et instantanément transparentes. Toute adresse est donc traçable par définition. L'exactitude voudrait que l'on désigne le bitcoin comme une monnaie *pseudonyme*, en ce sens que son anonymat est relatif. Nul n'a aucun moyen, en regardant la blockchain, de savoir qui se trouve derrière telle adresse ; en revanche, si l'on arrive à obtenir cette information par un autre biais, on pourra remonter toutes les transactions de ladite adresse. Cette subtilité a son importance car elle pose le problème de la fongibilité, qui sera abordé au prochain chapitre, mais elle remet aussi en question l'accusation de monnaie de la drogue que l'on porte contre le bitcoin. Bitcoin n'est pas anonyme mais discret. Pour avoir une discrétion plus grande, Satoshi Nakamoto a implémenté dès le début la fonctionnalité de rotation d'adresses qui fait que les adresses sont considérées comme potentiellement jetables car utilisées une seule et unique fois. Nous verrons dans le point III, 2 comment d'autres projets essaient soit de permettre à Bitcoin de devenir anonyme, soit de créer d'autres concepts.

Il y a de nombreux *wallets* différents sur le marché, avec de nombreuses caractéristiques différentes. Nous allons les classer ici par commodité d'utilisation, pour nous attirer un peu de reconnaissance du lecteur qui vient de pénétrer dans l'antre complexe du Bitcoin !

Les *wallets* les plus simples sont les *webwallets* : ils sont généralement entretenus par une société qui détient les clefs à la place du client. Celui-ci n'a dès lors qu'un identifiant et un mot de passe, comme sur la majorité des sites classiques. Il aura dans ce portefeuille accès à la plupart des fonctions monétaires de Bitcoin et pourra même créer parfois des portefeuilles à plusieurs signatures au sein de ce site. Un des autres avantages de ces portefeuilles est l'accès sur tous les supports, dans n'importe quel endroit ayant un accès à Internet et un navigateur. Bien que

très faciles à utiliser, ces portefeuilles sont à considérer, justement, comme des portefeuilles dont on peut accepter d'être dépouillé sans trop de perte, et à déconseiller pour stocker à long terme, comme dans un coffre, l'épargne en bitcoin. Car on comprend aisément qu'ils rendent tributaires d'un tiers qui gère en réalité les clefs, alors que le principe même de Bitcoin est d'éviter cela. Certains pourront tout de même avoir des services exclusifs pouvant justifier cette « prise de risque ». On citera en exemples : Xapo, Coinbase ou Blockchain.info, mais de nouveau, juste pour la monnaie que l'on veut avoir « sur soi ».

Ensuite viennent les « clients légers », qui ont l'avantage de ne pas télécharger l'intégralité de la Blockchain mais seulement les en-têtes des blocs (solution commode notamment pour les mobiles). Ils passent souvent par l'intermédiaire d'un serveur tiers, mais cela ne compromet pas l'intégrité du jeu de clefs qui n'est pas stocké à distance. Il est juste possible qu'un jour les serveurs faisant tourner le logiciel client lourd (client/serveur) soient indisponibles pour diverses raisons. Mais cela n'arrive que très rarement. C'est le juste milieu entre le *vault* (coffre-fort) lourd et le *webwallet*. Ces « clients légers » sont généralement disponibles sur beaucoup de systèmes d'exploitation mobile et bureau. Ils possèdent bien souvent une *pass-phrase* (ou phrase de passe), appelée *seed*, permettant de régénérer la clef en cas de perte de l'appareil. Cette *seed* est un ensemble de mots générés aléatoirement, en nombre habituellement supérieur à 12. Cette sécurité d'un format très commode peut et doit être inscrite soigneusement sur un papier que l'on ne perdra pas. Ces portefeuilles sont d'une manière générale très pratiques au quotidien et idéaux pour commencer à acheter et dépenser des bitcoins. On citera en exemples : Copay, Breadwallet ou Mycelium.

Mais les *wallets* n'existent pas seulement sous forme de logiciels, il y a aussi ce que l'on appelle des *hardware wallets* qui sont des portefeuilles physiques/matériels. Ils confèrent une sécurité accrue grâce à des facteurs de sécurité supplémentaire comme des puces par exemple. Bien souvent reliés en USB à un ordinateur, ils sont suppléés par un logiciel dédié ou par des logiciels tiers les supportant. La sécurité de ces portefeuilles est excellente et leur utilisation très facile. Il faut selon nous les considérer comme des *vaults* : le mobile reste pour l'instant plus utile pour un paiement quotidien. Ils sont en revanche une solution de thésaurisation à court, moyen ou long terme qui semble tout à fait idéale. Mais à la différence des logiciels qui, eux, sont tous gratuits, ces *hardwares* sont payants. On citera en exemple : Ledger, Trezor ou KeepKey.

Puis il y a les clients lourds, qui seront des nœuds complets du réseau. Ils ont l'avantage d'être totalement indépendants de quiconque. Ces portefeuilles seront le plus souvent utilisés par des passionnés de Bitcoin car cela permet au réseau de posséder un nœud de plus, et donc un relai de plus. Il est important qu'il y ait un nombre de nœuds conséquents sur le réseau Bitcoin, de sorte à avoir une bonne propagation des transactions. Mais ils seront aussi utilisés par des entreprises ayant besoin d'utiliser toutes les fonctionnalités de Bitcoin. Ces clients sont toutefois vraiment lourds car ils téléchargeront la blockchain dans son intégralité (proche de 100 Go à fin 2016[58]) et le relai des transactions prendra de la bande passante et de la mémoire vive. Un problème demeure avec ces portefeuilles en général à disposition des ordinateurs : ils sont dépendants de la sécurité de l'environnement utilisé. Par conséquent, si l'ordinateur est infesté de virus, rien ne dit que la clef ne soit pas dérobée (on peut cependant la chiffrer avec un mot de passe). Ce sont donc des portefeuilles destinés à des usages bien précis et que l'on réservera à un public plus averti. On citera en exemples : Bitcoin-core, Armory ou mSIGNA.

Enfin, les moins commodes de tous les wallets sont ceux qu'on nomme les *cold wallets*, dont la particularité est d'être déconnectés d'Internet. Ce sont par exemple une clef privée et une adresse générées sur un ordinateur non connecté à Internet que l'on note dans un endroit sécurisé. Il est également possible de ne noter cela nulle part et de considérer pouvoir la garder en tête, on appelle cela un *brain wallet*, qui pourra être une suite de 12 mots que chacun encodera à sa guise. Moyens extrêmement sûrs et très peu corruptibles, ils sont cependant aux antipodes de la commodité. Pour dépenser les bitcoins envoyés sur l'adresse, il faudra d'abord réécrire entièrement la clef privée pour après envoyer les bitcoins. Ce sont donc des moyens de thésaurisation à long terme mais en aucun cas des *wallets* de convenance pour faire du shopping. On citera comme exemple : BitAddress ou WarpWallet.

Notre rapide tour d'horizon terminé, nous ne pouvons que conseiller au lecteur de tester lui-même et concrètement les exemples en question ; chacun trouvera chaussure à son pied. Bitcoin contient déjà dans son protocole un grand nombre de possibilités monétaires très bien exploitées par ces différents *wallets*. Comme l'écrit joliment Benoît Mandelbrot au détour d'un livre plutôt stimulant sur l'approche fractale des marchés : « Pour réellement saisir ce qu'est l'économie, laissez tomber les livres et les cours et essayez-vous au commerce des vêtements.[59] »

Maintenant que nous avons vu comment faire des transactions, concentrons-nous sur les possibilités transactionnelles qui s'offrent à nous. Il faut revenir ici sur les fonctions intégrées par défaut dans le protocole Bitcoin et utilisables par le biais de certains services ou certains *wallets*. Comme nous l'avons expliqué précédemment, les transactions comportent des scripts (sorte d'actions à conditions), même en ce qui concerne l'acte le plus simple qui est de dépenser des bitcoins. Nous avons aussi vu le pratique nLockTime qui permet de bloquer des bitcoins avant un temps donné. À celui-ci s'ajoute une autre manière de bloquer des bitcoins depuis fin 2015, nommée OP_CHECKLOCKTIMEVERIFY qui complète nLockTime et en augmente les possibilités[60]. Il permet de créer des transactions à terme autonomes, ce qui rend inutile toute intervention humaine après la programmation de la transaction. Cependant, cela implique également que ce genre d'opérations soit irréversible.

Mais il ne s'agit là que d'une faible partie de toutes les possibilités offertes directement par le protocole. En effet, il est déjà possible avec bitcoin d'effectuer ce que l'on appelle des *smart contracts*. Cette terminologie provient de Nick Szabo qui inventa ce terme en 1994[61] pour spécifier qu'il fallait importer la logique du droit des contrats dans certains cas informatiques et commerciaux. Mais le terme de « contrat intelligent » est un peu trompeur : le contrat n'est pas intelligent, mais surtout intelligible pour la machine. Et cela permet de conférer une autonomie à la machine. Nous préférerons dès lors parler de contrat auto-exécutable, ce qui exprime l'idée qu'il ne nécessite pas de tiers pour fonctionner une fois les conditions réunies, bien que le terme précis de « contrat » soit discutable d'un point de vue juridique.

Dans Bitcoin, ces contrats peuvent prendre la forme de conditions associées à des fonctions. Les principales fonctions de Bitcoin sont, comme nous l'avons vu, la signature pour prouver la propriété de ce bien immatériel qu'est un bitcoin. Mais sa variante dite « multisignature » autorise l'utilisation d'une adresse à plusieurs, tout en ayant des mécanismes de consensus prédéfinis. Pour l'instant le protocole permet de créer des adresses partagées avec 2 à 15 personnes et un facteur d'accord libre entre 1 et 15. Et, encore une fois, dans la dure loi des contrats auto-exécutables il n'y a pas de retour en arrière. Un chiffre déterminé ne pourra être modifié et ainsi le nombre de personnes requises pour débloquer les fonds ne changera pas en cas de désaccord. Ce type de portefeuille peut être très utile pour les associations notamment, et nous l'utilisons d'ailleurs au Cercle du Coin.

Cette simple action montre la puissance de la monnaie programmable. En effet, qui dit libération de fonds sous condition préalable avec un consensus au sein d'un groupe dit mutuelle. Organiser l'aspect technique d'une petite mutuelle ne prend plus que quelques secondes avec Bitcoin. Et ce n'est que le début.

Une autre fonction déjà très utile est celle des *payment channels*, qui permettent par exemple de faire des transactions avec paiement à la livraison. Grâce à ce procédé les bitcoins peuvent être envoyés à un vendeur, celui-ci ne les percevant qu'une fois qu'il a cloturé le paiement lorsqu'il a expédié le colis. Si la période d'expiration est dépassée, le payeur est remboursé. Cela permet aussi de faire de simples contrats de *crowfunding* : si telle somme est récoltée dans un temps requis, les fonds sont envoyés à une adresse précise (pourquoi pas sur l'adresse multisignature des porteurs du projet ?) et dans le cas contraire tous les participants sont remboursés. Ces contrats sont très simples, mais déjà d'une efficacité et d'une rigidité redoutables. On constate aussi la pertinence de ce genre d'interactions pour une monnaie. Mais nous aborderons cela un peu plus loin.

Enfin, une dernière possibilité est celle laissée par les fameux 80 caractères libres après la fonction OP_RETURN. Cet espace disponible a permis la naissance de méta-protocoles, nommés *colored coins*, *open assets* ou autres, qui vont se servir de la fiabilité du réseau Bitcoin et de sa blockchain pour donner une coloration à certains bitcoins. À partir d'une fraction de bitcoin, il est possible d'émettre sa propre monnaie. Ces *colored coins* constitueront un excellent support pour les monnaies locales complémentaires le jour où leurs promoteurs cesseront d'opposer leurs idéaux à ceux du Bitcoin. Ils découvriront alors pour les MLC une solution bien moins coûteuse, facile à installer, fiable et ludique : certains l'ont déjà fait grâce à l'aide de Colu, à Tel-Aviv, Liverpool ou Londres.

Mais cela pourrait aussi amener à se développer des petites places de marché d'actions non cotées. Nous pensons notamment aux sociétés de *crowfunding* qui fonctionnent sur un principe de financement contre part et non contre contrepartie. Tous ces petits acteurs pourraient s'échanger ou se céder des titres plus facilement s'ils étaient considérés comme vrais en étant un jeton dans la blockchain. Plusieurs entreprises du secteur Bitcoin ont commencé à faire des levées de fonds avec distribution de parts en *colored coin*. C'est le cas de Mycelium Wallet qui a cédé 5 % de son capital en émission de *colored coins* à la hauteur de 1MYC = 1BTC. Ces actions sont désormais librement échangeables sur la plateforme d'échanges décentralisés Bitsquare.

Un dernier cas d'usage pourrait être celui des monnaies temporaires. Dans le cadre d'un évènement de type festival, les organisateurs préfèrent généralement ne pas avoir à gérer de cash et ils font souvent le change contre des jetons dans un seul endroit centralisé. Autre idée, cela a déjà été mis en œuvre, la coloration permet aussi de faire des jetons de collection émis en une occasion spéciale ou à des personnes particulières. Le caractère inaliénable et éternel s'accorde très bien avec les collections. Bref, c'est un nouveau monde qui s'ouvre avec les méta-protocoles.

Et tout cela n'est qu'un aperçu du potentiel de Bitcoin. Bientôt viendront les *sidechains*, *Lightning* ou le projet *Rootstock* dont nous parlerons au point III, 2. Et cela fera de Bitcoin un protocole absolument protéiforme. En effet, au travers de nos pérégrinations nous n'avons pour l'instant fait que reconnaître l'aspect monétaire évident de Bitcoin. Nous avons constaté qu'il offre des fonctions permettant l'exécution de contrats auto-exécutables qui facilitent ainsi les transactions monétaires aux règles simples. Autre constat : les mécanismes de base de Bitcoin ont permis le développement de tout un écosystème de processeurs de paiement avec des *wallets*, pour la majorité libres, ouverts et gratuits. Nous avons enfin observé que la liberté du protocole a très rapidement inspiré certains pour écrire eux-mêmes d'autres protocoles de facilitation de gestions de titres numériques. Désormais, nous espérons que le lecteur a une idée suffisamment éclairée sur le fonctionnement et les possibilités offertes par le protocole Bitcoin.

2- Croquis des caractéristiques tant numériques que monétaires du bitcoin

Les propriétés numériques du Bitcoin

Si notre lecteur est parvenu jusqu'ici, c'est qu'il a été suffisamment intéressé (par les trois premiers chapitres) et rassuré (par le point II, 1). Il peut dès lors aborder les fonctions monétaires du bitcoin, non sur le mode du déni (ce n'est pas une « vraie » monnaie), mais sur le mode de l'analyse : quel genre de monnaie est le bitcoin ?

L'inventeur du bitcoin l'a d'abord décrit comme *A Peer-to-Peer Electronic Cash System*. Une appellation limpide dès ses débuts : celle de système de cash électronique en pair-à-pair. Cela ne nous donne pas pour autant un adjectif unique à employer en français. Or ce choix nous plonge au cœur de la chose.

Du point de vue des pouvoirs publics et des médias, la chose paraît entendue : le bitcoin est une monnaie « virtuelle ». Nous allons donc commencer par expliquer pourquoi ce mot est inapproprié, bien qu'il soit largement repris. Ainsi, lors des présentations que des consultants organisent pour les banques au sujet de la « technologie blockchain », revient souvent l'assertion selon laquelle on peut certes, jeu amusant ou expérience instructive, y faire circuler une devise « virtuelle » comme le bitcoin, mais tout aussi bien des devises « réelles » comme l'euro, ce qui serait évidemment plus utile, plus concret. La différence paraît évidente, et le décor ainsi planté conduit à la conclusion désirée : ce qui est utile, c'est « la blockchain ». Or cette analyse triviale indique seulement le point de vue de l'orateur par rapport au cyberespace, elle ne cerne pas le bitcoin.

Le *bitcoineur*, comme Alice, est passé de l'autre côté du miroir. Dans le monde des sens physiques, celui qu'Alice appelle *the old room*, c'est-à-dire dans ce qui est pour nous le monde des États territoriaux, l'euro est bien réel. Il tinte sur le comptoir, peut se glisser dans la poche et même réduit à une simple écriture comptable que l'on manipule par carte ou par téléphone, il se raccroche à cette réalité tangible primitive. À l'inverse, personne ne voit le bitcoin, il a peut-être une valeur, puisqu'il s'achète et se vend, mais tant qu'il n'est pas changé contre euro, cette valeur est virtuelle, sauf chez quelques trop rares commerçants amis qui l'acceptent en paiement. N'oublions jamais l'aspect contextuel en comparant l'incomparable.



Alice au Pays des cyber-merveilles (article de Jacques Favier)

Mais de l'autre côté du miroir, sur une blockchain, que ce soit celle du bitcoin ou une copie, c'est l'unité de compte de ladite blockchain, le *token* qui est la chose en soi, réelle. Le bitcoin, tel qu'il est sur sa blockchain, est tout entier l'être et le signe, bien réel dans ce monde de signes et de lois mathématiques. En revanche, tout ce que l'on veut y accrocher d'autre, tout ce qui vient de l'autre monde (devise classique régulée par une banque centrale, action inscrite dans un registre du commerce, contrat régi par une loi nationale) ne sera jamais sur la blockchain employée à cet effet qu'une représentation, une promesse, un contrat relatif aux objets classiques. Comme d'habitude, les points problématiques sont les tunnels menant du tangible à l'intangible. Ils ne peuvent pour l'instant exister qu'à l'aide d'un tiers. Réel ou virtuel, cela ne définit donc pas la monnaie, bitcoin ou euro.

Une fois écarté l'adjectif « virtuel », reste les débats sur le choix de l'adjectif qui convient le mieux au bitcoin : numérique, *digital*, électronique, cryptographique, décentralisé… Ces débats sont à la fois techniques – pour cerner en un seul mot l'essence de la chose – et juridiques – parce qu'ils visent à se nicher dans un statut ou à en éviter un autre. Ainsi, dans l'Union Européenne, le terme de monnaie électronique implique-t-il *une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement*. Quant aux mots *distribué* et *décentralisé*, ils nous semblent décrire mieux le registre (la blockchain) et le processus de validation (minage), que son unité de compte (le bitcoin) lui-même.

Avant de le caractériser comme monnaie, il semble qu'il faille rappeler que le bitcoin est d'abord un *objet numérique*, bien que l'on voie, hélas, plus souvent employé le mot *digital*, à l'opposé des recommandations de l'Académie française.

De prime abord, on pourrait dire que l'euro existe aussi sous forme numérique, mais en réalité ce sont les registres des banques qui sont numériques. Un inventaire informatique du stock d'un caviste ne transforme pas les bouteilles recensées en objets numériques, il les représente. Une liste informatisée des anges du ciel n'en fait pas non plus des objets numériques. C'est donc par abus que certains banquiers prétendent qu'après tout leur monnaie est aussi numérique ou digitale. Elle est essentiellement virtuelle car elle ne correspond à rien de réel en raison de sa création *ex nihilo* par le crédit.

Le bitcoin est essentiellement numérique parce qu'il n'existe que sous forme numérique, non pas comme transcription numérisée d'un objet physique ou sensible (une image, une mélodie) ou comme représentation scripturale d'un actif ou d'une dette, ou comme élément d'un inventaire d'objets tangibles ou non, mais comme la *res ipsa,* surtout qu'ici il est bel est bien question de langage !

Pour méditer sur la spécificité du bitcoin, réfléchissons un instant sur deux grandes conséquences du développement du commerce en ligne. Avec le commerce en ligne, ce qui s'est développé, ce sont les livreurs, leurs estafettes et leurs scooters, en attendant pour, dès demain, les drones. Un an avant la naissance du bitcoin, un petit film amusant avait été posté sur Youtube, vantant une clef USB d'où coulerait directement les meilleurs vins : « Avec le USB Wine, et en vous connectant au Wine Store, vous pouvez télécharger directement vos vins depuis chez vous parmi un choix de plus de 1 200 crus [62] ». Les objets tangibles ne se numérisent point. Et quand bien même ils le feront un jour (en branchant une imprimante 3D en sortie de l'ordinateur recevant le message) on n'aura jamais, en bout de course, qu'une copie. Peut-être le débat sur la reproductibilité à l'infini qui posait problème à l'art dans les années Warhol va-t-il de nouveau se poser à une échelle nouvelle.

Ce qui est numérisable, en revanche, voyage fort bien : une photo, une mélodie, un film. Tout le monde à l'habitude de prendre une photo et de l'envoyer à un ami, qui la reçoit presque instantanément. Seuls les plus anciens s'en émerveillent encore. Mais la photo reçue n'est, là aussi, que la copie de la photo envoyée (toujours en possession de l'émetteur) ou plutôt son double : l'information n'est pas dégradée et l'examen des fichiers ne permettrait pas d'identifier un original et une copie. C'est un peu gênant pour le commerce, voyez du côté de l'industrie du disque et même du cinéma. Pour contrer ce phénomène les industriels ont d'abord imaginé de surimposer, de tatouer, de taguer : le logo d'une chaîne de télévision sur les images d'un match dont elle possède seule les droits de reproduction, l'heure de prise de vue d'une photographie. On a imaginé d'incorporer un verrou dans le fichier, comme sur les articles de journaux « réservés aux abonnés ». Tout cela n'arrête que les plus scrupuleux et les moins débrouillards… Pourtant les DRM (*Digital Rights Management*) sont loin d'être abandonnés et commencent à être utilisés de manière de plus en plus perverse, par exemple dans les processeurs les plus répandus sur le marché. [63] Le combat du verrouillage, qui semble perdu d'avance, n'est pas encore fini.

Dire du bitcoin qu'il est un objet horodaté ne paraît donc pas, de prime abord, particulièrement révolutionnaire en informatique où l'horodatage est largement employé dans les journaux d'événements

(habituellement sous la forme d'une séquence de caractères représentant la date et l'heure à laquelle est survenu un événement, de façon à faciliter la comparaison entre événements)[64]. D'ailleurs, l'enthousiasme avec lequel certains présentent la « technologie blockchain » comme ayant le principal avantage de gérer un registre horodaté est plutôt comique, même s'il faut entendre que cet horodatage est infalsifiable d'une part, et qu'il n'est pas effectué par une autorité centralisatrice d'autre part. Contrairement à une date de publication sur un blog, il est impossible que quiconque change la date d'une transaction Bitcoin.

Qu'est-ce qui est réellement horodaté, et comment ? Citons Satoshi Nakamoto : « Le réseau horodate les transactions à l'aide d'une fonction de hashage qui les traduit en une chaîne continue de preuves de travail (des empreintes), formant un enregistrement qui ne peut être modifié sans ré-effectuer la preuve de travail. » Chaque « bloc » de transactions est constitué, comme on l'a vu plus haut, de deux parties : l'en-tête contenant un horodatage de la création du bloc, et la partie centrale qui contient une liste de transactions. Donc, à proprement parler, toutes les transactions ne sont pas horodatées individuellement. L'horodatage est le même pour toutes les transactions d'un bloc, et il peut actuellement y en avoir autour de 1500 dans chaque bloc. L'heure retenue n'est pas celle de la transaction mais celle où le mineur a reçu l'information transactionnelle ; tant que la transaction n'est pas validée, elle garde sa date initiale. Deux horodatages sont donc possibles, celui de l'heure de la réception de la transaction par le nœud qui peut être enregistrée hors de la blockchain (impossible sans tiers donc non fiable), et celui de l'heure où la transaction a été confirmée, minée et donc ajoutée à un bloc dans la blockchain (fiable et infalsifiable). Il peut donc y avoir un décalage entre la date d'émission de la transaction et sa date de réception par le mineur, mais de l'ordre d'une latence de quelques secondes tout au plus. En revanche, ce décalage est bien plus grand, de l'ordre de plusieurs minutes, au niveau de l'inscription dans la blockchain. Si cela ne gêne guère dans le cadre d'un processus de transaction, cela ne fait pas de la blockchain une machine à horodater à la milliseconde près, mais plutôt à l'heure près. Cependant, on peut imaginer des améliorations permettant d'avoir un horodatage plus précis sur la blockchain si c'est un jour nécessaire.

Une autre caractéristique du bitcoin comme objet numérique, qui tient, en partie, à cet horodatage, est le fait qu'il ne soit pas copiable. Le bitcoin est le premier objet numérique non copiable. On va naturellement copier une adresse (la série de 26 à 35 signes) voire une clef (la série de 64) sur plusieurs supports. Mais avoir deux clefs de chez soi ne donne pas un second appartement ! Ce bitcoin est inscrit à une adresse précise, avec son historique précis. Le copier reviendrait à l'envoyer à une seconde adresse tout en le conservant aussi à la première (comme avec une photo qu'on envoie à un ami). C'est ce que l'on appelle le *double spend*, l'un des redoutables problèmes qui se posaient à tous les concepteurs de monnaies numériques décentralisées, et que nul ne pouvait gérer que par l'existence d'une autorité centralisatrice empêchant ce double usage de la même somme.

Le bitcoin rend le *double spend* impossible, notamment du fait de l'horodatage et de la vérification des mineurs. L'attaquant (le tricheur) serait placé dans un processus aléatoire en raison du caractère probabiliste du temps de résolution, dont on a déjà dit qu'il était un temps *exponentiel*. Ses chances elles-mêmes vont décroitre exponentiellement avec le temps et tendre rapidement vers zéro[65].

Ce *double spend* est aussi impossible en raison de la façon dont sont concrètement effectuées les transactions, et en particulier grâce au mécanisme considérant la plus longue chaîne comme gagnante.

Il est de plus en plus rare d'effectuer une transaction avec des bitcoins vierges, disons natifs. Dans le portefeuille du payeur, il doit y avoir un solde suffisant pour acquitter le montant de la transaction. Mais – exactement comme dans un portefeuille physique – il n'y a pas forcément l'appoint. Ainsi un portefeuille assez modeste peut-il détenir des fractions de bitcoins issues d'un très grand nombre de transactions antérieures, chacune dotée de sa propre histoire. En fait, chaque petite fraction a son histoire, parfaitement publique et horodatée comme cela a été expliqué précédemment.

Ceux qui vérifient et valident les transactions ont quelques minutes pour vérifier les soldes, et répudier d'éventuels *double spends*. Une fois la transaction validée, il devient même impossible de réussir un second usage du bitcoin dépensé… puisqu'il n'apparaît tout simplement plus à l'adresse où il était détenu, comme un billet remis chez l'épicier n'est plus dans la poche du client.

La dernière caractéristique de cet étrange objet numérique, horodaté et non-copiable, c'est qu'il n'est qu'assez médiocrement fongible. Une pièce d'un euro vaut une autre pièce d'un euro (en fait et même en droit, sauf valeur de collection à prouver) et un fichier permettant l'exécution d'un film ou d'une chanson vaut un autre fichier identique permettant le même spectacle (en fait, sinon en droit). Pour en rester à la monnaie, quand on paie en

cash (dans les limites fixées par la loi), une bonne mine suffit. Si le billet est faux, le commerçant le rend s'il est sympathique, le banquier le confisque[66]. Si le billet provient d'un vol de fourgon blindé et que la banque en détenait les numéros, il est possible de se voir poser quelques questions (au moins sur la bonne foi de la personne impliquée). Mais nul ne peut savoir matériellement si le billet n'a pas été gagné par un travail non déclaré ou contraire aux bonnes mœurs, un commerce illicite ou l'exploitation d'esclaves. En réalité, les tests menés sur ce qui laisse des traces (la cocaïne notamment) laissent songeurs : tout le monde a vraisemblablement des billets infectés dans sa poche, mais c'est (sans doute) de bonne foi et en quantité (statistiquement) normale[67]. Avec les avoirs en bitcoins, les traces de cocaïne, mais aussi de vols, sont beaucoup plus faciles à retrouver. Nous y reviendrons.

Les propriétés monétaires de cet objet numérique

Il est temps, après avoir défini le bitcoin comme un *objet* numérique singulier, d'expliciter ce qui en fait une *monnaie* singulière. Nous avons jusqu'ici implicitement traité du bitcoin comme d'une monnaie, partant du principe qu'un lecteur curieux est en sympathie suffisante avec l'objet étudié pour ne pas se placer dans une attitude négative et stérilement critique.

Parmi ceux qui dénient cette qualité monétaire au bitcoin, l'argument favori est qu'il n'est pas frappé au nom d'un État ou émis par une Banque Centrale. Ce ne sont là que des restrictions juridiques portant sur la définition d'une monnaie *légale*, sans épuiser le débat sur le point de savoir si la monnaie appartient aux rois, aux peuples ou… aux marchands comme le pensait au XIV^e^ siècle le moine économiste et mathématicien Oresme, traducteur d'Aristote[68].

Plus subtile est la critique (émanant surtout d'économistes) qui dissèque les fonctions classiques de la monnaie listées par Aristote[69] (unité de compte, réserve de valeur et intermédiaire des échanges) pour contester que le bitcoin puisse les assumer toutes parfaitement. Michel Aglietta, par exemple, considère que le bitcoin n'est qu'un actif spéculatif couplé à une technologie de paiement. C'est aussi, curieusement, le point de vue de Bernard Lietaer, par ailleurs chantre de la biodiversité monétaire et des monnaies dites « alternatives ». Nous verrons au point II, 3, en abordant l'inventaire des usages hétéroclites du bitcoin, s'il satisfait à toutes les fonctions d'Aristote, et dans quelle mesure.

Mais ici, nous allons en rester au pragmatique dicton *money is what money does*, confortés par l'arrêt rendu en octobre 2015 par la Cour de Justice de l'Union Européenne[70] en faveur du sieur Hedqvist qui entendait gérer sa plateforme d'échange entre bitcoin et monnaies classiques sans acquitter de TVA, puisqu'en sont exonérées les opérations sur « les devises, les billets de banque et les monnaies qui sont des moyens de paiement légaux. » La CJUE lui a donné raison.

Nous voulons ici souligner non ce que Bitcoin, en tant que monnaie, n'est pas ou n'a pas, mais ce qu'il est, alors que les autres devises ne le sont pas : c'est une monnaie rare, très divisible et programmable.

Sa première spécificité, unique dans l'histoire en 2009, est d'être une monnaie à encours définitivement fixé. Bien sûr les monnaies de jadis étaient assez rares pour être précieuses, mais on découvrait des mines nouvelles et le stock d'or ou d'argent augmentait. Le bitcoin est d'un métal dont on ne connaît qu'un seul gisement, limité, et dont l'extraction est régulée.

D'autre part, c'est une monnaie à création programmée. Du temps des rois, la quantité de métal disponible ne dépendait pas immédiatement des besoins ou des décisions politiques. Les choses évoluèrent différemment avec les émissions de monnaies fiduciaires qui vinrent ensuite. Certes les monnaies d'autrefois ne furent pas conçues pour être illimitées : les premiers billets de banque (suédois, anglais) devaient correspondre à une encaisse et même les assignats révolutionnaires devaient correspondre à la valeur des « biens nationaux ». Seulement, entre le déficit, la guerre, une bonne dose de facilité et une pincée de malhonnêteté, tout se conjugua pour faire tourner la planche à billet. L'expression a conservé son pouvoir évocateur jusqu'à ce jour, résistant à la marginalisation de la monnaie papier, à la loi de 1973 plafonnant les avances directes de la Banque de France à l'État, au tournant historique de 1984, à l'article 104 du traité de Maastricht et à l'article 123 de celui de Lisbonne dépossédant littéralement les États de leur pouvoir de création monétaire.

S'il n'y a plus aujourd'hui de planche à billet, ni même d'expansion classique de la masse monétaire au service des gouvernements, les politiques d'assouplissement quantitatif (*Quantitative Easing*) à l'origine d'une

explosion sans précédent des bilans des banques centrales sont clairement une forme de création monétaire, ciblée seulement en direction des marchés financiers et sans grand effet sur la croissance. Comment peut-on imaginer que, si la création monétaire se matérialise sous forme d'intérêts bancaires, celle-ci soit propice à créer de la liquidité hors du marché secondaire ? Cette politique, largement mise en œuvre après l'apparition du bitcoin, a suscité de multiples critiques dont celle qui nous intéresse ici venue des monétaristes orthodoxes et des économistes de l'école dite « autrichienne ».

Lointains successeurs d'Oresme, pour qui la monnaie appartient à ceux qui la gagnent et l'utilisent, et qui seuls peuvent en définir le statut, les penseurs de l'école autrichienne critiquent, à la suite de Friedrich Hayek (1899-1992), les interventions étatiques sur les taux d'intérêt et sur la monnaie. Le retour à l'étalon-or (avec des banques qui ne pourraient prêter qu'à la hauteur de leurs actifs) est considéré par Hayek[71] comme le seul système tolérable malgré ses imperfections tant que les affaires monétaires sont entre les mains du gouvernement. Au-delà, l'une des idées apparues au sein de cette école est le concept de banques libres, sans régulation ni banque centrale, dont la concurrence pour l'émission de signes monétaires serait gage de qualité de celle-ci : les monnaies privées. Cette situation fut celle de 1716 à 1845 en Ecosse ou de 1891 à 1934 au Canada, pays qui ne connut alors aucune faillite bancaire. Le bitcoin s'inscrit comme un concurrent ou complément, libre et universelle, des monnaies des États.

Le bitcoin est donc créé par un algorithme, selon une loi mathématique (*vires in numeris*), avec une offre qui se raréfie au cours du temps alors même que l'engouement croît. Il n'y aura pas plus de 21 millions de bitcoins en tout et pour tout à l'horizon de 2140, et en pratique la limite sera déjà presque atteinte en 2032. Sur ce sujet, les positions des uns et des autres sont irréconciliables et le débat difficile. Aux uns, cela apparaît au mieux comme une sottise arbitraire (pourquoi 21 millions ?) et au pire comme un schéma de Ponzi potentiellement dramatique par ses effets déflationnistes. Aux autres, le montant limité de l'encours paraît comme la certitude absolue de la valeur de la monnaie. La difficulté que sa « rareté » pourrait occasionner serait pour eux aisément résolue par sa très grande divisibilité (pratiquement infinie), autre caractéristique numérique de cette nouvelle devise. Essayons donc de passer en revue les arguments.

Les règles mathématiques apparaissent incohérentes ou arbitraires à ceux qui ne les comprennent pas, surtout quand elles heurtent une représentation spontanée simpliste : les petits enfants demandent souvent pourquoi le nombre π n'est pas tout rond. Il semble qu'en fait Satoshi Nakamoto n'ait choisi de grandeur de manière arbitraire qu'en matière de temps (*time is money*) en fixant une diminution de la rémunération selon une périodicité de 4 ans, ce qui peut correspondre à une olympiade, à une durée de temps constante (compte tenu de l'année bissextile) ou à quelque autre considération gardée secrète. Le rythme de validation toutes les dix minutes peut aussi être considéré comme semi-arbitraire, même si des études[72] révèlent sa grande pertinence par rapport à la vitesse de propagation dans le réseau et à divers paramètres techniques. En 4 ans, il y eut environ 210 388 intervalles de dix minutes, un nombre sans doute arrondi à 210 000, le nombre de blocks séparant deux *halvings*. Restait à répartir la création (une fois décidé pour des motifs propres que celle-ci serait limitée) en une suite de fractions. La suite inspirée de Zénon (un demi plus un quart plus un huitième etc) a une somme qui tend vers 1 et elle a été retenue sous la forme 50 bitcoins, plus 25, plus 12,5, etc. formant un total de 100 qui, multiplié par 210 000 blocs pour chaque fraction établit le fameux total de 21 millions. Tous les nombres d'origine tombent juste en base binaire, ce qui pourrait aussi être une raison supplémentaire étant donné que toutes ces écritures ne sont que des 0 et des 1.

La « rareté » de bitcoin comme devise comporte certainement une dimension idéologique. Pourtant, avec 50 bitcoins créées toutes les dix minutes au cours des quatre premières années, son inflation à deux chiffres était impressionnante : plus de 100 % la première année, encore 32 % en fin 2012 à la veille du premier *halving*, lorsque la rémunération passa à 25 bitcoins. Elle était encore supérieure à 8 % à la veille du second *halving* en juillet 2016 et restera assez longtemps dans la gamme des 4 % pour ne passer sous les 1 % que *dans* la prochaine décennie. Pour le dire autrement, il y avait 2,6 millions de bitcoins créés à la fin de la première année, 10, 5 millions en novembre 2012 à la veille du premier *halving* et 15,7 millions en juillet 2016 à la veille du second. Inutile d'insister sur le peu de valeur qu'aurait une monnaie classique émise à ce rythme ! Or, malgré une forte volatilité, le bitcoin qui ne valait rien à sa naissance, et dont la capitalisation totale n'excédait pas le prix d'une chambre de bonne sous les toits de Paris à la veille de son premier *halving*, a connu une incroyable courbe en J, menant cette capitalisation à près de 12 milliards de dollars dans les derniers jours de 2013, suivie d'un plongeon d'un an jusqu'à 2,4 milliards et une d'une reprise qui l'a ramenée autour de 10 milliards lors du *halving* de juillet 2016 et d'une quinzaine au début de 2017. Autant dire que le bitcoin ne se comporte pas, jusqu'à présent, en monnaie inflationniste.

L'appréciation du cours, incompréhensible du côté de ceux qui annoncent la mort de Bitcoin (plus de cent faire-part en 8 ans[73], dont plusieurs signés de « Nobel » d'économie[74], les guillemets pour rappeler qu'ils ne sont pas distingués par une Académie mais récompensés par une banque centrale), serait donc le stigmate de deux crimes : une monnaie déflationniste et un schéma de Ponzi. Il suffit de réfléchir quelques secondes pour voir que les deux crimes peuvent difficilement être concomitants !

Ponzi est le « point Godwin » en finance, surtout depuis l'affaire Madoff, laquelle n'est pas née au sein des marges libertaires mais au cœur mondain de l'establishment. Dans un tel schéma, comme le capital est consommé, il faut de plus en plus d'acheteurs jusqu'à ce que tout s'écroule. Or sur les *exchanges* de bitcoin, nul n'est besoin de deux acheteurs pour un vendeur ! Une pyramide de Ponzi[75] ne repose sur rien, et se cache derrière un mensonge. Madoff montrait à ses clients des ordinateurs inutiles et des courbes bidon pour les convaincre. Le protocole de bitcoin est en *open source*. Ceux qui disent que Bitcoin ne repose sur rien ignorent seulement ce sur quoi il repose.

Sa performance exceptionnelle comme actif financier en 2013 en fait-elle un schéma de Ponzi ? Non. Tout le monde voyait monter le titre. C'était peut-être très spéculatif, il y a certainement eu une bulle et des acheteurs naïfs, sans idée sur la valeur fondamentale de l'actif, attirés par l'appât d'un gain rapide. Mais tout cela était public. Les titres vendus par Madoff n'étaient cotés nulle part et le grand public n'a entendu son nom que le jour de sa chute. La chute du bitcoin en 2014 n'en fait pas davantage un Ponzi. Il a certes baissé presque continument, mais en bon ordre. Ceux qui avaient secrètement souscrit chez Madoff se sont réveillés un beau jour en apprenant que leurs titres ne valaient plus rien et que M. Madoff coucherait en prison.

La critique du caractère déflationniste du bitcoin est plus élaborée : sa rareté, la difficulté croissante de son minage, et un engouement croissant se conjuguent effectivement pour pousser sur le long terme la valeur du bitcoin à la hausse. Bien sûr, les détracteurs qui affirment que « sa valeur ne repose sur rien » ne devraient pas être autorisés à s'inquiéter d'un effet déflationniste. Mais ses supporters, qui ajoutent l'utilité du bitcoin (on y reviendra) à la liste des facteurs de hausse ne peuvent éluder la critique.

Certes le bitcoin est extrêmement divisible : non en 100 centimes mais en cent millions de « satoshis ». Donc si le bitcoin doit un jour valoir non plus 1 000 mais 1 million d'euros, on pourra toujours payer son café avec quelques centaines de satoshis. Cet argument, qui satisfait la plupart des *bitcoineurs*, ne prend manifestement en compte que la seule difficulté matérielle : si l'on avait dû conserver l'or depuis 1914 tout en gérant l'inflation, il aurait fallu écrire « 20 francs » sur des pièces non plus de 6,45 grammes, mais de plus en plus petites, des milliers de fois plus petites. Il est effectivement plus facile de diviser un bitcoin qu'une pièce en or. Mais c'est, selon nous, ne pas répondre tout à fait à la question. La mauvaise monnaie chassant la bonne, celui qui a compris l'utilité (donc le potentiel d'appréciation) du bitcoin à tout intérêt à continuer de payer son café en dollar ou en euro pour l'instant. Le bitcoin est-il alors, du moins temporairement, une monnaie à faible circulation ? Même si les transactions croissent régulièrement, il est évident que le bitcoin ne s'est pas répandu dans le large public comme certains l'avaient peut-être imaginé au moment de sa première bulle, vers 2013, et que l'on peut s'en accommoder ou s'en lamenter parce que « l'argent n'aime pas rester immobile. Il aime sortir et se faire de nouveaux amis. »[76]

On reviendra au chapitre suivant sur la multiplicité de ses usages possibles, pour tenter de cerner les « vrais » emplois du bitcoin à l'avenir.

Compte tenu de ce qui vient d'être dit, dénoncer le caractère déflationniste du bitcoin ne peut se faire qu'en supposant qu'il soit universellement adopté, tout en expliquant dans la même phrase que cela ne peut marcher. C'est en plus oublier que, contrairement aux monnaies classiques, Bitcoin est un protocole. Il est agile et peut être mis à jour au cours du temps face aux problèmes auxquels il peut être confronté.

Il reste une spécificité majeure : le bitcoin est une monnaie programmable. On a vu des exposés sur la « technologie blockchain » montrer comment celle-ci pourrait mettre en relation des objets qui feraient entre eux et sans nul centralisateur des transactions automatiques. On a entendu dire que la blockchain pourrait créer des Uber ou des Airbnb décentralisés, sans financiers prédateurs au centre. Et sur les diapositives projetées, pour symboliser ces paiements automatisés sur des blockchains qui vont « beaucoup plus loin que les seules applications financières » comme il convient de le dire en début de présentation pour que les banquiers présents consentent à écouter, de jolis symboles €. Il y a un *hic*, cependant, qu'il est presque malséant de rappeler : l'euro n'est pas programmable, ce n'est pas une *smart money*. Accessoirement, les systèmes informatiques des banques sont

rigoureusement fermés et il est bien dur de créer une application sur la plateforme de sa banque. Le bitcoin, dont le programme est en open-source, est, lui, programmable.

Les perspectives que cela ouvre en termes d'utilisations contribuent aussi, en partie, à lui donner sa valeur…

La valeur du bitcoin : une interrogation ardue

Entre particuliers, dans les réseaux *Local Bitcoin*, dans des guichets de change, comme *La Maison du Bitcoin* à Paris, ou automatiques (surtout présents en Suisse ou en Belgique, mais il en existe aussi en France), mais surtout sur des plateformes de mise en relation ou de trading, le bitcoin s'achète et se revend. Il a donc un prix et une liquidité certaine. En l'absence de marché régulé, les cours affichés sur les diverses plateformes peuvent varier, mais cela attire des arbitragistes qui contribuent à réduire les écarts instantanés. Certains médias spécialisés agrègent et moyennent ces données, affichant ainsi un index des « cours » du bitcoin, à peu près à la façon dont on donne jour par jour le « cours de l'or ».

On peut critiquer la volatilité du bitcoin qui reste encore très forte, bien qu'il faille remettre cette critique dans son contexte : celui du poids monétaire total du Bitcoin. Mais ni les scandales liés à son utilisation à des fins illégales, ni les vols massifs par des pirates exploitant l'insuffisant niveau de sécurité de certaines plateformes, ni l'escroquerie de certains gestionnaires de plateforme, ni le dégonflement de la bulle de 2013, ni les menaces émises par certains régulateurs, ni les débats parfois acrimonieux des principaux développeurs de BIP (*Bitcoin Improvement Proposals* : propositions d'amélioration du protocole Bitcoin), ni les désaccords violents et intéressés sur les moyens d'accompagner la montée en charge du réseau n'ont ramené sa valeur à zéro. Au plus bas de sa chute consécutive à la bulle, la capitalisation de bitcoin restait proche de 3 milliards de dollars.

Ainsi posé le constat est simple : le bitcoin ne vaut pas rien. Mais que vaut-il ? Pour être plus précis : qu'est-ce qui lui donne sa valeur, proche en fin 2016 d'une quinzaine de milliards de dollars aux yeux de ceux qui achètent, vendent et détiennent cette devise, et qui sont en 2016 peut-être un peu plus d'un million dans le monde ?

Parmi les sceptiques, les plus adroits sont ceux qui avouent leur incapacité à percevoir ce qui donne sa valeur au bitcoin. Ainsi faisait ingénument Alan Greenspan en décembre 2013 : *« You have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it »*. Sans doute forçait-il quelque peu son talent.

La première réponse, malveillante mais possible, est que cette valeur ne serait qu'une illusion, soutenue par un montage pyramidal de type « Ponzi ». On l'a déjà réfuté par l'argument de la transparence de Bitcoin, qui détone avec l'opacité propre aux montages pyramidaux. Autre réponse possible : les arnaques de ce type ne se relèvent que rarement de leur première chute.

Il en est de même, une fois dissipée l'illusion, de ces bulles qui, même sans mauvais génie caché, fonctionnent toutes depuis la plus ou moins mythique tulipomanie hollandaise du milieu du XVII^e^ siècle sur l'enthousiasme naïf et l'appât du gain.

Après la tulipe, le coquillage fournit une autre réponse à ceux qui, ne comprenant ni la prouesse technologique ni l'utilité d'un actif numérique non copiable, distribué, horodaté et sécurisé, ne peuvent mesurer sa valeur. Avec mépris, ils se trouvent drôles en comparant le bitcoin aux coquillages des primitifs. Les *bitcoineurs* retournent le compliment : on voit mal en quoi un coquillage, possédant des qualités esthétiques, suffisamment rares et dont les sites de cueillette sont contrôlés, aurait moins de valeur intrinsèque qu'un billet de banque et pourquoi il ne pourrait pas fournir, aussi bien, un support matériel à un ensemble de liens sociaux[77]. Cette comparaison, désinvolte mais fréquente révèle donc un malaise inconscient sur la valeur de la confiance par ailleurs si bruyamment évoquée en matière de monnaie légale.

Si l'on en vient aux comparaisons non malintentionnées, celle qui, recherchant le fondement de sa valeur, fait du bitcoin un « or numérique » est sans doute la plus commune. Elle ne fait pourtant pas l'unanimité au sein des bitcoineurs eux-mêmes, tant du fait de la multiplicité des usages et des perceptions du bitcoin que d'une relative incompréhension sur l'or. Ainsi bien des gens soutiennent-ils que l'or est un choix conventionnel, une construction sociale vaguement assise sur d'ancestrales croyances religieuses. Le tout en citant la *relique barbare* de

Keynes sans grands égards ni pour le texte de celui-ci[78] ni pour les données de la physique. Dire de l'or qu'il a été choisi par commodité (grande valeur dans un faible volume) n'en explique pas la grande valeur.

La valeur de l'or, attestée dès la préhistoire, provient de la conjonction de sa rareté, de sa beauté et de son inaltérabilité, pour mettre entre parenthèses ses capacités physiques remarquables découvertes plus tard dans l'histoire. Dès lors, il n'est pas insensé de comparer le bitcoin à l'or : sa rareté qui lui est par ailleurs reprochée est évidente ; sa beauté ne se révèle certes qu'aux initiés, encore que l'émerveillement devant la « technologie blockchain » soit une forme d'hommage profane ; enfin son inaltérabilité doit être mesurée comme celle de l'or indépendamment de considération sur le maintien de sa valeur de marché. L'or est inaltérable non parce qu'un napoléon d'or vaudrait à coup sûr 220 € dans un siècle, mais parce qu'il pèsera toujours 6,45 grammes à 900‰, sans évaporation, pourrissement ou oxydation. Un bitcoin n'offre aucune garantie de valoir pour toujours 1 000 € mais, tant que quelques ordinateurs dans le monde tourneront et entretiendront le réseau, il sera identique à lui-même dans son essence et dans ses potentialités. À cet égard, l'argument d'un changement de paradigme avec l'apparition à terme indéterminé de l'ordinateur quantique est souvent invoqué. Mais c'est un argument peu percutant : les algorithmes *quantum-proof* (résistant à l'ordinateur quantique) sont d'ores et déjà théoriquement écrits[79]. En outre, il est difficile de prédire quoi que ce soit quant à l'apparition d'un ordinateur quantique car ce n'est pas un changement paradigmatique sociétal mais carrément d'ampleur physique ! Cet argument apocalyptique met en outre de côté le fait que la totalité des systèmes informatiques mondiaux seraient mis à mal, y compris ceux des banques.

L'or est une monnaie internationale. Un napoléon pèse 6,45 grammes à 900‰, un souverain britannique pèse 7,99 g à 916‰ : au-delà des jolies gravures qui ornent les monnaies, une règle de trois permet d'effectuer l'équivalence et le change dans la vraie monnaie qui n'a pas de patrie, l'or fin au poids, dont les vertus sont universellement appréciées. C'est aussi pour cela qu'il a longtemps servi de monnaie pivot, notamment au niveau de la Banque des Règlements Internationaux. Le bitcoin apparaît plutôt méta-national qu'international puisqu'aucun État n'en a fait de version nationale, même si de nombreuses banques centrales travaillent sur des devises cryptographiques nationales[80]. Les services qu'il peut rendre sont les mêmes aux pôles et sur l'équateur, en deçà des Pyrénées et au-delà.

Après cette comparaison avec l'or, une autre explication fréquente de la valeur du bitcoin est la prise en compte de la puissance de son réseau, non pas en nombre de participants ou en volume d'échanges quotidiens, mais en puissance électrique engagée dans le maintien de l'intégrité des transactions. On est ici sur un aspect difficile à comprendre bien qu'il soit aisé à caricaturer. On va donc commencer par quelques chiffres, avant d'examiner la controverse.

Les « mineurs », pour participer au vote sur la validité de chaque bloc de transactions, doivent se livrer à de lourds calculs, comme cela a été expliqué au point II, 1. Le vote n'est valable que si le mineur résout en sus un problème qui n'a, par lui-même, aucun intérêt intrinsèque. Il fournit simplement la « preuve de travail » de chacun, clef de voûte de l'intégrité du vote. Ce travail consiste à effectuer un nombre incroyable de fonction de hashage sur les données du bloc à valider que l'on assortit d'une série alphanumérique variable, jusqu'à trouver celle qui provoque un hash commençant par un nombre requis de zéro. Autant dire à lancer une pièce en l'air des milliards de fois jusqu'à obtenir 68 fois « pile » de suite. On exprime la puissance des machines qui effectuent ces calculs en nombre d'opérations de hashage effectuées chaque seconde, et qui se compte en milliards. Une machine *ad hoc* (ce ne sont plus depuis des années des ordinateurs, mais des ASIC, c'est-à-dire des circuits imprimés conçus pour cette seule tâche) est, fin 2016, communément capable d'effectuer 4 860 milliards d'opérations de hashage par seconde. On estime que l'ensemble des mineurs effectue, jour et nuit, 1,7 milliard de milliards de ces opérations. C'est le seul chiffre « sûr ».

En se fondant sur la consommation moyenne de ces machines, on peut (toujours fin 2016) estimer à 423[81] MW la puissance électrique nécessaire. Pour fixer un ordre de grandeur, ce serait la moitié d'un réacteur nucléaire ou, pour faire moins effrayant, de l'ordre de 200 éoliennes. Cette puissance, si on multiplie les chiffres par 365 jours et par 24 heures, représente une consommation de 3,7 milliards de kilowattheures. La plupart des mineurs est aujourd'hui en Chine, où le coût de l'énergie est sans doute inférieur aux plus bas prix européens qui sont de l'ordre de 12 centimes en France et 9 en Autriche. En comptant 8 centimes, la dépense annuelle actuelle serait de 300 M€. Sans compter l'amortissement des machines. En regard, et en comptant que cela rapporte 12,5 bitcoins toutes les 10 minutes durant un an, le rapport en année pleine aurait été de l'ordre de 420 M€ sur la base d'un cours moyen 2016 de 600 euros le bitcoin, correspondant au cours au moment du *halving*.



Le coût énergétique de Bitcoin (article de Pierre Noizat)

On voit donc que les chiffres se tiennent, ou qu'il y a en tout cas un « ordre de grandeur » malgré les aléas sur le coût de l'électricité et le prix fluctuant du bitcoin. On notera qu'il est amusant dans un système apprécié des libertariens de recourir à un calcul de valeur de type marxiste équivalent à la difficulté de (la preuve de) travail fournie. Voici pour les chiffres.

On peut crier à la gabegie. On a lu que le bitcoin consommait déjà autant que l'Irlande, bientôt que le Danemark. On lit moins ce que consomment les banques : d'après Pierre Noizat[82], plus que le bitcoin pour leurs seuls guichets automatiques (c'est-à-dire pour une partie de la gestion de ce cash dont elles assurent qu'il est résiduel). On ne réfléchit pas non plus sur le coût énergétique total d'une monnaie construite sur la dette, laquelle gonfle forcément de manière infinie dans un monde fini.

Mais on peut aussi considérer que l'énergie consommée l'est pour défendre la première communauté décentralisée, la première expérience de monnaie libre, l'intégrité d'un registre qui peut devenir un bien commun de l'humanité. Au-delà, une courte réflexion sur ce qu'est la finance s'impose : en faisant des transactions, nous déplaçons de la valeur dans l'espace. En empruntant ou en épargnant, nous la déplaçons dans le temps. Qu'épargnons-nous pour « nos vieux jours » si ce n'est… l'énergie qui abonde dans l'âge adulte et fait défaut dans la vieillesse ? On connaît la définition par Dostoïevski de l'argent comme « de la liberté frappée »[83]. Bitcoin, c'est de l'énergie électrique condensée.



Contenu en énergie, contenu en calcul ?
(article de Jean-Paul Delahaye)

Or numérique, énergie capitalisée, le bitcoin n'aurait aucune valeur s'il n'avait pas d'utilité. Cette question de son utilité peut être abordée au travers d'une autre comparaison : celle du timbre-poste.

Quand on reproche au bitcoin de violer le monopole régalien sur la monnaie, on oublie qu'un autre monopole régalien est déjà passé à la trappe : celui des Postes et Communications, qui n'avait évidemment rien d'immuable. L'extravagante fortune acquise en quelques siècles par la famille allemande des Thurn-und-Taxis rappelle qu'une poste privée a déjà existé et qu'avec ou sans l'État, la Poste est toujours une puissance. Comme la Banque avec les Médicis, la Poste conduisit les Thurn-und-Taxis à deux doigts de la souveraineté. De même, en 1832, quand le système de Morse apparut, il en naquit la Western Union. Chaque mutation dans le transport d'information crée une puissance financière.

Dépassons les anecdotes historiques sur les timbres servant de monnaie d'appoint en cas de crise. Au-delà de sa « commodité », le timbre a bel et bien une valeur réelle et liquide. Le timbre est un petit billet de banque, libellé en… gramme-temps.

Celui qui aurait accumulé des timbres-poste fin 2014 avant la hausse sans surprise du 1er janvier et celui qui aurait acheté des billets de banque suisses avant la décision surprise de la BNS auraient-ils fait des plus-values différentes ?

Dans le second cas, l'euro s'est dévalorisé par rapport au franc suisse, dans le premier par rapport au gramme-temps. Sur la vignette ne figurent plus, souvent, qu'un poids et l'indication d'une vitesse. Le prix du transport d'une vingtaine de grammes à l'autre bout du monde est négocié sérieusement puisque les coûts sont

répartis sur plusieurs pays et il n'est pas excessif car les Postes ne font pas les profits des banques. Le timbre, mieux que le billet, a une « vraie valeur » : on sait précisément le service que l'on acquiert.

Si l'utilité du Bitcoin était celle d'un timbre, sa valeur serait-elle du même ordre de grandeur ? Non, car pour déposer la trace d'un titre, d'une garantie, d'une hypothèque ou la formule d'une molécule tout en disposant d'une date certaine, d'une confidentialité appréciable et d'un temps de transport de l'ordre de 10 secondes, une microparticule de bitcoin suffit. Demain, le bitcoin, monnaie programmable, pourrait servir autant à traiter de l'information qu'à échanger ou conserver de la valeur.

Les seuls humains s'envoient plus de 20 milliards d'emails réels par jour. Il y a 10 milliards d'objets connectés à ce jour, il devrait y en avoir autour de 100 en 2050[84]. Qui peut dire ce qui va se passer quand les machines, qui n'ont pas de personnalité juridique, vont entrer en transactions réciproques ? Une authentification des transactions par le calcul paraît très adaptée à leur nature.

Les 21 millions de bitcoins sont divisibles chacun en 100 millions de petits bouts. Comme il faut tout de même ajouter un pourboire à chaque transaction, on peut poser l'hypothèse qu'on ne se servira jamais de moins d'un millionième, soit 21 mille milliards d'unités disponibles (nombre proche – soit dit en passant – de celui de la base monétaire mondiale qui est évaluée à 22 mille milliards d'unités en dollars[85]) ceci pour peut-être 100 milliards d'utilisateurs (humains, transhumains et mécaniques) de 2050. Cela fait un stock théorique moyen de 210 de ces « timbres digitaux » par utilisateur. Encore faut-il soustraire du stock le nombre de bitcoin perdus, problème qui sera abordé au point III, 1[86].

Si chaque millionième de Bitcoin valait un cent, la capitalisation totale de Bitcoin serait de 210 milliards de dollars, soit environ 2 fois celle d'UPS, 4 fois celle de concurrents comme Fedex ou DHL (ou une fois la capitalisation de ces trois seules entreprises). En termes de chiffre d'affaires, 5 fois celui d'UPS ou 10 fois celui de Fedex. Bref, un prix de 10 000 $ pour ce carnet de timbres qu'est un bitcoin apparaît plausible à terme, sinon immédiatement raisonnable…

Allons plus loin : à 4 $ du millionième (soit le prix moyen d'un envoi recommandé dans le monde), chaque bitcoin vaudrait 4 M$. Les entreprises payent cependant bien plus cher encore que 4 $ pour la sécurité de leurs colis : environ 10 $ en moyenne si on divise le chiffre d'affaires d'UPS par le nombre de simples plis (25 % en nombre) et de colis transportés.

Au total, le prix du bitcoin dépendra du nombre de transactions méta-monétaires échangées en 2050 par les humains, mais aussi par les objets connectés. Cette réflexion, qui revisite la distinction entre le bitcoin devise et Bitcoin la technologie, amène à imaginer pour ce petit timbre programmable du futur une valeur plus élevée qu'aucun billet de banque. Un bon connaisseur, Wences Casares, patron de Xapo, donnait ainsi son sentiment : une chance sur 5 que le bitcoin ne vaille plus rien un jour, mais plus d'une chance sur 2 qu'il vaille un jour plus d'un million de dollars.

3- Ébauche des usages hétéroclites du bitcoin

Le bitcoin peut-il être une monnaie classique ?

Bien des critiques superficielles contre Bitcoin, de celles qu'on assène avec plus de rhétorique que de pertinence, commencent par « si tout le monde voulait s'en servir… ». Oui, si 7 milliards d'hommes voulaient se servir du seul bitcoin pour toutes leurs transactions, il y aurait pour l'instant de gros problèmes. Mais cela ne marcherait pas mieux avec le franc suisse, et cela ne prouve pas qu'il soit dénué d'utilité ni de valeur. À vrai dire, on prouverait aussi bien l'inutilité d'un ascenseur, qui peut difficilement servir à tout un immeuble à la fois.

La question n'est donc pas de savoir si Bitcoin peut servir à tout le monde à la fois, mais s'il peut, à l'occasion, rendre toute la gamme des services que l'on attend traditionnellement d'une monnaie. On va ici s'écarter de l'ordre classique d'énumération des trois fonctions aristotéliciennes[87] et poser les questions dans l'ordre suivant : sert-il à régler ses achats ou payer ses dettes ? De réserve de valeur dans le temps ? D'étalon dans les échanges ?

Bitcoin peut-il servir à régler ses achats ou à payer ses dettes ? Répondons tout de suite « oui » et puis distinguons, parce que les choses ne sont jamais binaires. Si l'on détient des bitcoins ou plus exactement si l'on détient la clef privée permettant de mouvoir des bitcoins inscrits à une adresse publique du livre, pouvons-nous nous en servir, comme des euros que nous avons en poche ou en banque, pour régler un achat ?

La réponse classique serait : oui, si la contrepartie (le commerçant, par exemple) l'accepte. Mais cette réponse qui laisse penser que le bitcoin serait une sorte de jeu « entre adultes consentants » passe à côté de la question. Bien sûr les transactions entre amis (remboursement de petites dépenses, dettes de jeux, transactions ludiques ou pédagogiques, locations de chambre ou de voiture) peuvent se faire en bitcoin et entre *geeks* ce sera le plus souvent en transférant directement les sommes via des applications en ligne ou téléphoniques. À ce stade, on est presque encore dans la « monnaie de jeu ».

Un commerçant, dans un pays donné, facture et tient ses comptes dans la monnaie légale. Mais le cours forcé signifie qu'il ne peut pas refuser ladite monnaie, non qu'il ne puisse en accepter une autre : le Marché aux Puces voit passer bien des dollars, les cafetiers à Genève acceptent volontiers l'euro et l'intégralité du Liban traite même indistinctement la livre libanaise et le dollar. Cependant le commerçant paye la TVA et comme tout un chacun diverses charges dans la monnaie légale. Le plus souvent, d'autre part, il ne possède un compte en banque que dans cette devise. Il fait donc son affaire des devises reçues, n'en conservant qu'à hauteur de ses besoins professionnels (fournisseurs ou voyages éventuels) ou personnels.



Découvrez le Cercle du Coin !

Avec le bitcoin, les choses sont légèrement différentes. Pour l'accepter, le commerçant doit être équipé d'une application sur son téléphone, sa tablette ou l'écran de sa caisse et doit en outre être éduqué : il affiche alors un autocollant « Nous acceptons le bitcoin » qui va attirer l'œil des *bitcoineurs*. Ceux-ci connaissent souvent d'avance l'adresse, car des sites comme « bitcoin.fr » recensent ces commerçants. Ici, on est dans une démarche communautaire. Souvent le commerçant est un *bitcoineur*, ou du moins manifeste une sympathie de principe pour les idéaux anti-autoritaires de la communauté. On trouve donc bien des commerces informatiques (matériel, sécurité, création de sites, hébergement et assistance) ou de jeux vidéo, mais aussi des restaurants ou des boutiques ciblant les jeunes technos. C'est le cas du Sof's Bar de la rue Saint-Sauveur à Paris, qui abrite divers *meetups* et le siège social du « Cercle du Coin » et de presque tous les commerçants du Passage du Grand-Cerf[88]

dans le quartier Montorgueil. Bien sûr, le commerçant paye la TVA et d'autres dépenses en euros, mais il peut (à titre personnel ou comme un compte en devises) conserver une part des bitcoins reçus.

Le phénomène étant plus développé sur Internet, davantage de sites proposent de payer en bitcoin. Très militants au début, comme les sites de dons en ligne ou Wikileaks, ils sont de plus en plus dans une logique d'expérimentation d'une offre alternative. Le petit logo ₿ y figure sans commentaire à côté de ceux de Visa ou de PayPal. Des sites vedettes, comme celui de Dell, Overstock ou Microsoft, ou des opérateurs de services de transport à participation publique, comme Transdev ou Expedia, acceptent le bitcoin. Il est fort probable que leur processeur de paiement fasse l'opération de change instantanément.

Plusieurs « militants » ont tenté – et réussi – des tours du monde en bitcoin. Encore une fois, la dimension communautaire est importante dans cette démarche, son objectif étant d'échanger des idées autant que des marchandises ou des services.

Au-delà de ce paiement en bitcoin « affiché », il est en possible de payer pratiquement partout avec une carte portant le logo Visa ou MasterCard et sur laquelle le porteur ne détient en réalité que des bitcoins. L'exemple le plus connu est la carte Xapo. Son porteur possède une adresse bitcoin, par laquelle la carte peut être rechargée. En se connectant sur le site de Xapo, il peut suivre son « compte » qui n'est qu'en bitcoin. À l'instant où il fait usage de sa carte, partout dans le monde, pour retirer de l'argent dans un DAB ou régler un commerçant, la banque prestataire de Xapo crédite le bénéficiaire en devise légale et débite le porteur de la contre-valeur en bitcoin. On peut donc payer en bitcoin partout où le bitcoin n'est pas accepté, et dans une discrétion totale. Certaines permettent même l'inscription d'un pseudonyme sur la carte, tout en vérifiant strictement l'identité du porteur, ce qui nous ramène à la distinction de ce qui doit être secret et de ce qui doit rester discret : si le commerçant est payé, quel besoin a-t-il de connaître le nom de la demoiselle qui le paye ?

Ainsi est-il raisonnable de répondre « oui » à la première question : le bitcoin peut effectivement servir, directement ou indirectement, d'instrument d'échange pour régler ses achats. Il le fait déjà ! Le cas des dettes est moins clair, car aucun établissement de crédit ne consent aujourd'hui de dettes en bitcoin, et ceci nous renvoie à sa nature de monnaie-valeur, par opposition à la monnaie-dette créée *ex nihilo* par les établissements de crédit. Mais il faut noter que le *peer-to-peer lending* existe avec le site BTCJam par exemple, qui a effectué plus de 18 millions de dollars de prêts en Bitcoin depuis 2012. Enfin, le bitcoin ne permet pas de régler directement ses impôts, mais ceci est une autre histoire sur laquelle on s'est déjà penché au point I, 3.

Par rapport aux qualités qu'Aristote pouvait attendre d'un moyen de paiement, il faut ajouter deux facultés : la divisibilité et la fluidité.

Le bitcoin est plus divisible que toute autre devise. La divisibilité (qui manque au diamant) est essentielle pour faciliter l'échange de la marchandise contre le signe monétaire. La langue française possède une étonnante expression, qui souligne l'importance de cette qualité de divisibilité : « faire la monnaie » qui veut dire rendre la différence entre un paiement par excès et la valeur du bien.

Sa fluidité est sans égale. Par rapport aux premiers transports de numéraire, la première révolution fut la lettre de change. Malgré de notables progrès du système bancaire international (SWIFT, SEPA, TARGET, etc.) il n'offre pas aux utilisateurs bancaires et non bancaires de système de transfert aussi rapide, sûr et peu coûteux que Bitcoin. Est-il normal qu'un virement bancaire puisse prendre plus de deux jours au XXI^{e} siècle, quand aucun transfert physique de fonds n'a véritablement lieu ?

Seconde question : le bitcoin sert-il à conserver de la valeur dans le temps ? On vient d'examiner sa capacité à transporter de la valeur dans l'espace, que le bénéficiaire soit à portée de main ou à l'autre bout du monde. La seconde question concerne le transport dans le temps. Au total, la finance ne ressort jamais que de combinaisons de ces deux transports.

Avec la notion d'intérêt sur l'argent sont apparues celles de capitalisation (un euro capitalisé à 2 % par an double en 35 ans) et d'actualisation (un euro dans 35 ans, actualisé à 2 %, ne vaut que 50 centimes aujourd'hui). Pour l'euro, monnaie sans valeur intrinsèque, la conservation de sa valeur repose, pour faire outrageusement simple, sur le pari qu'une baguette de pain qui vaut un euro aujourd'hui en vaudra sagement 2 dans 35 ans : l'argent placé en banque et justement rémunéré – les taux d'intérêts ne sont pas fixés au hasard – doit conserver sa valeur, c'est à dire *in fine* son pouvoir d'achat. Ce qui est à peu près le cas quand tout va bien. Il est pourtant rare que tout aille bien toute une vie…

En va-t-il différemment d'une monnaie-valeur ? De nouveau, il nous faut regarder ce qu'il en fut durant des

siècles avec l'or. Répétons ce qui a déjà été dit : l'or n'est pas inaltérable parce qu'un napoléon d'or vaudrait à coup sûr dans un siècle son prix aujourd'hui, ni même parce qu'il permettrait d'acheter le même poids de pain, mais parce qu'il pèsera toujours 6,45 grammes à 900‰, sans évaporation, pourrissement ou oxydation. Pour autant, sur le temps long un petit bout d'or conserve mieux sa valeur qu'un petit morceau de papier représentant une confiance énorme dans le gouvernement. Les plus anciens se souviennent des récits de leurs grands-parents sur ce que devinrent les billets remis aux patriotes qui versèrent leur or en 1914. Mais Voltaire disait déjà qu'« une monnaie papier, basée sur la seule confiance dans le gouvernement qui l'imprime, finit toujours par retourner à sa valeur intrinsèque, c'est à dire zéro »[89].

Si l'or conserve sa valeur, il ne le doit pas à sa seule inaltérabilité, mais aussi à sa rareté. La preuve du contraire fut administrée quand il cessa soudain d'être rare, avec l'afflux d'or des Amériques, provoquant un « renchérissement » des biens.

Le bitcoin, rare et inaltérable (en l'état de nos connaissances au bout des huit premières années de l'expérience), semble raisonnablement destiné à conserver sa valeur. Du moins à moyen et long terme. L'expérience de l'année 2014 (un cours divisé par 5), même si elle n'est pas inédite dans l'histoire de la monnaie, fait encore planer une ombre sur le bitcoin.

Naturellement, ceux qui en achètent, et pour certains en accumulent, font le pari que, bien loin d'une simple conservation de sa valeur, il va connaître une importante hausse. À la racine de cette conviction on trouve une défiance proche de celle de Voltaire pour la monnaie papier, un peu d'effroi devant l'emballement de la politique de création monétaire dans les programmes de *Quantitative Easing*, une forme de « survivalisme » monétaire, mais aussi la foi dans le développement des usages de Bitcoin dans un monde où les échanges décentralisés vont s'imposer comme la technologie la plus sûre, la plus respectable et la plus efficace en matière de transferts et d'enregistrements divers.

Il est, pour finir sur ce point, assez risible de lire, chez les détracteurs du bitcoin, qu'il ne vaut ou ne vaudra plus rien un jour par ce qu'il ne « repose » sur rien, qu'il est horriblement déflationniste et destiné, s'il s'imposait, à connaître une appréciation inéluctable. Ils prouvent que, si l'on peut penser une chose excessive on peut aussi en penser deux à la fois, et contradictoires.

Le bitcoin peut-il servir d'unité de compte, d'étalon de la valeur ? Nous avons gardé pour la fin cette troisième question, pourtant souvent présentée en premier. Une monnaie doit pouvoir servir d'unité de compte.

En plaçant en premier attribut de la monnaie cette fonction-là, on rend hommage à Aristote et à son *Ethique à Nicomaque*[90], dont Keynes lui-même écrivait : « on n'a jamais parlé de si bon sens – avant ou après ». Or Aristote, qui aborde la monnaie à propos d'une dissertation sur la justice, au chapitre de la justice réciproque, écrit exactement que « par l'effet d'une convention toute volontaire, la monnaie est devenue en quelque sorte l'instrument et le signe du besoin ». La monnaie « rend les choses commensurables entre elles et les amène ainsi à l'égalité ». Il met ainsi d'abord l'accent sur les fonctions unité de compte, puis, pour que la justice implicite dans la transaction se maintienne dans le temps, sur la fonction de réserve de valeur : le petit jeton portant le symbole de telle ou telle cité est ensuite l'effet d'une convention.

Pourquoi, alors, avons-nous suivi l'ordre inverse ? D'abord parce que, dans la pratique, le récit qui commence par la fonction d'étalon est toujours celui, si naturel aux penseurs libéraux qu'il n'est souvent même plus discuté, du troc initial dans le village préhistorique auquel « on » aurait mis fin astucieusement par l'instauration de la monnaie. Qu'aucun historien, ni aucun explorateur, n'ait jamais trouvé de place de marché primitive où l'on échangerait concrètement un mammouth contre des antilopes n'affecte point les tenants de ce récit. On se souviendra cependant que l'écriture comptable fondée sur la dette de biens est la première trace de monnaie dont nous disposons grâce aux tablettes sumériennes ou aux papyrus. Mais l'enjeu est ailleurs : en posant qu'a priori l'être humain échange, naturellement, voire toute la journée, et ceci sans État, sur un marché qui serait une donnée de nature, on voit trop bien quelles fins politiques on poursuit. Aristote est beaucoup plus nuancé[91].

Au sujet du bitcoin on ne peut suivre le chemin imaginé pour l'invention de « la » monnaie : il s'agit de l'invention d'une « nouvelle » monnaie. Or, depuis que Bonaparte créa le franc Germinal, chaque monnaie nouvelle a été établie, en France, en référence à la précédente. Si l'on se souvient que le franc Germinal était pour ainsi dire un sous-produit du système métrique, on comprend qu'il ne faut pas moins qu'une révolution et un homme providentiel pour instaurer un nouvel étalon. Ensuite, l'habitude fait son œuvre. Comme le notait un célèbre

pamphlet contre l'affairisme d'État, « on s'habitue peu à peu à regarder avec des yeux plus doux les traits qui sont partout imprimés sur le signe matériel de nos jouissances »[92].

Dans la seconde partie du siècle dernier, les plus jeunes s'étonnaient de la persistance chez leurs parents de l'étalonnage en « anciens francs » : les ainés répondaient en riant que leurs propres parents comptaient bien en sous ! Mais le plus étonnant est que tout ce petit monde comptait en franc (ancien ou nouveau) alors que l'inflation mesurée par l'Insee, jamais réellement contenue après le plan Pinay et le nouveau franc (1er janvier 1960), repartit de plus belle, refranchit la barre des 5 % après mai 1968 et celle des 10 % après la guerre de Kippour, pour se maintenir entre 9 et 13 % durant dix ans. En 15 ans la valeur de ce franc que l'on évoquait chaque jour (l'ancien et le nouveau !) fut en fait divisée par 4. Certes les salaires augmentaient, la petite bourgeoisie remboursait ses crédits immobiliers en monnaie de singe[93], les historiens et les économistes s'arrangeaient avec des tables de conversion et le prix du pain. Mais qui étalonnait quoi ?

On oublie souvent que le franc-or (0,29 gramme de fin), qui avait servi de référence à l'expérience de l'Union latine de 1865 à 1927, servit de monnaie de compte à la Banque des Règlements Internationaux (à Berne) jusqu'au début du XXIe siècle. Qu'est-ce que cela signifie ? Qu'il y a étalon et étalon…

Ce rappel était nécessaire pour risquer l'hypothèse selon laquelle le bitcoin ne jouera pas de sitôt le rôle d'étalon dans la vie quotidienne et dans les rues commerçantes. Non pas qu'une rue commerçante ne puisse pratiquer le double affichage, comme ce fut le cas, par exemple, en Israël dans les années d'hyperinflation (1984-1985, mais les prix restèrent doublement affichés et dans la pratique calculés en dollars durant des années), mais parce que trop d'obstacles s'y opposent : l'habitude, que l'on vient de souligner, le paiement de la TVA et des charges en monnaie légale, la volatilité relative (jusqu'ici) du bitcoin, la taille trop limitée de la communauté de ses utilisateurs…

Cependant il faut nuancer ce constat et le contextualiser historiquement. Que le bitcoin ne serve pas d'étalon dans la rue ne le prive pas de cet attribut ailleurs. Le bitcoin a réellement servi d'étalon dans plusieurs opérations spécifiques. La première semble avoir été, durant l'été 2014, le financement par la communauté (*crowdfunding*) du développement du projet Ethereum, une plateforme décentralisée présentée comme une sorte de « bitcoin 2.0 ». L'unité de compte de cette nouvelle blockchain, l'ether, fut mis en vente au prix de 2000 ethers pour un bitcoin, sans aucune référence au dollar ou à l'euro, et ceci l'année même du plongeon de bitcoin qui avait perdu la moitié de sa valeur depuis le 1er janvier quand débuta l'opération, et devait en perdre encore autant ensuite avant d'entamer sa longue remontée.

La levée de fonds d'Ethereum connut un succès appréciable : 31.591 bitcoins, ce qui représentait à ce moment 18 millions de dollars. Voilà un montant dont bien des banquiers d'affaires s'honoreraient, en communiquant sur leur rôle de monteur, facilitateur ou conseil. Or cette levée de fonds s'est réalisée de manière dérégulée, méta-nationale et interne au cyberespace. De manière décentralisée, en somme.

Depuis lors, d'autres opérations ont été menées, soit en bitcoin soit en ether, pour financer de nouveaux projets sur la base de l'une ou l'autre blockchain. Les sommes en jeu sont désormais loin d'être négligeables. Plus l'économie fonctionnant sur une blockchain se développera (et tout le monde assure qu'elle se développera, même si le monde de la finance régulée s'efforce de le faire sur des blockchains fermées ou consortiales, sans référence au bitcoin) plus des levées de fonds décentralisées se feront en monnaie décentralisée.



Et si vous en achetiez un petit peu ? (expérience)

Enfin il y existe un second indice du rôle d'étalon qu'acquièrent le bitcoin et l'ether. Même si cela ne concerne que le petit monde marginal des traders, ceux qui arbitrent ether contre bitcoin ou achètent et vendent les divers crypto-jetons (que nous examinerons au point III, 2) comptent en bitcoin, ce qui tend d'ailleurs à rendre

leur conversation un peu hermétique aux tiers. Les plateformes d'échange proposent toutes l'option d'affichage des cours en bitcoin, comme on pourrait le faire classiquement en dollar ou en euro.

Si le bitcoin sert de monnaie de réserve, de monnaie pivot du cyberespace, il y servira aussi d'étalon. C'est d'ailleurs le cas sur toutes les plateformes d'échanges spécialisées qui acceptent une multitude de cryptomonnaies. Plusieurs n'acceptent aucune monnaie légale, leurs pairs de trading (par exemple BTC/ETH bitcoin contre ether) étant quasiment toutes fondées sur le bitcoin.

Muni, à des degrés divers, des trois attributs de la monnaie, Bitcoin est une « vraie monnaie », pas une « monnaie pour jouer » comme celle du Monopoly. Reste à savoir dans quels usages elle pourrait s'imposer.

Une monnaie accessible, adaptable et programmable

Nous venons d'examiner les attributs canoniques d'une monnaie classique, et de voir que le bitcoin les possédait tous, jusqu'à un certain point. En rester là, ce serait penser que cette merveille technologique n'a pourtant pas un statut monétaire dépassant celui, un peu étriqué, des petites « monnaies locales complémentaires ». Or celles-ci (que l'on rencontre souvent dans la littérature sur le bitcoin, que ce soit pour les confondre ou pour affirmer leur supériorité morale) n'ont évidemment aucune fonction d'étalonnage puisqu'elles sont strictement liées à l'euro, et ne peuvent pas conserver leur valeur dans le temps pour la double raison qu'elles sont généralement conçues pour être « fondantes », c'est-à-dire pour perdre progressivement leur valeur et inciter à la consommation locale, et que nombre de ces monnaies finissent, avec ou sans fonte, par sombrer dans l'oubli.

Dire ce que le bitcoin a « de plus » que les devises légales en termes de fonctionnalités, ce sera aussi souligner ce que celles-ci ont, parfois, « de moins ».

Le bitcoin est une monnaie accessible qui est adaptée à la *remittance*. Le bitcoin est, d'abord, une monnaie accessible. Cette assertion peut surprendre, tant le néophyte risque d'éprouver un rien d'effroi quand il décide de se lancer dans l'aventure, d'acheter ses premiers morceaux de bitcoin ou de s'en servir. Il y a certes une barrière technologique pour celui qui n'a pas (ou ne sait pas qu'il a déjà sur son mobile) un lecteur de QR Code, un « second facteur d'authentification », un compte sur l'Appstore d'Apple ou sur le Google Play Store dont il n'aurait pas égaré le mot de passe, etc.

Mais cette perception de la difficulté doit être nuancée et elle est souvent un marqueur d'âge ou de classe sociale. Nombre d'orateurs qui expliquent de manière hautaine que le bitcoin ne peut pas fonctionner « dans la vraie vie » en disent plus sur leur vie que sur la technologie. C'est le cas de celui qui s'était illustré en devant confesser, après son réquisitoire, qu'il n'avait jamais réussi à télécharger un portefeuille. On peut faire la comparaison avec Skype qui a séduit les *geeks* mais aussi les travailleurs émigrés. Pour le dire plus crûment : bien des bourgeoises parisiennes ne l'ont découvert qu'après les nounous philippines qui gardent les enfants des autres toute la journée et ne voient les leurs que le soir et sur écran [94].

En outre, les gens qui font l'opinion, dans nos sociétés, n'ont pas de difficultés pour ouvrir un compte. Mais c'est loin d'être le cas de tout le monde : il faut tout de même généralement avoir un justificatif de domicile ou d'autres pièces justificatives, ce que n'ont pas forcément des personnes en situation précaire. Il en va de même pour les « délits de faciès » bancaires : rien n'oblige une banque à accepter de recevoir une personne qu'elle ne souhaite pas voir, et beaucoup ignorent leurs droits bancaires ou n'ont tout simplement pas le temps de faire une démarche. Si l'on en croit les chiffres, il y aurait tout de même plus de 1 % de non-bancarisés en France [95], soit l'équivalent de la ville du Marseille. Passons… Ils auraient été 10 millions aux USA en fin 2010 [96]. À l'échelle de la planète, le chiffre des *unbanked* est difficile à établir. Il aurait été à la même époque de 2,5 milliards d'après une étude de Mc Kinsey.



Un petit reportage datant du printemps 2014 et disponible sur Youtube[97] (*Bitcoin in Uganda*) raconte comment un américain de Brookline, Massachusetts, lassé de perdre deux jours et bien plus de 10 % sur ce que sa femme Ronah et lui-même envoyaient à Ronald, son beau-frère, jeune étudiant en comptabilité en Ouganda, a acheté ses premiers bouts de bitcoin et comment Ronald s'en est fort bien débrouillé à Kampala pour les échanger contre les shillings locaux. D'autant qu'en Ouganda un téléphone mobile coûte beaucoup moins cher à l'année qu'un compte en banque.

Il faut faire un effort pour comprendre ce dernier point, qui peut changer la perception que les uns ou les autres ont sur la chose : dans de nombreux pays émergents, où le téléphone mobile est roi, ouvrir un compte en banque est beaucoup plus difficile que de télécharger une application supplémentaire. N'oublions jamais que nous avons plus d'efforts à fournir pour nous tourner vers des alternatives, telles que bitcoin, dans nos sociétés où tous les services bancaires et financiers fonctionnent « suffisamment » bien pour que l'on ne se pose pas trop de questions. À cet égard, certains ont vu, dans ce que l'on appelle en anglais la *remittance*, c'est-à-dire le transfert et la remise en main de fonds, l'eldorado du bitcoin.

Les grandes sociétés spécialisées (du type Western Union, qui dans certains cas entretient des quasi-monopoles, notamment via des partenariats avec la Poste, ou MoneyGram) communiquent peu sur le taux de chargement, préférant afficher largement des photos d'enfants « du monde » tout sourire parce qu'ils ont reçu l'argent de leurs parents. Le rapport du produit brut sur le volume d'activité, quand il apparaît, semble encore s'établir souvent au-dessus de 10 %, mais rien n'interdit de penser qu'il est noyé dans de « gros mouvements » faiblement chargés. Même si la concurrence commence à jouer, et malgré les remontrances du G8 lors du sommet de l'Aquila, le taux de chargement demeure très élevé sur les « petits montants » ou sur certaines destinations.

La nature des flux[98] varie fortement. Les principaux pays « receveurs » sont ainsi l'Inde, la Chine, les Philippines, le Mexique, le Nigeria, l'Egypte, le Pakistan et le Bangladesh, mais on y trouve aussi la France (en 4^{e} position, avec près de 25 milliards reçus contre plus de 70 pour l'Inde et de 60 pour la Chine). Les principaux pays « envoyeurs » sont les USA, devant la Russie, l'Arabie saoudite ou la Suisse. Autant dire que chaque flux s'explique par une situation particulière : présence d'une communauté dont les pratiques suivent des circuits officiels (et traçables) ou bien se fondent sur le bouche-à-oreille et des solutions informelles, présence de travailleurs immigrés ou d'étudiants étrangers appartenant à la classe moyenne (flux inversé), etc.

Dans de nombreux pays, le flux d'argent représente plus de 15 % du PNB. Au niveau mondial, le volume global a explosé depuis le début du siècle et dépasse actuellement les 430 milliards de dollars.

Le bitcoin n'est évidemment pas le seul moyen de contournement : depuis les procédés informels jusqu'aux solutions offertes par certains nouveaux entrants, notamment du côté des sociétés de téléphonie mobile, la gamme s'étoffe. Cependant, avec un temps de transfert de quelques secondes et un coût qui se mesure au troisième chiffre après la virgule, il offre de puissants attraits. En ajoutant à cela une sécurité hors-pair.

On le constate au regard du public qui vient acheter, pour quelques billets de banque glissés dans des « BTM » (Bitcoin Teller Machine), des fractions de bitcoin envoyées sur une adresse dont quelqu'un, au pays, doit posséder la clef. Sans doute tous les billets glissés dans la machine n'ont-ils pas été gagnés dans les formes requises. Mais faut-il, en matière de fraude, systématiquement regarder la paille avant la poutre ? Western Union se montre-t-il trop soupçonneux sur les quantités de cash qu'il fait transiter chaque année ?

Au reste, l'argent des émigrés n'est pas le seul qui peut transiter ainsi. Qui n'a pas connu l'angoisse d'avoir à transférer de toute urgence une somme dans un pays inconnu parce qu'un enfant ou un parent s'y trouve en difficulté ? Si le voyageur possède une simple carte de paiement prépayée, affichant le logo Visa et rechargeable en bitcoin, de type Xapo, on peut lui porter secours en quelques secondes, qu'il soit au milieu du désert, sur le toit du monde ou sur un navire en mer, un dimanche d'août. Quelle banque fait cela ?

Et quelle banque gère les flux de piécettes, les fameuses pièces jaunes qui firent le succès de Madame Chirac, aussi efficacement que la blockchain ? Le bitcoin peut s'avérer la monnaie idéale des tout petits paiements : un QR code à montrer devant l'œil de son ordinateur, un « bouton » sur lequel on clique, et une toute petite somme peut être envoyée pour une donation, pour payer une page de journal, ou par exemple payer le droit de ne pas voir l'écran de pub… le tout de manière fluide, sans avoir à sortir sa carte de crédit, subir les lourdes procédures de

sécurité des banques (exemples : le SMS qu'il faut attendre et dont on doit reproduire le code reçu sur l'ordinateur, ou le code que l'on obtient avec la petite machine Sésame qu'il faut avoir toujours près de soi, etc.).

Tant et si bien que les banques elles-mêmes regardent la chose avec intérêt, notamment pour la copier, tout en butant sur une difficulté qui devrait sauter aux yeux : on ne peut vraiment transférer ainsi que l'unité de compte de la blockchain, quelle qu'elle soit, et pas des « vrais » euros ou dollars. On y reviendra au point III, 3.

Ainsi, le bitcoin, monnaie adaptable, pourrait convenir aux pays émergents ou en crise. Sa capacité à transporter sa propre valeur presqu'instantanément et presque gratuitement ne suffirait peut-être pas à établir un écosystème si sa détention n'avait aucun intérêt. Il est entendu qu'on peut le changer après l'avoir reçu, comme celui qui l'a envoyé a changé sa monnaie légale contre du bitcoin. Ce change lui-même, dans un sens ou dans l'autre, n'est pas très onéreux – beaucoup moins que le change manuel d'espèces ou que le change en banque – mais il introduit de nouvelles barrières.

Celui qui reçoit du bitcoin peut le changer en cash (localement, dans une boutique plus ou moins formelle) ou sur une plateforme, ce qui revient à ouvrir un compte ailleurs… une solution qui n'est pas forcément à la mesure de ceux qui ont déjà du mal à avoir un compte dans leur propre lieu de résidence.

On a du mal à chiffrer les choses. Mais il est probable que certains, en bout de chaîne dans le pays receveur, gardent le bitcoin, et pas seulement parce qu'ils spéculent sur sa hausse.

Dans bien des pays émergents, le fait de détenir des bitcoins peut faciliter la création d'une (petite) entreprise : celle-ci peut agir, s'installer et surtout facturer des clients (locaux ou lointains, par exemple sur Internet) pratiquement dès le premier jour.

Dans bien des pays où la stabilité des grandes devises est inconnue, le bitcoin offre une réserve dont la volatilité (décroissante) apparaît tolérable. Le fait de détenir des bitcoins y sécurise l'argent gagné, proie souvent trop facile d'un gouvernement prédateur et de ses agents corrompus et violents, mais aussi d'un banditisme endémique qu'entretient une économie reposant entièrement (notamment loin des centres urbains) sur la circulation de billets de banque.

Enfin, là où des gouvernements impuissants élèvent des barrières, le bitcoin perce les murs, pour lui comme pour ses porteurs qui n'ont « rien à déclarer » lorsqu'ils s'en vont.

Le bitcoin constitue ainsi une monnaie complémentaire évidente pour de nombreux pays émergents, mais aussi pour ceux qui sont menacés par diverses formes de crises. L'hyperinflation et le manque physique de monnaie fiduciaire ont pavé la route du bitcoin en Argentine, ce pays qui porte pourtant le nom de l'argent ! Le bitcoin a sa place dans le kit de survie financière là où les frontières se ferment ou pourraient se fermer, là où la « résolution » des spéculations financières des banques se fait avec l'argent de leurs clients, là où les billets de banque peuvent être démonétisées dans la nuit.

Peut-on sauter un pas de plus, et faire du bitcoin la monnaie des « non-bancarisés » ? Cela passera par deux évolutions fortes, toutes deux en marche d'ailleurs : des solutions de plus en plus pratiques et simples, accessibles aux gens les moins habiles techniquement, et un nombre suffisant de commerces acceptant directement le bitcoin. Il semble y en avoir sensiblement plus, et c'est un signe, à Buenos Aires qu'à Paris. La seule question pourrait être de savoir quand cela arrivera, entre 10 et 25 ans. Cela pourrait aller aussi vite que la dernière révolution qu'est Internet en ce sens que c'est la seule infrastructure complexe nécessaire. Pas besoin de câbles ou de services supplémentaires, tout est « presque » déjà là.

Le bitcoin est enfin une monnaie programmable, ce qui en fait un instrument pour le micro-don, le *crowdfunding* ou le *crowdlending*. En attendant l'Internet des objets (qui sera évoqué au point suivant), le bitcoin s'avère déjà être une monnaie qui, parce que programmable, peut servir, mieux que les monnaies classiques, de moyen de paiement dans certaines opérations.

Entendons-nous d'abord sur ce que « programmable » signifie ici, avec quelques exemples, qui vont déjà bien au-delà de ce que permettent les applications de paiement offertes par les banques. Un paiement simple consiste à envoyer du bitcoin d'une adresse (celle du payeur) à une autre (celle du bénéficiaire). Mais des opérations plus complexes peuvent être ordonnées. D'abord, le bitcoin peut être envoyé sur des adresses à plusieurs titulaires, ce qui permet bien des choses, y compris d'en faire une monnaie affectée. Ainsi, des aides médicales pourraient être

envoyées au compte d'un bénéficiaire sur une adresse où les transactions suivantes devraient être signées par lui-même et par son pharmacien.

Le bitcoin peut être envoyé à une adresse où il resterait bloqué jusqu'à une certaine date (ou un certain événement). Par ce procédé, le *timelock*, il devient impossible de débloquer les bitcoins par aucun moyen tant que la condition temporelle n'est pas effectuée.

Le bitcoin peut être transféré automatiquement à l'adresse (d'un héritier, par exemple) si le compte où il se trouve n'a pas été modifié durant un an. Le transfert (paiement) peut être automatiquement lié à un achat : ainsi le prix d'un plat ou d'une consommation peut être débité dès qu'est passé l'ordre au restaurant en flashant le QR code du plat désiré.

Mais le caractère « programmable » du bitcoin dépasse largement ces commodités. La technologie ou le protocole qui fait circuler la propriété des unités de bitcoin sur sa blockchain permet, comme on l'a dit, d'éliminer les intermédiaires, ou du moins de les réduire, au premier rang desquels les plateformes assurant des services de paiement. Alors on peut imaginer que des investisseurs ou des prêteurs envoient directement leur argent au porteur de projet de façon sécurisée, par l'intermédiaire de la blockchain, en utilisant le bitcoin. Les tiers de confiance ne disparaissent pas pour autant, il en faudra toujours pour certaines situations, c'est en revanche leur libéralisation.

Encore au-delà, on pourra aussi utiliser ce qu'on appelle les « contrats intelligents », sur lesquels on reviendra au point III, 2, à savoir des petits objets numériques incorporant une ou plusieurs lignes de code pour mettre en œuvre des commandes du genre « si ceci… alors cela ». Ces contrats intelligents peuvent être intégrés directement sur les jetons de certaines blockchains, comme Ethereum, mais ils peuvent aussi être proprement greffés avec une gamme d'événements plus réduite sur les jetons de bitcoin pour profiter de la robustesse et de la taille de cette blockchain. Avec ces contrats, on peut imaginer réaliser les « contrats de prêt » (*crowdlending*) mais aussi numériser les bons de souscriptions (*crowdfunding*) et ainsi en créer de véritables actifs numériques sécurisés (*digital assets*).

Là où les banquiers classiques parlent d'IPO (*Initial Public Offering*) pour désigner les introductions d'une valeur en bourse, comme cela se fait depuis des décennies, on voit apparaître en parallèle une cryptosphère où se réalisent des ICO (*Initial Coins Offering*) : on achète directement en bitcoin les jetons des nouvelles organisations, qui ne sont d'ailleurs pas forcément des sociétés, mais peuvent elles-mêmes être décentralisées.

Ces actifs numérisés, crypto-actions ou crypto-obligations, sont facilement transférables à un tiers de manière sécurisée et à un coût négligeable… la blockchain permettra donc aussi de créer des marchés secondaires. On peut y voir une application très claire pour les sociétés de *crowfunding* qui font rentrer leurs clients au capital des sociétés. Ils pourront ainsi céder très facilement leurs parts sur des marchés libres ou régulés.

Finalement, le bitcoin a ouvert la voie à une technologie qui permet d'automatiser les deux principales missions d'une plateforme de financement participatif. Certaines banques ont vu le risque et prétendent implanter de petites blockchains privées pour gérer « leur » plateforme de *crowdfunding*. Mais la façon dont la banque gère ses propres *process* a-t-elle la moindre importance quand la même technologie permet de s'en passer ?

Le bitcoin, cash numérique fluide, accessible, adaptable, programmable… est-il la première méta-monnaie ou, pour parler comme Hegel, « la monnaie de la sortie de la monnaie » bancaire ?

La première véritable « méta-monnaie »

Nos amis philosophes de la Grèce antique ont forgé des concepts fort commodes, notamment celui de la métaphysique. Celle-ci permet de bien définir ce qui est « au-delà du réel », bien que le terme ait été avant tout la dénomination utilisée par Aristote lui-même pour désigner tout simplement ses ouvrages écrits après *La Physique*. En effet, le préfixe *méta* en grec ancien peut autant servir à désigner « après » (dans l'idée de succession) que, et c'est ce que les platoniciens des ères suivantes ont choisi, « au-delà ». D'où l'idée de métaphysique au-delà de la nature, au-delà du réel.

Il est fascinant de constater que Bitcoin épouse les deux sens. Alors pourquoi se priver de cette appellation qui le détermine si bien ? Elle a la particularité d'axer les aspects novateurs de Bitcoin sur ses particularités philosophiques, sociologiques et techniques, mais aussi sur ses utilités, contrairement au néologisme « cryptomonnaie » qui révèle uniquement ses aspects discrets et cryptographiques, ou au terme de monnaie « décentralisée » qui ne fait ressortir que son architecture de réseau.

Le terme de méta-monnaie n'explicite pas ces termes, mais il a l'avantage de les contenir tous et il nous semble tout de même moins effrayant, peut-être, que les autres pour qui serait confronté par hasard à ce concept. Nous allons donc passer en revue les caractères de cette méta-monnaie et ce que cela inclut. C'est l'occasion d'effectuer une synthèse de ce que le lecteur aura pu croiser tout au long de ce livre pour ceux qui le liraient dans l'ordre, et de découvrir un grand nombre de particularités d'un coup pour ceux qui commencent par ce chapitre.

Comme nous l'avons vu, Bitcoin est une monnaie « d'après » d'un point de vue philosophique ou sociologique. On entend parfois parler du monde de l'après-monnaie ou du monde sans-monnaie. Cela nous semble un peu illusoire. Les hommes ont toujours eu et auront surement toujours à échanger des biens et des services, et la monnaie est tout de même d'une commodité sans pareille pour cela.

Bitcoin s'inscrit davantage dans ce que l'on peut imaginer quand on parle de post-démocratie. Celle-ci n'évoque nullement la fin de la démocratie mais au contraire une démocratie augmentée, *liquide* et non plus représentative, notion parfois contradictoire avec l'idée même de démocratie au sens étymologique. Le Bitcoin est une méta-monnaie car c'est la monnaie d'après la monnaie comme nous l'avons toujours connue. Elle est toujours une monnaie, mais elle appelle un changement paradigmatique de l'idée de monnaie.

Tout d'abord parce qu'elle n'est pas été émise par un souverain placé en surplomb et qu'elle est donc horizontale et décentralisée. Ensuite parce qu'elle est en adéquation parfaite avec notre monde actuel qui est avant tout numérique. De ce fait, elle embrasse les attributs du numérique avec sa rapidité et son universalité.

Bien sûr les auteurs de ce livre pourront être taxés de progressisme, mais ils préfèrent penser que la technique représente tout de même une chance pour l'humanité. Comme Kant rêvant à sa Société des Nations[99], qui ne naîtra que plus tard et bien imparfaite…

Penser constitue déjà la première étape de tout changement. Et Bitcoin permet de penser une monnaie mondiale et fonctionnelle, non émise par un monopole régalien. Il ne s'agit pas d'une pensée volage ou arbitraire ; la technique nous montre chaque jour que cela fonctionne. Même s'il est toujours utile de rappeler que Bitcoin est avant tout une expérience : une expérience avec une forte valeur (autour de 15 milliards de dollars) et partagée par des centaines de milliers de personnes, mais une expérience tout de même. Et ce malgré toutes les mises à jour effectuées depuis la naissance de Bitcoin et tout l'écosystème autour de lui, qui tendent à le faire sortir du cadre expérimental.

Mais, après toutes ces réserves et précautions, nous restons certains qu'il est bon de faire l'expérience de Bitcoin. C'est la seule façon de ressentir vraiment sa nature méta-monétaire.

Déjà, ne serait-ce que pour le geste, le signe, nous sommes dépassés. Bitcoin n'a encore que très peu de symboles. Garderons-nous les gestes de la main que nous faisons pour désigner l'argent quand il s'agira de Bitcoin ? Sans pièce, sans billet rien ne sert de frotter son pouce contre son index. Que deviendra le cliquetis de l'intro de la chanson *Money* des Pink Floyd ? Ce sont là des indices de la rupture symbolique que Bitcoin accomplit avec une forme classique de monnaie.



Bitcoin et les symboles (conférence filmée, par Adli Takkal Bataille)

Et puis le bitcoin est aussi un savant mélange entre le cash et la carte de crédit. Il est à la fois électronique comme la carte bancaire (qui rassure aisément par son caractère physique et tangible, mais dont on ne peut oublier qu'elle est un instrument de monnaie numérique) et discret comme le liquide. Encore une fois cet état de fait semble dépasser la monnaie telle que nous la connaissons, grâce à la force unificatrice qu'est Bitcoin, qui essaye de garder le meilleur de chacun de nos moyens de paiement dans le sens de nos libertés, tout en innovant si besoin.

Et les machines ? Comme évoqué dans le chapitre précédent, Bitcoin pourrait aussi être la monnaie des machines. Avec déjà plus de 10 milliards d'objets connectés sur la planète, mais bientôt 5 fois plus en 2020[100], Bitcoin ou une autre méta-monnaie ont de très grandes chances de devenir leur monnaie d'échange.

De nombreux cas existent où les machines ont des interactions transactionnelles. Plusieurs variantes demeurent. Dans un premier temps nous pouvons prendre pour exemple les machines connaissant une transaction de l'humain vers machine. Dans l'état actuel des choses, toutes ces machines doivent passer par des tiers lorsqu'il s'agit d'une transaction électronique, l'information n'étant pas intégralement dans la machine ou sur la carte bleue : à un moment où à un autre la banque est interrogée ou, dans le cas contraire, il y a un risque de cash-back. Cela inclura par ailleurs des frais de transaction faramineux par rapport au nombre d'opérations journalières.

Prenons un exemple simple : les portiques et bornes de transports en commun urbains. Pour l'instant, la machine doit faire appel à un processeur de paiement pour pouvoir accepter les cartes bleues, sans quoi les paiements seraient pré-acceptés, avec un vrai risque de fraude. Ce qui fait que toutes les machines du métro de Paris ne sont pas encore équipées de capteurs NFC permettant de payer directement au portique. Pour pallier cela, les sociétés de transports en commun fournissent des tickets ou cartes rechargeables à l'unité (*Oyster* à Londres) ou au forfait (*Navigo* à Paris). Cela leur permet au moment du passage du portique de ne pas avoir de frais bancaires sur ces micro-transactions, mais cela leur permet surtout d'éviter de faire une longue et couteuse requête bancaire. Dans le cas de bitcoin, il n'y aurait rien de tout cela.

Trois solutions sont possibles pour les portiques. Soit ils sont tous détenteurs d'un portefeuille Bitcoin qu'ils remplissent et décaissent automatiquement. Soit l'opération de solde à intervalle régulier est effectuée manuellement. Soit enfin ils ont juste à observer la blockchain Bitcoin pour savoir si un paiement est passé sur une adresse extérieure. C'est aussi simple que ça. Comme tous les portefeuilles Bitcoin sont interopérables du fait que c'est un protocole et non uniquement un logiciel, il n'y a plus de problème de normes types Mastercard, Visa ou Amex. Et tout cela en permettant à la société de transport de faire de conséquentes économies et aux consommateurs de gagner du temps, de la discrétion et de l'argent en n'achetant plus des tickets qu'il n'utilisera finalement pas. C'est une belle prouesse mais ce n'est qu'un fragment des possibles.

L'Internet des objets, dans l'imaginaire commun, a tout de même quelque chose de plus excitant qu'un simple portique, électronique ou non[101]. Mais il faut bien penser que cela serait généralisable à tous les portiques du monde : des autoroutes aux entrées de musée et bien d'autres. Avec en plus une preuve indélébile du paiement en cas de problème.

Autre exemple plus amusant : imaginons un réfrigérateur qui analyse directement son contenu en temps réel et passe commande automatiquement chez un marchand prédéfini (ou pas ? il pourrait comparer les prix) quand un aliment manque. Sachant que le réfrigérateur pourrait être lié à un site de recettes et commanderait alors automatiquement les aliments manquant correspondant à une recette consultée à un autre moment de la journée dans un tout autre endroit. Pareillement pour le lave-linge qui commanderait sa lessive quand celle-ci serait insuffisante. Pour l'instant ce genre de services pourrait être imaginable, mais il faut que le site sur lequel le client commande ait sa carte de crédit enregistrée, ce qui augmente les risques. Avec Bitcoin, le lave-linge a ses propres clefs privées ou un compte joint avec son propriétaire et ses bitcoins qu'on peut recharger facilement.

Tout cela est encore un peu lointain. Nous sommes pour l'instant dans la phase de « *monitoring* » avec l'Internet des objets. Si l'on observe aujourd'hui la majeure partie des objets connectés, ceux-ci ont pour faculté d'être liés à un site Internet ou à une application où il est possible d'obtenir des informations sur l'objet en question.

On pourrait prendre l'exemple de tous les objets de surveillance de santé, mais prenons plutôt un exemple dans la botanique ou l'agronomie : un objet connecté permettant de connaitre l'humidité de la terre et d'autres paramètres serait seulement capable actuellement de recommander des actions à faire pour une plantation. Mais

dans l'idéal de l'*Internet of things*, il est un peu dommage d'avoir recours à un humain pour effectuer une tâche aussi simple que de commander de l'engrais en fonction de l'état de la terre.

Et on peut imaginer d'aller plus loin, si ce genre d'appareil a une vocation professionnelle. Les serres en sont déjà pourvues mais l'intervention de l'homme est souvent nécessaire. Avec des transactions, tout devient plus simple, l'objet botanique communique directement avec les mécanismes d'arrosage qui pourraient payer l'eau au compte-goutte, sans mauvais jeu de mot, au lieu de la payer mensuellement.

Dans une perspective encore plus élaborée, dans le domaine de l'énergie par exemple, le système de chauffage de la serre serait lui aussi connecté aux capteurs dans la terre et s'occuperait de négocier automatiquement sur un marché décentralisé d'opérateurs énergétiques (n'oublions pas qu'il y a de forte chance que nous nous dirigions vers un marché de l'énergie bien plus décentralisé, avec des millions de petits producteurs d'énergie) le meilleur prix, voire le meilleur moment par rapport au prix pour se déclencher, et bien sûr de payer la note en temps voulu. Tout cela de manière totalement autonome.

Bitcoin permet cela, il rend possible une parfaite autonomie et automatisation des objets connectés. Ils peuvent s'émanciper de l'homme, au sein de leur fonction. Et les exemples ici ne sont qu'une fraction minuscule des perspectives possibles sur ce type de problématiques.

Si un jour nous arrivons à faire le lien difficile entre un bien tangible et un bien intangible, c'est aussi tout le monde de la propriété qui pourra être bouleversé. Les maisons, forcément intelligentes, possèderaient des serrures s'ouvrant en exécution d'un contrat cessible. Un *token* sur la blockchain ne peut être dupliquée, c'est le moyen le plus efficace d'avoir une serrure numérique. Mais la question de l'identité d'un objet ou d'un humain dans un système d'échanges décentralisés est encore un problème de taille pour l'instant. Il est encore impossible, en effet, de faire un lien sûr entre le cyberespace et les territoires et les choses tangibles non numériques.

Le Bitcoin pourra vraiment être la monnaie de l'Internet des objets quand ceux-ci, et c'est un point capital, possèderont un langage transactionnel. Cela posera évidemment un nombre impressionnant de questions éthiques ou juridiques, mais nous ne pouvons pas résoudre ces questions avant d'être confrontés à des entités concrètes et se fondant sur ces principes nouveaux. *Wait and see.*

Toutefois l'Internet des objets n'est qu'une possibilité de développement pour Bitcoin. Ce n'est pas cette perspective en soi qui fait que Bitcoin est bien plus qu'une monnaie, qu'il va au-delà. Car, pour l'Internet des objets, Bitcoin n'est une méta-monnaie qu'au sens sociétal. Certes, la monnaie ne sert plus uniquement aux humains mais aussi aux machines, mais c'est ici l'usager qui est une nouveauté, pas encore l'usage lui-même.

Pourtant Bitcoin est une véritable mine de cas d'usages extra-monétaires… Même si nous aimons rappeler que sa fonction première, centrale, essentielle, est transactionnelle et monétaire. D'où le terme de méta-monnaie. Les à-côtés sont en quelque sorte les bonus du film d'un DVD mais ils ne remplacent pas le film lui-même et ne pourraient exister sans lui.

Les usages concrets, c'est-à-dire déjà approuvés et utilisés à petite échelle, sont la « preuve d'existence » que confère la blockchain de Bitcoin (comme toutes les autres blockchains, certes, mais comme la valeur probante d'une blockchain se mesure à sa solidité et à sa large utilisation, Bitcoin est *de facto* la blockchain avec la valeur probante la plus fiable). Pour l'instant celle-ci n'a pas valeur de preuve au sens du droit en France.

Mais les autorités devront tôt ou tard statuer sur les tampons d'horodatage fiables et infalsifiables d'une blockchain ou de blockchains. Nous disons bien d'une blockchain ou de blockchains car il faudra bien la nommer par son nom ou alors établir les normes techniques très précises de celles pouvant avoir une valeur probante.

Il faut surtout regarder les conséquences, ou l'absence de conséquences de telle ou telle révolution annoncée par telle ou telle institution, entreprise ou corporation. Les notaires, lit-on parfois, seraient ainsi en train de travailler sur un projet de blockchain privée. Et alors ? Ce rajeunissement (ou ce sauvetage) de leur tampon ne changera absolument rien à la situation actuelle. Le tampon serait modernisé, mais au service d'une profession privée qui offre des garanties publiques dont elle détient historiquement le monopole. Cela n'en fera pas un tampon public, fiable et disponible à tous. L'annonce de telles blockchains va rarement au-delà du plan *com*.

De quoi parle-t-on ici ? Bitcoin permet, comme nous l'avons expliqué, d'inclure au sein de chacune de ses transactions (fût-ce une transaction de quelques milli-bitcoins) 80 caractères de textes. Cela semble très peu mais

c'est amplement suffisant pour déposer l'empreinte SHA-256 d'un document puisque ces empreintes font 64 caractères. Il suffit alors de conserver le fichier original dont on a calculé l'empreinte pour prouver a posteriori, en cas de besoin, que l'on a bien créé un document à telle date. Même en cas de perte de clefs, le hash sera toujours présent dans la blockchain.

Il ne faut toutefois pas considérer l'adresse d'émission de la transaction support de cette empreinte comme une preuve à part entière de propriété sur le document « racine », sauf dans le cas précis où l'on pourra aussi prouver une extrême rigueur dans la sécurisation des clefs. Mais en ce qui concerne la propriété intellectuelle, par exemple, il suffit effectivement de signer le document original qui a été hashé et accolé à une transaction.

On entend souvent dire que la blockchain serait en ce sens la fin des intermédiaires, mais elle annonce avant tout la libéralisation des intermédiaires, comme dit précédemment. En effet le tampon fiable, infalsifiable et éternel devient un commun et non plus la propriété de certains, exactement comme le tampon symbolique de l'État sur les pièces de monnaies ou la signature du Gouverneur sur les billets de banque. Dès lors, chacun pourrait avoir le rôle de l'INPI et il pourrait y avoir des « breveteurs » indépendants qui seraient jugés selon leur talent à faire des plans avec des normes et des descriptions inégalables. Un tel professionnel pourrait même effectuer un contrat intelligent avec son client en mettant la transaction avec l'empreinte dudit brevet dans la blockchain en échange d'une certaine somme de bitcoin. Ce serait une sécurité de plus, car il y aurait alors une trace de la transaction entre le « breveteur » et son client qui, en théorie, émettrait la transaction au même moment et dans des adresses liées.

Voici le parfait exemple d'un des « au-delà » monétaires de Bitcoin qui rend pertinente la dénomination de méta-monnaie. Il peut faire plus qu'une monnaie. Nous parlions précédemment du timbre, mais c'est aussi une monnaie-lettre. En plus de sceller des transactions, sa blockchain scelle des textes ou des fichiers accolés à ces transactions.

Les informaticiens, doués d'un sens certain pour l'optimisation, ont réussi à faire des 80 caractères d'espace libre dans les transactions, après ce que l'on appelle un OP_RETURN, un monde nouveau. Ainsi, comme décrit précédemment, il existe des techniques permettant de colorer des bitcoins et donc de créer des *assets* (fonds) de jetons : pour quelques centimes, on pourra créer un fonds de plusieurs millions de jetons qu'il sera également loisible de distribuer comme bon semblera au(x) créateur(s). Tout cela en bénéficiant de la sécurité de Bitcoin. On choisit souvent l'exemple de la représentation de valeur, le jeton représentant une action par exemple, même s'il reste difficile de faire le lien entre une propriété tangible et une propriété du cyberespace.

Le vote constitue un cas d'usage plus concret. Il est très facile d'effectuer des votes fiables et infalsifiables avec cette technique. Il suffit de distribuer aux votants des jetons sans valeur, si ce n'est la valeur requise pour l'émission initiale équivalente à quelques poussières de bitcoin. Comme tout est transparent, il est aisément vérifiable que la somme de base est égale au nombre de votants, et que chaque votant n'a qu'un jeton. C'est donc un moyen peu couteux et extrêmement sûr de permettre le vote électronique.

Quel plaisir de clore ces différents exemples sur l'apport démocratique que pourrait concrétiser Bitcoin. Le jour où le vote électronique se généralisera, il sera possible d'avoir des démocraties bien plus participatives et des votes bien plus sûrs. Nous pourrions voter de façon bien plus fréquente, et sans grand coût (sans doute aussi sans grands drames) pour des choses usuelles, mais aussi réduire l'opacité et la corruption. Pensons, par exemple, à ce que serait l'intervention des citoyens pour juger eux-mêmes entre les différents appels à projet pour la construction de telle ou telle infrastructure publique, une fois rendu public après l'examen préalable par des professionnels des coûts et des normes…

Nous n'avons fait là qu'énumérer une petite partie des choses qui font que Bitcoin est une méta-monnaie. Résumons-nous. Bitcoin est une monnaie, mais c'est aussi une monnaie nouvelle, celle « d'après », celle qui change notre paradigme actuel de la monnaie sous toute ses coutures : philosophiques, anthropologiques, sociologiques, symboliques, techniques, etc. Mais c'est aussi plus qu'une monnaie, tant au niveau de ses utilisateurs (humains et machines) que de ses utilisations, désormais non limitées à l'échange de valeur. Comme le fait remarquer Andreas Antonopoulos dans ses conférences, dire que Bitcoin est une juste une monnaie numérique, c'est un peu comme dire que *« the Internet is a fancy telephone »*.



Andreas Antonopoulos explique Bitcoin (conférence filmée)

Le point III, 2 reviendra sur ses autres usages. Nous espérons que ce terme de « méta-monnaie » aura attisé la curiosité du lecteur et l'incitera à l'utiliser pour faire de même avec ses pairs. Qu'il n'hésite pas ! Le lexique est libre et horizontal, tout comme Bitcoin !

III

Histoire passée et présente d'une monnaie jeune, féconde et universelle

1- UNE ENFANCE DIFFICILE, UNE ADOLESCENCE TURBULENTE : LE BITCOIN DANS LA ZONE À RISQUE

Les mythes fondateurs

Le premier mythe fondateur est certainement l'absence de géniteur. Qui a créé Bitcoin ? Satoshi Nakamoto, qui a signé de ce nom le livre blanc *(white paper) Bitcoin : A Peer-to-Peer Electronic Cash System* et l'a publié le 31 octobre 2008 sur une liste de diffusion assez confidentielle, puis sur le site Bitcoin.org dont il avait réservé le nom le 19 août. Il prétendait alors être un japonais de 37 ans qui aurait travaillé sur ce projet depuis 2007.

C'est en janvier 2009 qu'il sortit la première version du logiciel *Bitcoin-QT* et créa les premières unités de sa monnaie, à raison de 50 bitcoins toutes les dix minutes, largement pour lui seul durant quelque temps. En décembre 2010, il publia un dernier message sur le forum *bitcointalk* [102] qu'il avait créé puis, juste avant son départ, il intronisa comme son successeur Gavin Andresen, un informaticien diplômé de Princeton, en lui donnant, pour prévenir le réseau en cas de problèmes graves, une clef d'alerte qui devrait être révoquée en 2017 [103]. Enfin, en mai 2011, il livra ce qui peut ressembler à un testament : « *Je suis passé à autre chose et je ne serai probablement plus là à l'avenir.* »

Qui est réellement Satoshi Nakamoto ? Tous les éléments d'un roman sont réunis, surtout si l'on songe (et chacun y songe) que Satoshi doit détenir au moins un million de bitcoins [104]. Dans les rêves les plus fous de la communauté, son magot en ferait un jour l'homme le plus riche du monde. S'il n'a pas perdu sa clef !

Parmi toutes les hypothèses, on rencontre bon nombre de noms de précurseurs déjà évoqués au point I, 1, mais aussi des noms comme Michael Clear, un irlandais spécialiste des codes, ou Martti Malmi, un informaticien virtuose finlandais, le dernier à avoir reçu un message de Satoshi, d'autant que son nom a disparu du site de Bitcoin le jour où Satoshi Nakamoto a cessé de répondre aux internautes, ou Jed McCaleb, créateur de la plateforme d'échange MtGox, ou Shinichi Mochizuki, un mathématicien japonais spécialisé dans la théorie des nombres ou encore Vili Lehonvirta, un économiste finlandais, ancien programmeur de jeux vidéo.

Le nom qui revient le plus souvent est cependant le nom de Nick Szabo, membre influent des Cypherpunks, qui avait, entre 1998 et 2005, développé avec quelques autres le concept de *Bit Gold* [105], une monnaie numérique décentralisée qui annonçait en pensée le Bitcoin. Ou bien Hal Finney, décédé aujourd'hui, qui échangea la première transaction en bitcoin avec Satoshi et fut aussi le premier à écrire en deux mots le terme « block chain ». Mais Bitcoin a d'autres précurseurs, et Nick Szabo a dit que le père de Bitcoin pouvait tout aussi bien être Wei Dai.

Certaines hypothèses sont plus douteuses : en 2013, deux chercheurs israéliens (Ron et Shamir) dénoncèrent sur la base d'indices plutôt ridicules Ross Ulbricht (le propriétaire du site illégal Silk Road) comme étant l'inventeur. Quelques mois plus tard, une journaliste de *Newsweek* découvrit un californien de 64 ans passionné par les mathématiques, la cryptographie et les trains miniatures : ce cryptographe aurait travaillé sur des projets confidentiels pour le compte de l'armée et de grandes entreprises. L'homme, d'origine japonaise, qui s'appelait Dorian Satoshi Nakamoto, jura n'avoir jamais entendu parler du bitcoin auparavant et finit par donner une

interview pour nier poliment. Mais son image fit le tour du monde et inspira largement les artistes de la communauté ! Dès le lendemain de la fracassante révélation de Newsweek, un message avait été posté depuis le compte original du créateur de Bitcoin, inactif depuis plus de 4 ans, disant sèchement *Je ne suis pas Dorian Nakamoto* [106]. L'auteur de ce dernier message était-il pour autant Satoshi, ou un hacker ? Vertige d'un mystère en abîme…

Aucun consensus n'existe. Le plus grand nombre de suffrages va sans doute à Nick Szabo. D'ailleurs, en avril 2014, une équipe universitaire [107] a comparé le fameux *white paper* de 2008 aux publications de 13 suspects et désigné Szabo comme l'auteur « principal » du document de 2008. Un an plus tard, un journaliste du *New-York Time* publia une enquête qui confirmait les travaux des linguistes universitaires bien que celle-ci l'ait amené à rencontrer Szabo qui réitéra ses dénégations.

L'idée que Satoshi soit un groupe a ses supporters, même si les contours de cet hypothétique groupe varient au gré des spéculations.

À côté de l'hypothèse du groupe on trouve aussi celle du consortium, comme celui qu'auraient secrètement formé les quatre groupes technologiques Samsung, Toshiba, Nakamichi et Motorola dont les syllabes initiales évoquent le nom du mystérieux inventeur. Plus loin encore dans le complot, Bitcoin serait une opération noire de la NSA regroupant jusqu'à une cinquantaine de personnes.

Le plus récent épisode, en 2016, fut celui de la revendication par l'australien Craig Wright, adoubé par Gavin Andresen, mais dont plusieurs experts ont démontré qu'il s'agit d'une escroquerie. Wright promit alors de nouvelles preuves, avant de renoncer définitivement quelques jours plus tard. Certains ont dit que ce mythomane avait de longue date semé des indices plus ou moins crédibles ou fabriqués de toutes pièces, d'autres qu'il pourrait avoir joué un rôle mineur dans l'équipe qui créa Bitcoin.

Le fait que le « magot » de Satoshi soit resté intact depuis l'origine accrédite ou suscite diverses rumeurs, et étaye l'hypothèse que la clef ait été partagée entre plusieurs personnes dont une qui a pu mourir ou perdre son secret.

Ce magot ne semble qu'un détail au vu de l'avantage d'avoir un géniteur inconnu. Bitcoin ne pourrait être ce qu'il est aujourd'hui sans la « disparition » de Satoshi Nakamoto. Si Bitcoin n'a pas de tête, c'est aussi parce qu'il n'a pas d'inventeur, de leader, d'héritier ou d'inventeur. La gestion du code est totalement horizontale. Chacun peut travailler sur une version du protocole Bitcoin et la proposer au monde. Si le consensus décentralisé se dirige vers cette version, c'est elle qui sera adoptée. Actuellement, l'équipe de développement ayant le consensus est composée d'une quarantaine de personnes, dont pour certaines on ne connait que le pseudonyme. Encore une fois, tout dans ce milieu se fait par réputation. L'avantage de l'absence de leader identifié, c'est qu'il n'y a pas de volonté prioritaire comme on le sent chez Ethereum avec Vitalik Buterin. Il n'y a personne vers qui se tourner, à qui déléguer sa réflexion. Bitcoin et ses hommes doivent trouver des accords et réfléchir ensemble pour concevoir le protocole le meilleur possible. La communauté Bitcoin, elle aussi, est *acéphale*.

Quoi qu'il en soit des raisons du silence de Satoshi, son absence et son silence sont plus qu'un mystère, un fait majeur qui pèse parfois d'un certain poids sur la communauté. Que cette communauté ait un fondateur « mythologique » suggère deux comparaisons, avec le Peuple élu ou la Ville éternelle.

De Moïse aussi on a tout dit : enfant trouvé par une princesse, enfant d'une servante volé par une princesse, enfant de la princesse, demi-frère du roi, prince hérétique. Et puis Freud est arrivé et a affirmé que Moïse, quel qu'il soit, était un étranger au peuple qu'il a inventé. La Bible dit qu'il ne pourra pénétrer en terre sainte : serait-ce à dire que l'on n'avait plus besoin de lui ? Moïse a inventé un dieu insaisissable dont Pharaon se moque parce qu'il est « sans réalité concrète ». Cela peut faire réfléchir à la nature des critiques portées aujourd'hui contre le bitcoin. Ce sont des critiques « idolâtres », défendant l'honneur des banques centrales, comme de petits temples païens, conservant chacun son stock d'or et adorant son idole locale… Avec son dieu invisible, Moïse a en réalité inventé un peuple sans tyran. Bitcoin, qui n'a pas d'or dans sa cave, n'a pas non plus de tyran dans son palais.

Pensons aussi à Romulus. C'est le fils d'une louve, qu'il s'agisse d'un animal sauvage ou d'une simple prostituée. Comme Moïse, il est abandonné sur un panier confié au fleuve et recueilli par des bergers. Rome est née un peu du hasard, avec des origines hors du système. Romulus n'hérite de rien. Avec sa charrue, il trace deux axes perpendiculaires et un fossé : sa ville sans tradition est d'abord toute mathématique. Ces murailles sans

pierres font rire son frère qui saute par-dessus le sillon. Romulus tue Rémus qui avait cru, lui aussi, que le nouveau système n'avait « aucun fondement concret ».

À travers ces deux comparaisons on peut explorer ce que l'histoire, la mythologie, voire la psychanalyse, suggèrent comme pistes pour comprendre les conséquences de cette absence de père du bitcoin. Satoshi Nakamoto est un vrai mythe, parce que son absence interroge, inquiète et finalement libère les énergies.

La pizza à dix millions est un second mythe fondateur, touchant à la naissance héroïque d'une monnaie inattendue.

Il faut le répéter encore une fois : longtemps le bitcoin fut sans valeur, un jeu entre une poignée de mineurs, quelques dizaines tout au plus au bout de plusieurs mois. Le 15 janvier 2010 un site s'était amusé à estimer le prix d'un bitcoin et afficha un « prix » de 0,001 $ pour le 10 mai 2009[108]. L'un des mineurs lança un jour l'idée que cette improbable monnaie devrait permettre de faire au moins un repas. Aucun restaurant, évidemment, n'acceptait (ni même ne connaissait) Bitcoin. Le 22 mai 2010 un étrange *deal* eut lieu. Un appel avait été lancé le 18 sur le forum Bitcointalk par Laszlo Hanyecz, un développeur vivant en Floride : qui accepterait de commander une pizza (et de la payer en argent légal) contre une somme en bitcoin ? De Londres, un bitcoineur accepta de commander une pizza mythique (deux, en fait !) chez Papa John's à Jacksonville, et de les régler par Visa, contre 10 000 bitcoins. L'arrivée des pizzas le 22 mai au soir fut annoncée photo à l'appui sur Bitcointalk[109].

Il n'y avait alors aucun vrai marché du bitcoin. Les premiers bitcoineurs le créèrent entre eux vers la même époque, en partant d'une approximation consensuelle du coût du minage. Le bitcoin coûtait environ 0,008 $. Avant la fin de la semaine, les échanges se réalisaient à 10 fois ce prix.

Pour autant, il n'y a jamais eu de « pizza à dix millions », c'est une histoire écrite rétroactivement et qui incorpore la même erreur anachronique que le reproche, souvent fait à Bitcoin, d'être une monnaie dont la détention est extrêmement inégalitaire – on lui reproche aussi d'être un Ponzi, mais quelqu'un qui imaginait le bitcoin à 1 000 $ aurait-il échangé 10 000 bitcoins contre une ou deux pizzas ?

En revanche, chaque année, le 22 mai, des milliers de pizzas sont partagées partout dans le monde. Ignorer cela, c'est passer à côté de ce qu'est bitcoin. De l'euro, seuls les banquiers et les politiciens assurent qu'elle est « notre monnaie ».

Les premiers bitcoins perdus présentent la face douloureuse du même récit des commencements. La route vers Bitcoin avait été pavée d'échecs divers et rien n'indiquait que le bitcoin vaudrait un jour d'avril 2011 un dollar, puis un gramme d'or vers la fin de l'été 2011, puis une once d'or à la fin novembre 2013 ni qu'il culminerait à plus de 1 000 dollars peu après. En janvier 2010, soit un an après sa naissance, les 1,6 million de bitcoins déjà minés n'avaient pas de vrai cours de marché et la première transaction avec le monde réel (la fameuse pizza) n'avait pas eu lieu ; en janvier 2011 il y avait 5 millions de bitcoins qui valaient en tout 1,5 million de dollars, en janvier 2012, les 8 millions de bitcoins minés valaient 41,6 M$.

On ne conserve évidemment pas avec autant de soin une pièce en cuivre et une pièce en or. Certains bitcoins ont pu être considérés comme des jouets sans valeur intrinsèque, obtenus au cours d'une expérience de minage ou d'échange pédagogique ou ludique. Comme tant de jouets, ces bitcoins ont été oubliés, abandonnés, perdus. Quand les médias ont signalé l'explosion des cours, bien des gens se sont aperçus qu'ils possédaient un trésor. Seulement c'est une chose de fouiller son grenier pour retrouver de vieux jouets devenus *collectors*, ou de rechercher l'or de grand-père dans la cheminée, c'en est une autre de récupérer des bitcoins dont on a perdu la clef. Si cette clef a été inscrite sur un bout de papier, les chances de la retrouver après deux ou trois ans sont minces, si elle est dans un fichier écrasé ou dans un ordinateur perdu, les chances sont quasi-nulles.

Le cas le plus célèbre est celui de l'informaticien britannique James Howells. En 2009, quand un simple ordinateur portable permettait de miner, il avait ainsi accumulé 7 500 bitcoins. En 2010 l'ordinateur tombe en panne, et comme beaucoup de pro, il le désosse et garde le disque dur, au cas où. À l'été 2013, en rénovant sa maison du Pays de Galles, il décide de passer un bon coup de balai. En novembre, le cours explose littéralement, tous les médias parlent soudain du bitcoin, le meilleur placement de l'année. Et là, James Howells est saisi d'un doute affreux : il fouille sa maison en tous sens, il ne retrouve pas son disque dur. Il se rend à la décharge de Pillgwenlly, Newport… mais son disque dur y git sous des tonnes de déchets qui couvrent la surface d'un stade de foot.

Son histoire a fait le tour du web[110]. Elle n'est sûrement pas unique ! Ce qui est frappant, c'est que la malheureuse victime de sa propre erreur n'est pas un homme inexpérimenté dans la chose informatique. Tous les professionnels avouent avoir, au moins une fois, commis une imprudence, omis de faire une sauvegarde, jeté une clef USB sans avoir reporté tous les fichiers ou égaré un mot de passe ou une clef cryptographique.

Rapportée au bitcoin, cette faiblesse humaine pose une série de questions. La première est de tenter de mesurer le nombre de bitcoins qui peuvent être perdus. Or l'analyse de la blockchain ne permet que de dénombrer les « zombies », ceux qui sont inscrits à une adresse qui n'est plus jamais débitée, voire qui ne l'a jamais été depuis sa création. Une étude très détaillée de juin 2014[111] mesurant ce phénomène sur 18 mois (donc sur la période où le cours du bitcoin avait connu 4 000 % de hausse) estimaient leur nombre à près de 30 %, soit 3,9 millions de bitcoins sur les 13 millions déjà minés alors. On y trouve des adresses contenant jusqu'à 70 000 bitcoins, mais surtout un grand nombre d'adresses contenant 50 bitcoins, correspondant à une « récompense » de minage durant les 4 premières années de l'expérience : des gens qui ont miné quelques heures ou quelques jours, ont touché la récompense et arrêté le jeu. On trouve des adresses qui semblent correspondre à des coffres forts dans lesquels un magot a été viré un jour à partir d'autres adresses vives pour être désormais conservé sur une clef de type USB, sans vocation à être utilisé. On y trouve des comptes qui semblaient vivre et qui un beau jour sont devenus inertes. Enfin on trouve des millions d'adresses ne contenant que quelques millièmes de bitcoin : des adresses expérimentales, qui ont servi à des jeux, à des démonstrations, à des essais.

Bien sûr, le plus gros magot dormant est notoirement celui du fondateur, facile à identifier en traçant les mouvements à partir des adresses créditées des premières récompenses. Satoshi, s'il est toujours en vie, a-t-il perdu volontairement ou involontairement sa clef ? Attend-il un événement et si oui lequel ? A-t-il l'intention de le donner ou de le distribuer, dans une démarche philanthropique ou politique ? Cela fait, on en conviendra, bien des hypothèses possibles, avec des conséquences bien différentes sur la valeur à terme des bitcoins « vifs ».

Mais il y a un autre aspect à considérer autour de ces bitcoins perdus : ils soulignent d'une certaine façon la difficulté qu'il y a à être soi-même responsable de sa clef informatique. C'est aussi ce qui fait que nombre de bitcoins (monnaie conçue pour se passer de banque) sont en réalité détenus sur des plateformes qui agissent de facto comme des sortes de banque : le client souvent ne possède plus sa clef (c'est la plateforme qui la détient) mais seulement une sorte de code PIN lui permettant d'accéder à son compte. Et cela convient très bien à nos contemporains, formatés par des décennies d'usage d'un compte en banque. Seulement cette solution-là n'est pas sans risque non plus : tous les grands « braquages » de bitcoin, qui vont être évoqués au point suivant, ont exploité non des failles du protocole Bitcoin mais des failles de sécurité de ces plateformes.

Vade retro, Bitcoin

Nous y voici, enfin ! Le récit des trafics illicites sur la Route de la Soie (*Silk Road*) ou de la crapuleuse faillite de MtGox aura donc attendu la page 173, mettant peut-être à l'épreuve la bienveillance du lecteur. Sans vouloir taire les erreurs de jeunesse du bitcoin, il ne nous a pas semblé qu'elles avaient vocation à constituer l'introduction ou le chapitre pédagogique de notre ouvrage. Expliquerait-on l'activité d'une banque en commençant par le désastre du Crédit Lyonnais, la faillite de Lehman Brothers, la condamnation de HSBC à près de 2 milliards de dollars d'amende pour blanchiment d'argent de la drogue[112], toutes affaires qui se sont pourtant déroulées au cœur même du système ?

Inversement il n'est pas question d'éluder des affaires qui renseignent sur les risques liés à l'environnement de la nouvelle monnaie décentralisée.

C'est en juin 2011 que Joe Manchin, sénateur de Virginie occidentale, réclame la fermeture d'un site en ligne anonyme offrant toutes sortes de drogues, *Silk Road*. Cet appel semble être resté assez longtemps sans écho sérieux, mais le FBI commença surveillance et infiltration dès novembre.

Silk Road fonctionnait depuis février 2011 sur le modèle des places de marché qui ne font que mettre en rapport acheteurs et vendeurs, mais gérait aussi une activité de séquestre temporaire des fonds lui permettant d'arbitrer d'éventuels litiges. Transactions et séquestres étaient exclusivement en bitcoin, non pas d'ailleurs directement, mais sous la forme de « comptes en bitcoin » sur la Route de la Soie, qui de ce fait tenait une forme de « banque », et peut-être même la plus grosse qui ait jamais existé pour Bitcoin.

La drogue assure sans doute la majeure partie des revenus du site. On y trouve 13 000 références de stupéfiants, jusqu'aux plus violents, car en l'absence de tout contrôle certains vendeurs jouent sur la similarité de molécules moins coûteuses pour proposer des produits (encore plus) dangereux. Le site met donc en place, comme sur eBay, un système d'évaluation des parties.

Mais ce n'est pas sa seule marchandise. On trouve (un temps) des armes, des faux papiers, des offres de piratage de comptes, des logiciels pour déverrouiller des ordinateurs ou voler des mots de passe et bien des choses dites *off-limits* sexuellement ou politiquement : manuels de guérilla ou de confection d'armes chimiques. Enfin, le site offre aussi un forum où les membres peuvent échanger leurs commentaires sur les vendeurs ou leurs conseils sur la façon la plus discrète de recevoir leurs colis.

Car avant d'évoquer les solutions sophistiquées d'anonymisation, il faut souligner que l'acheminement des marchandises se fait tout bonnement par la poste ou les sociétés de fret. Cependant, pour que celui qui reçoit un paquet illégal puisse éventuellement clamer sa bonne foi, la dissimulation des traces d'achat puis de paiement s'avère essentielle.

Sur *Silk Road*, acheteurs et vendeurs ne sont pas pseudonymes comme sur les sites de rencontres où l'anonymat n'est que celui des parties mais où les opérateurs conservent toutes les traces, et l'ordinateur de chacun également. Il faut distinguer ici plusieurs facteurs d'anonymat : celui des sites, celui de la navigation, et enfin celui des transactions.

Ce que l'on a appelé le *deep web* n'est pas juridiquement défini et consiste dans la masse des sites accessibles en ligne aux internautes mais non indexés par les moteurs de recherche classiques. On a parlé dès 2001 de 90 % de l'Internet, peut-être par analogie avec l'iceberg, mais il est très probable que cette partie immergée soit écrasante, de l'ordre de plus de 5 000 fois le web visible (99.98 %) selon des études assez récentes [113]. Ce sont notamment les blogs privés, les pages protégées par des mots de passe, des formulaires ou des *captchas*, et aussi des pages publiques que leur structure rend opaques aux algorithmes des moteurs.

En revanche le *Darknet*, popularisé dans le grand public vers 2010, mais qui existait depuis aussi longtemps que l'Internet, est celui de pages qui ne sont pas même accessibles avec les navigateurs classiques, celles par exemple dont l'adresse se termine en « .onion » ce qui évoque métaphoriquement un principe du routage dit en oignon qui fait rebondir les échanges au sein d'Internet afin de neutraliser les analyses de trafic.

Avec ce type de routage, la connexion et la source d'un message peuvent être rendue presque impossibles à tracer, grâce au design et au fonctionnement spécifiques d'une dizaine de réseaux différents, dont Tor (*the onion router*) développé depuis les années 90 est le plus connu. Les trafics de drogue sur le net n'ont donc pas attendu Bitcoin ! Nous ajouterons que l'armée américaine est une des organisations à l'origine du projet Tor. Aujourd'hui Tor est considéré comme assez sûr, mais pas absolument car il a été prouvé de nombreuses fois qu'il était possible de réussir à observer le système en jouant à son jeu, en devenant un nœud anonymisant. De nombreux autres projets, peut-être même plus efficaces, n'ont cependant pour l'instant pas son aura.

Le règlement des transactions restait en 2009 le maillon faible des activités illégales dans le *dark web*. Que les acteurs des marchés illégaux aient compté parmi les premiers utilisateurs du bitcoin s'explique alors aisément. Cependant, Tor n'a pas été développé pour eux mais en partie par des militaires américains qui l'infiltrent sans doute toujours. Tor ne sert pas qu'à eux mais contribue aussi à contourner la censure, à assurer la liberté d'enquête des journalistes ou la vie privée des internautes. De la même manière, il est peu probable que Satoshi Nakamoto ait été trafiquant ou consommateur de drogue dure, et le bitcoin a su trouver d'autres utilisateurs.

Lorsque, le 2 octobre 2013, le FBI appréhende Ross Ulbricht qui vient de se connecter dans une bibliothèque publique de Chicago, la presse cite des chiffres fondés sur son rapport public, mais en préférant le plus souvent les retranscrire en dollars. Or le bitcoin a commencé le mois d'octobre 2013 à 100 $, un niveau qui n'était absolument pas celui des années 2011 ou 2012, et il l'a terminé à 200 $. Etablir un bilan en dollars de la *Silk Road* gonfle la réalité quand les conversions sont refaites par des journalistes aux cours de la fin 2013 ou de 2014 alors que sur les 33 mois de fonctionnement de la *Silk Road*, le cours a tourné durant 24 mois autour de 10 $ [114].

Entre sa création en février 2011 et juillet 2013, *Silk Road* aurait vu passer un peu plus de 1,2 million de transactions, pour un total de 9,5 millions de bitcoins, générant 614 305 bitcoins de commissions pour le site. Ce sont ces chiffres en bitcoin qui, convertis en dollars au cours du jour se sont transformés en 1,2 milliard de dollars de ventes et 80 M$ de commissions.

En octobre 2013, le site aurait détenu (commissions et séquestres) un peu plus de 26 000 bitcoins qu'il faudrait rajouter aux 144 000 saisis au même moment sur l'adresse supposée de Ross Ulbricht. Ces bitcoins seront revendus aux enchères par l'administration américaine.

Les 1,2 million de transactions sur la *Silk Road* sont à comparer au total de 6,9 millions de transactions enregistrées depuis l'origine jusqu'au 2 octobre sur la Blockchain [115]. Soit une proportion de 17 % si l'on considère qu'elles ont toutes eu lieu sur la Blockchain, un peu moins (15 % ?) si l'on pense que bien des transactions ont eu lieu en « compte *Silk Road* ». Les 614 305 bitcoins gagnés par le site représentaient environ 5 % des bitcoins existants en octobre 2013. Il est donc incontestable que ce marché illicite a joué un rôle dans l'économie du bitcoin. Pas de quoi cependant étayer l'identité remarquable « bitcoin = drogue » qui va être répétée ensuite durant des mois. Inversement, même en reprenant le chiffre absurde de 1,2 milliard de dollars sur trente-trois mois, la *Silk Road* aurait pesé bien moins de 1 % du marché total de la drogue aux USA !

Pour conclure, notons que le 2 octobre, le site « bitcoin.fr » qui fait référence en France annonçait de façon non équivoque « une excellente nouvelle pour tous ceux qui militent en faveur d'un usage responsable de Bitcoin » et poursuit : « le site clandestin *Silk Road*, plateforme de marché pour toutes sortes de produits illicites, vient d'être fermé par la justice américaine. » Bien sûr, on pouvait aussi lire au même moment de nombreux râles de libertariens trouvant que cette mise en prison était une atteinte de l'État envers la liberté des affaires.

L'enquête et le procès ont retenu l'attention à bien des égards : curiosité parfois inquiète quant aux investigations par lesquelles le FBI avait pu percer le réseau Tor, parfois amusée quand on apprit que le génie du mal avait laissé trainer son adresse rossulbricht@gmail.com ; spéculation sur la véritable identité du fondateur « Dread Pirate Roberts » puis sur la véritable personnalité de Ross Ulbricht, accusé semble-t-il de pas moins de neuf recrutements de tueurs à gage (sans un seul cadavre à exhiber au tribunal…) mais présenté par d'autres comme un idéaliste luthérien ; éclat de rire enfin quand deux agents du FBI se retrouvèrent à leur tour accusés de blanchiment de bitcoins volés. Le feuilleton reprit avec la réouverture du site (dès novembre 2013) et sa nouvelle clôture un an plus tard.

Toutes ces fermetures n'ont pas arrêté le trafic sur le *Darknet* ; elles n'ont fait que le décentraliser un peu plus. Comme souvent lors de la fermeture de monopoles numériques successifs, vient un moment où le réseau a de nombreux acteurs sans monopole de sorte à ce que personne n'attire trop l'attention. Ce fut aussi le cas des sites de torrents : depuis les fermetures de *ThePirateBay*, *Isohunt* puis de *KickAssTorrent* à la fin de 2016, il n'y a plus de grands noms du torrent, mais il est quasiment toujours aussi facile de télécharger.

Le procès mit à jour une palpable incompétence technologique des politiques, des juges et de certains médias. On eut parfois le sentiment qu'Ulbricht était également condamné pour une invention technologique incompréhensible donc néfaste et pour un projet politique repoussant. Quand on cite à la barre les parents de jeunes gens décédés d'overdose, il est un peu ridicule d'ajouter que « ce que vous avez fait était terriblement destructeur pour le tissu social. » Ce fut pourtant un point critique pour la juge américaine : « l'intention avouée de la *Silk Road* était de se placer au-delà de la loi. Dans le monde que vous avez créé au fil du temps, la démocratie n'existait pas ». Or, si le trafic de stupéfiant est punissable, l'absence de sentiment démocratique (ou de ce qu'un quinquagénaire américain entend par là) l'est-elle ? La lourde condamnation à la prison à vie tient-elle à l'un ou à l'autre ? Certains retinrent que le marché sur *Silk Road* se montrait bien plus horizontal et démocratique que le marché *mainstream* dominé par d'énormes monopoles comme Walmart ou Amazon.

Au-delà d'un soutien à Ross Ulbrich circonscrit dans la frange libertarienne dure [116], le procès révéla donc d'autres clivages. L'invocation de la démocratie et des lois nationales pour des actes commis dans un cyberespace constitue-t-elle un argument suffisant et convaincant aujourd'hui pour la jeunesse mondialisée ? Il n'y a rien d'étonnant à ce qu'un *geek* et un juge ou un politicien se comprennent mal. Peut-on pour autant parler de destruction du tissu social ? On peut fort bien ne pas se reconnaître dans les idoles de l'ancien monde, et n'être ni fou ni immoral.



Comment on devient le « baron de la drogue (film)

Or, quelques mois après les dégâts occasionnés par la *Silk Road*, le monde du Bitcoin allait traverser une nouvelle tempête, qui elle aussi allait susciter bien des amalgames et amplifier le discrédit sur une révolution technologique et sociétale incomprise.

MtGox avait été créé des années avant Bitcoin par le programmeur Jed McCaleb, qui fut aussi l'un des fondateurs de la monnaie Ripple, comme une plateforme d'échange de cartes du jeu vidéo de *Magic : The Gathering Online*. Ayant découvert Bitcoin dès 2010, il transforma MtGox pour en faire une plateforme spécialisée dans cette nouvelle monnaie, mais il la revendit trois mois plus tard en mars 2011 à Mark Karpelès, informaticien français qui s'était installé au Japon en 2009.

Trois mois après ce rachat, le nombre des comptes de la plateforme avait été multiplié par vingt. Deux ans plus tard, et malgré le très grand nombre de plateformes créées, MtGox représentait 70 % des volumes d'échange sur la nouvelle devise qui commençait elle-même son ascension. Karpelès a sans doute été dépassé par la croissance, essayant d'embaucher des gestionnaires expérimentés sans parvenir à les attirer. Les incidents se multiplièrent, comme si la montée en puissance n'était pas convenablement sécurisée.

Le 24 février 2014, Karpelès doit suspendre les transactions puis, le 28 février, placer MtGox sous la protection du régime japonais de la faillite. En avril, le liquidateur annonce un trou de 850 000 bitcoins (dont 750 000 appartenant aux clients) manquants ou volés et dont la valeur à ce moment n'était pas éloignée du demi-milliard de dollars. Karpelès plaide le piratage, et, à la télévision japonaise, s'incline devant la caméra. Faillite ou arnaque ? Les extraits de sa vie au Japon dans le film *Rise of the Bitcoin* donnent l'impression d'un homme égaré, dépassé pas son succès. Le profil de Karpelès, asocial à gros QI mais *hacker* naïf, permet d'imaginer une négligence transformée par un trop long silence en délit caractérisé, une manipulation tentée pour gagner du temps, ou un Ponzi pur et simple.

Sur le coup, certains émirent l'hypothèse que MtGox avait subi un vol très important (peut-être dès juin 2011) et tentait depuis lors de poursuivre les échanges en vivant sur une toute petite réserve. D'autres pensent au contraire que le trou a été fait peu avant le gel des retraits. Mais en mars certains employés confessent avoir trouvé, dès 2012, que Karpelès confondait ses réserves et l'argent des clients. Durant son propre procès, Ross Ulbrich essaya même, sans grand succès, de le faire passer pour le vrai créateur de Silk Road.

Par la suite on retrouva 200 000 bitcoins et il apparut que les premières disparitions dataient de 2011, soit avant même le rachat à McCaleb, qui s'était fait voler 80 000 bitcoins et avait conseillé à Karpelès de garder la chose pour lui. En juillet 2015, on commença à dire qu'une bonne partie des bitcoins disparus n'aurait jamais existé, et que MtGox aurait aussi manipulé le cours à la hausse avec des robots.

Karpelès fut finalement arrêté au petit matin à Tokyo le 1er août 2015, le lendemain du dernier jour où ses clients pouvaient légalement faire valoir leurs droits. À peine moins à plaindre que les clients, les juristes japonais eurent fort à faire. Il n'y avait jusque-là aucune réglementation concernant le Bitcoin. Il fallut faire face à une multitude de questions : est-ce un jeu, un bien, une chose physique, une monnaie ? Il n'était pas même aisé de définir les compétences respectives des différentes autorités. En mars 2014, le Premier ministre japonais déclarait à la fois qu'il n'avait pas de réponses à ces questions et qu'il ne savait même pas si la faillite de MtGox était liée à un délit ou à une banqueroute. Karpelès resta quelques mois en prison avant d'être libéré sur caution en juillet 2016 sans que la date de son procès ne soit fixée.

L'affaire MtGox fut interprétée fort différemment. Tous ceux qui souhaitaient du mal au bitcoin ne manquèrent pas de souligner que cette « monnaie virtuelle » était intrinsèquement dangereuse, qu'on pouvait se la faire voler au beau milieu de la nuit, quitte à mélanger cela à des considérations sans rapport sur l'absence de garantie étatique ou de sécurisation par le système bancaire.

L'affaire fut particulièrement mal traitée en France. On vit passer des bêtises monumentales, notamment celle faisant de Karpeles le « patron du Bitcoin »[117]. Les journaux, sans *distingo* ni nuance, sauf rarissimes exceptions, se complaisaient à le surnommer le « baron du Bitcoin », sûrement en raison de sa bonhommie. Cet épisode, impliquant en outre un opérateur français, a vraiment nui chez nous à l'image de la nouvelle monnaie. La vérité est que cette faillite crapuleuse avait tout à voir, au contraire, avec l'ancien monde, celle des « tiers de confiance » qui se transforment en Judas. Les avoirs détenus chez MtGox n'étaient pas directement des bitcoins, mais des créances en bitcoin comme dans une banque classique. Car c'est bien la plateforme qui détenait les clefs.

Dans les mois qui suivirent, d'autres plateformes subirent des attaques (extérieures ou intérieures) exploitant des failles de sécurité dans leur propre défense, mais qui n'avaient rien à voir non plus avec la sécurité propre de Bitcoin, à la différence de certaines affaires ayant affecté d'autres cryptomonnaies (on y reviendra au point III, 3). Certaines en moururent, d'autres se redressèrent.

On l'a déjà dit au sujet de la *Silk Road* : le monde des *geeks* bitcoineurs a sa morale, ce que Durkheim appelle son « social intériorisé ». Cette morale peut paraître extrêmement sévère à l'encontre de ceux qui sont victimes de leurs propres failles technologiques. *Sorry for your loss* dit-on simplement. Comme toute population pionnière, la Bitcoinie n'est pas exempte d'une certaine dureté. Mais c'est la dureté des conquérants.

La monnaie du cyberespace, menace pour les États ?

On l'a déjà dit et il est inutile de le cacher : à côté d'une réelle ambition de doter le cyberespace d'une monnaie qui en intègre la physique propre, on trouve dans la conception et l'entretien du projet Bitcoin une réelle défiance vis-à-vis des États. Peut-on pour autant comprendre la défiance de ceux-ci et justifier l'allergie irraisonnée de certains politiques ? Peut-on considérer le bitcoin comme une menace sérieuse à leur égard ?

C'est certes un actif relativement anonyme. Ceci a déjà été abordé aux points I, 1 et I, 3. Mais le stock total de bitcoin, dont la valeur en dollars fluctue de 3 milliards de dollars (au creux de 2015) à une quinzaine en fin 2016, représente-t-il une menace plus grande pour la paix du monde que les 1 100 milliards d'euros de billets de banque émis par la BCE (contre 740 en janvier 2009 quand surgit Bitcoin)[118] ou des 1 380 milliards de dollars[119] (contre 783) sans compter les 800 milliards que représentent les 20 000 tonnes d'or privé détenues en pièces et lingots[120] ?

Certes c'est un actif non régulé par une banque centrale, mais de même, les 15 milliards de dollars de valeur totale du bitcoin sont-ils de nature à mettre en danger les banques centrales plus que ne le font les 6 400 milliards de valeur de l'or, dont elles ne détiennent toutes ensemble qu'un petit quart[121] ?

En réalité, ce que l'on va passer en revue dans les pages qui suivent montre qu'à la base de tout ce qui est ressenti comme menace par les autorités, on trouve toujours la mobilité de Bitcoin, sa capacité à sauter les frontières dont les banques sont les douaniers.

La monnaie des États, qui sont toutes depuis 1971 dénuées de référence à un actif doté de valeur intrinsèque, fonctionnent sur un mixte variable de confiance et de coercition, mixte dont la plus ou moins grande ouverture des frontières donne une indication. La confiance est un thème de prédilection des « tiers de confiance » et des autorités. Celle que « les marchés » manifestent ou refusent est souvent évoquée. Celle des citoyens semble préoccuper moins de monde. Elle est difficile à mesurer réellement. Une enquête d'octobre 2014 révélait qu'au niveau de la zone euro « le taux d'opinion globalement favorable à l'euro se stabilise à 57 % ». Ce n'est pas énorme. Il va de soi que dans d'autres pays du monde, et dans des périodes troublées, cette confiance tend vers zéro. Les frontières sont là pour empêcher l'implosion.

La crise de Chypre en 2013 donna une illustration criante de la chose. Dans la nuit du 15 au 16 mars la zone euro proposa un premier « plan de sauvetage » refusé par le parlement chypriote, qui accepta néanmoins la restructuration de la Laiki, la deuxième banque du pays. Le 25 mars, le second plan comprenait une garantie des dépôts limitée à ceux de moins de 100 000 euros, la mort de la Laiki et le transfert à la Bank of Cyprus de ses seuls dépôts de moins de 100 000 euros et ses actifs.

Le mot de « chypriation » entra dans les conversations. D'abord parce que les invisibles frontières de l'argent avaient été fermées (un comble au sein d'une union monétaire) et que pendant douze jours, jusqu'au 28 mars, les

guichets des banques étaient restés clos. Ensuite parce que la dévaluation de 10 % des dépôts était une prédation extraordinaire et non une mesure fiscale consentie par un parlement élu, un recul de l'État de droit sans précédent dans une Union Européenne qui se proclame un parangon de la chose.

Le bitcoin connut sa première heure de gloire. Encore inconnu du grand public, il cotait 14 $ au début de l'année, il avait doublé à la mi-février, il valait 36 $ le 4 mars, 48 $ le 6, 74 $ le 21 mars, franchissait le seuil symbolique des 100 $ le 1er avril, joli « poisson d'avril » au système officiel en plein craquement. Ayant culminé le 9 avril à 238 $, il s'effondra littéralement (cours divisé par plus de 3 en 4 jours) mais brièvement et retrouva à 100 $ un support de moyen terme inimaginable au début de l'année.

Quel rôle la crise chypriote joua-t-elle réellement dans cet envol ? C'est ce qui est plus difficile à retracer. La presse fit assez vite le rapport. L'entrepreneur canadien qui avait installé à Chypre sa première machine de vente de bitcoin (BTM) eut son heure de notoriété.

La discrétion des transactions ne permet pas de cerner la part de Chypre dans celles-ci, mais au niveau mondial elles ne représentèrent pas un demi-milliard sur la période de la crise chypriote. Le record quotidien de transaction sur cette même période, une cinquantaine de millions de dollars, ne fut atteint qu'une fois au pic de la crise. Il est vrai que ces transactions, insignifiantes jusqu'à l'année précédente, n'avaient jamais dépassé les 4 millions de dollars jusqu'en janvier. L'essentiel des évasions se fit par les techniques éprouvées des banques.

Mais la crise chypriote joua un rôle symbolique. On le vit dans d'autres pays dont le système bancaire pouvait susciter l'inquiétude. Les téléchargements d'applications Bitcoin firent des bonds que l'on put, pour le coup, mesurer précisément. L'une des applications vedettes passa, dans la nuit du 18 mars, de la 526e à la 52e place des plus populaires sur iPhone en Espagne [122].

C'est deux ans plus tard que fut installé le premier BTM à Athènes. Les grecs étaient alors limités à 60 euros de retraits quotidiens dans un scénario qui, différent dans son mécanisme, ressemblait fort au chypriote dans ses manifestations tangibles.

Le 28 juin 2015, Alexis Tsipras, en plein bras de fer avec les autorités européennes, avait annoncé la fermeture des banques pour une semaine et l'instauration d'un contrôle des capitaux, tout en ajoutant que « les dépôts des citoyens dans les banques grecques sont absolument garantis ». Dans les rues, les distributeurs automatiques étaient pris d'assaut.

On remarqua au passage que PayPal n'était plus disponible, ce qui donna et donne encore à réfléchir. Le même jour, le nombre de recherches du mot « bitcoin » sur le site grec de Google était multiplié par 5. De même la principale plateforme grecque déclarait avoir multiplié par 7 son flux de nouveaux clients, avec cependant une moyenne de 150 comptes ouverts par jour et un rationnement de ses clients, à 250 dollars par jour et par compte, contre 1 000 dollars auparavant [123].

Comme dans le cas de Chypre cependant, l'effet réel de la crise doit plutôt être cherché au niveau mondial qu'au niveau local où il resta marginal. Dans le cas de la Grèce, l'effet sur le cours ne peut plus être isolé. D'abord parce que l'épisode se situe après 18 mois de dégringolade presque continue depuis le pic à plus de 1 000 euros au début de 2014, ensuite parce que si à la fin juillet, alors que la Grèce semblait sortir de l'impasse, le bitcoin poursuivait néanmoins sa reprise avec une hausse de près de 25 % en un mois, nombre de commentateurs opinaient que ce qui soutenait désormais son cours, c'était peut-être plutôt le krach boursier en Chine, pays dont le rôle spécifique dans l'économie du bitcoin s'était considérablement affirmé.

Ce qui fit, cette fois, une publicité mondiale au bitcoin, même s'il s'agissait d'un canular ou d'hypothèses douteuses, fut l'idée de voir la Grèce adopter, en cas de Grexit, le bitcoin comme monnaie d'usage, ou l'idée de se doter d'une crypto-devise en cas de fermeture définitive des frontières monétaires dans le fameux « plan B ». M. Varoufákis avait pourtant dès avril 2013 réfuté sur son blog la « dangereuse fantaisie d'une monnaie apolitique ». Pour lui, la création de monnaie politiquement dirigée restait évidemment un impératif. Il avait répété en février 2014 que du point de vue grec le bitcoin avait le défaut de l'or joint à celui de l'euro. C'est cependant dans le même article qu'il émettait l'hypothèse d'un « coin » assis sur… les futures taxes. Ce FT-Coin, dont on reparla épisodiquement jusqu'à la fin de la crise grecque, n'aurait été qu'un assignat cryptographique. C'était une rodomontade.

Divers journaux plus ou moins spécialisés annoncèrent le 1er avril 2015 que la Grèce adoptait le bitcoin. Cette plaisanterie à deux sous (ou deux satoshis) arrivait après des semaines d'annonces par diverses start-ups en mal de publicité de solutions de monnaies complémentaires ou cryptographiques miracles pour « sauver la Grèce ».

Au total, la crise grecque fut sans grand effet direct sur le bitcoin, et le bitcoin sans rôle majeur durant cette crise. On peut en tirer deux leçons : Bitcoin n'est pas conçu pour un territoire donné ou circonscrit mais pour un Internet global et sans frontière. En revanche il s'inscrit mentalement dans une remise en cause d'un système fondé sur l'inflation de signes monétaires qui rappelle sa genèse rebelle inspirée par la crise mondiale des *subprimes*. Encore en 2016, la chute brutale du bolívar au Vénézuela ou le retrait inattendu des grosses coupures en Inde ont également provoqué un sursaut d'intérêt pour les plates-formes locales de change de la crypto-devise et une montée générale des cours.

On peut penser[124] qu'à chaque crise financière ou monétaire une proportion plus importante de la population se tournera vers une option perçue autant comme une protection personnelle que comme un signal de défiance vis-à-vis des institutions.

Après avoir violé le droit à Chypre, l'Union Européenne décida de le réécrire. Par la directive du 15 mai 2014 « établissant un cadre pour le redressement et la résolution des établissements de crédit » il fut décidé que les clients des banques pourraient désormais être mis à contribution. En décembre 2015 ceci était discrètement transposé dans le droit français.

Dévaluer la monnaie pour aider les banques ou le gouvernement n'était pas sans précédent. Dans le cas de Chypre, qui ne contrôlait pas sa banque centrale, la chose avait juste été faite de manière transparente et brutale, par amputation plutôt que par inflation. Les bitcoineurs font généralement partie de ceux qui perçoivent le laxisme monétaire au-delà de ses seuls effets chez l'épicier. L'inflation des actifs, la création de bulles, l'injection de liquidités sidérantes, jusqu'à l'apparition de taux d'intérêt négatifs, tous les événements qui s'enchaînent depuis la crise dite des *subprimes* conduisent à une crainte diffuse tant sur la valeur réelle des actifs monétaires que sur la sécurité et la disponibilité des dépôts bancaires.

Or 2015 fut aussi l'année d'attentats spectaculaires qui justifièrent lois d'exception, mesures de surveillance et restrictions diverses. À chaque nouvel attentat furent mis en cause à la fois les moyens de communication chiffrés, l'emploi de l'argent liquide, les cartes prépayées et… le bitcoin, qui après le commerce de la drogue se retrouva donc accusé de faciliter celui des kalachnikovs. Toute nouveauté a toujours son lot d'accusations caricaturales : il suffit de regarder les archives sur Internet, sur les jeux vidéo ou sur la télévision… Le rock et la valse en son temps furent aussi décriés comme la musique du commencement de la fin !

Les journalistes en mal de sensation ou les ministres en situation de quasi-impuissance ne furent pas les seuls à le prendre comme bouc-émissaire : dès janvier 2015, on vit la *British Bankers Association*, un lobby regroupant 230 banques, associer dans la même phrase les mots *terrorism* et *Bitcoin*… alors même que le terroriste de la porte de Vincennes s'était financé chez Cofidis.

Il en faut souvent bien peu, et quand on se donne la peine de chercher les « sources », on trouve souvent la désinformation la plus grossière[125]. Un jour des *experts* européens avancèrent pour preuve de l'implication du bitcoin dans le financement du terrorisme un document d'experts américains qui, lorsqu'on le lit, cite un document israélien, lequel suppose que des terroristes arabes pourraient le faire. Une autre fois, un article du journal dw.com cite comme source l'*EU Institute for Security Studies* qui affirme que « le don est une source de revenu principale de l'organisation (Daesh) et certains de ces dons se seraient faits en monnaie virtuelle comme le Bitcoin afin de minimiser les risques de détection ». L'auteur de l'article parle d'une adresse (qu'il ne donne pas, alors que tout est transparent) contenant 20 millions de dollars, puis, après avoir suscité de nombreuses critiques, affirme que cette information n'est pas de lui et qu'elle aurait été ajoutée à son insu.



Bitcoin « in tempore belli » (article de Jacques Favier)

Dans le même genre, un membre supposé de l'organisation anonyme *Ghost Security Group* prétend que Daesh possèderait plusieurs adresses bitcoin dont une (qu'il ne donnera pas) contenant 3 millions de dollars. Le lendemain, un autre membre supposé de l'organisation dément cette affirmation sur un réseau social et rejette la faute sur le journaliste…

Sur de telles bases, on voit à la suite de nouveaux attentats les ministres des Finances du *G7*, ainsi que les ministres de l'Intérieur et de la Justice de l'UE se pencher sur les mesures à mettre en place afin de renforcer le contrôle du financement du terrorisme par le biais des « monnaies virtuelles ».

Finalement, un rapport du 18 janvier 2016 de l'Office européen de Police (Europol) [126] constate que « malgré l'affirmation de tiers suggérant que les monnaies anonymes comme Bitcoin sont utilisées par les terroristes pour le financement de leurs activités, cette affirmation n'a pas été démontrée par la police ». En gros, Europol revient sur ses propres dires.

Au vrai, les terroristes dont parlent les médias ressemblent peu à des *geeks* et leurs commanditaires, quand il y en a, ont certainement compris (notamment au travers des affaires liées à la drogue) que l'usage du bitcoin est bien trop risqué, car bien assez transparent pour les grands services de renseignement s'ils y mettent le prix. Et puis les recrues sont souvent loin d'être des as de l'informatique et sont très souvent fichées avant un quelconque départ. Rappelons qu'Ahmadou Coulibaly avait utilisé un circuit 100 % bancaire, usant même du crédit à la consommation et non du bitcoin pour acheter ses armes.

Ce qui ressemble à une forme de délire dans les accusations portées contre le bitcoin quant au financement du terrorisme retourne s'envelopper dans un écran de fumée : le discours officiel agrège et déforme les choses. Il suffit de parler dans la même phrase de la drogue, du crime et du blanchiment. Ensuite le blanchiment porte sur tout ce qui peut déplaire aux autorités, y compris à l'état de soupçon.

Et l'on revient au cœur des choses : la réalité de la monnaie des États, fondée sur la dette, la contrainte et la surveillance. Qu'est ce qui est vraiment visé et combattu ? Les usages criminels, aussi minoritaires soient-ils, ou l'émancipation apportée par Bitcoin ?

2- Bitcoin père de toutes les cryptomonnaies

Le laboratoire des alternatives

Comme toutes les inventions géniales, Bitcoin a déclenché un élan de créativité. Cette invention étant libre de droit, beaucoup ont essayé de la reprendre, les uns en changeant juste quelques paramètres, les autres en essayant de tout réécrire. On parle de *fork* pour les modifications partielles du code. Ce procédé datant des débuts de l'informatique, très développé en regard du système d'exploitation libre GNU/Linux, a été mis en œuvre avec Bitcoin où l'on parla assez rapidement de cryptomonnaies ou d'*altcoins* (*alternative coins*).

Ainsi Bitcoin est-il le père de toutes les cryptomonnaies, qu'elles soient des *forks* ou bien des inspirations utilisant ses principes de base (P2P, cryptographie, tokens, etc.). La communauté ayant une importance capitale dans Bitcoin – un effet de réseau conséquent et une large communauté sont indispensables à tout projet décentralisé – l'IRC *bitcoin-dev* et le forum *Bitcointalk* furent les lieux essentiels de cette créativité. Ainsi en 2010 naquit l'idée d'un projet nommé *BitDNS*, permettant d'utiliser le fait d'avoir un réseau décentralisé fonctionnel pour réussir à mettre un service de DNS (*Domain Name System*) totalement décentralisé et libre. Une récompense fut même promise à celui qui trouverait la solution.

En avril 2011, un anonyme publia une solution nommée NameCoin. C'était le premier *fork* de Bitcoin : il s'appuyait sur Bitcoin pour faire un autre protocole de monnaie décentralisée, qui hébergerait sur sa blockchain un service d'adressage. Grâce à ce système, il est possible pour n'importe qui de créer un nom de domaine en « .name » sans aucune censure possible. On voit parfois des sites de téléchargements illégaux fermés parce que leur adresse est saisie par les services de police. Mais dans des pays plus autoritaires, ce sont des sites d'opposants qui peuvent être suspendus. Cela est rendu impossible avec NameCoin, de la même manière qu'il est impossible de censurer une transaction Bitcoin. Cependant, il faut que le navigateur soit compatible et intègre le protocole.

L'ambition de développer des jetons qui complètent Bitcoin en assurant un ou des services inédits qu'il n'est pas à même de rendre a permis de nombreuses innovations. Assez rapidement, dès 2011, les altcoins furent elles-aussi valorisées, du fait de leur nature semblable à Bitcoin et donc de leurs propriétés monétaires.

La boîte de Pandore était dès lors ouverte, et les altcoins allaient se multiplier à une vitesse folle. Sur les plus de 1300 monnaies décentralisées [127] créées depuis 2009, peu sont dignes d'intérêt : ce sont des copies légèrement modifiées de Bitcoin. Mais les altcoins nous ont appris que la communauté est un aspect clef de la monnaie, même décentralisée.

Pour les plus sérieuses, on va voir qu'il y a trois raisons d'un *fork* : on peut toucher aux caractéristiques économiques (masse, émission, divisibilité, etc), aux caractéristiques techniques remplaçables (changement d'algorithme) ou enfin tenter d'apporter des propriétés inédites.

On voit dès 2011 plus de neuf nouvelles cryptomonnaies [128], dont le Tenebrix, qui n'eut pas un grand succès en raison de sa nature de prototype, mais dont l'apparition est symptomatique : le minage à cette époque devenait déjà plus concurrentiel sur Bitcoin. Les développeurs cherchaient des solutions pour continuer à miner avec un ordinateur classique. La solution fut de changer l'algorithme de hashage en remplaçant le SHA-256 par le Scrypt, avec très peu d'impact sur la sécurité.

Deux forks plus tard arriva celle qu'on désigne souvent à tort comme la première altcoin : le Litecoin. Créé par un ex-ingénieur de Google, Charles Lee, l'objectif de cette cryptomonnaie peut paraître discutable : donner plus de liquidité que Bitcoin en quadruplant sa masse monétaire et plus de rapidité avec des confirmations divisées par quatre. Modifications mineures, d'autant que cette cryptomonnaie n'était même pas la première à utiliser Scrypt, mais le Litecoin a rapidement joui d'une aura : elle était au Bitcoin ce que l'argent est (ou est supposé être) à l'or. Leurs prix ont par ailleurs été très longtemps corrélés et la capitalisation de Litecoin est restée la deuxième en montant jusqu'à l'arrivée d'Ethereum. La capitalisation de Litecoin était encore, fin 2016, de plus de 190 millions de dollars et elle a connu en mars 2017 un nouveau sursaut à plus de 400 millions de dollars. [129]

Cinq forks et dix mois plus tard naissait le PeerCoin. Son créateur, répondant au pseudonyme de SunnyKing, fut le premier à trouver un algorithme de consensus alternatif, le Proof-of-Stake (que l'on peut traduire par preuve d'intérêt ou preuve d'enjeu). Cette manière de vérifier les transactions a l'avantage d'être théoriquement écologique, car les transactions ne sont pas vérifiées par des calculs qui requièrent une puissance considérable mais par la possession de jetons avec un nœud en marche. Celui qui a le droit de valider est plus ou moins tiré au sort en proportion de la part de la monnaie qu'il possède. Bien que l'écologie soit utilisée contre Bitcoin comme un argument récurrent, il faut bien comprendre que le fait de ne pas dépenser d'énergie rend la blockchain en question plus sensible aux attaques de réécriture. Les hash ne sont plus, dans ce cas, le résultat d'un concours d'itérations mais dépendent du poids monétaire du réseau et ne sont donc pas aussi difficiles à résoudre que ceux du Bitcoin. La sécurité des monnaies PoS est donc encore très controversée, notamment en ce qui concerne l'immuabilité des transactions. De plus, il semble intuitivement plus facile de réussir à obtenir la majorité consensuelle du réseau en achetant la moitié des jetons plutôt qu'en essayant de s'emparer de la moitié de la puissance de calcul. Le Peercoin était d'ailleurs un hybride, couplé avec du PoW, ce qui réduit considérablement son intérêt écologique.

On vit aussi, en 2011, l'arrivée du Freicoin, qui se conduisait comme une monnaie à valeur fondante selon une idée théorisée en 1916 par Silvio Gesell.

De quoi dépendent en pratique la survie ou la mort de pareilles altcoins ? De plusieurs paramètres qui sont le nombre de nœuds (tant qu'il y'en a deux, la monnaie est « cliniquement » vivante), l'activité de la communauté et des développeurs et enfin leur attractivité sur les marchés (facteur qui dépend des trois premiers.)

En ce qui concerne les nœuds, c'est une problématique à laquelle doivent faire face toutes les cryptomonnaies, et c'est pour cela qu'on peut considérer que Bitcoin est la plus solide. Mais des monnaies peuvent arriver à des capitalisations supérieures à 1 million de dollars avec seulement quelques dizaines de nœuds. De toute manière, si gain d'attractivité il y a, on constate mécaniquement une hausse du nombre des nœuds.

La communauté est primordiale, c'est par elle que tout commence et elle va souvent assurer le marketing de la monnaie. Sans communauté, il est vraiment difficile d'avoir une adoption. Curieusement, on voit des altcoins perdurer plus de cinq ans, sans spécificités exceptionnelles, sans réelle activité monétaire ou financière,

uniquement en raison de leur communauté. Beaucoup de ces altcoins ont été la porte d'entrée dans la cryptosphère pour un grand nombre d'individus qui peuvent y attacher une valeur affective. Peut-être verrons-nous un jour une archéologie de toutes ces monnaies décentralisées avec des nœuds installés dans des musées.

L'activité des développeurs est interdépendante de la communauté : c'est aussi la communauté qui est au cœur du recrutement. Elle est à la racine des améliorations, des propositions nouvelles et des développements annexes comme des modules de paiement à destination des sites de e-commerce ou autre. On voit maintenant des altcoins soutenues par des sociétés, ce qui change la donne mais pourrait donner lieu (vu que le code est normalement libre) à un clone de l'altcoin en question maintenu par une communauté indépendante.

Enfin, les échanges sont indispensables à l'adoption de la monnaie. C'est bien souvent quand elles prennent de la valeur que les altcoins font parler d'elles. Au début, les plateformes avaient fait le choix de permettre de faire des paires en monnaies fiduciaires et en bitcoin. Rapidement, il s'est avéré qu'il était plus commode de « trader » uniquement en bitcoin, surtout avec l'arrivée de plateforme sans euro ni dollar, ne faisant que des paires en bitcoin et se nichant en outre dans un relatif vide juridique. Ainsi naquirent *Bter* (plateforme chinoise) puis Poloniex (la plus active), *Mintpal* (l'ex plus active, mais rachetée pour être dépouillée et fermée) et *Bittrex*. Tout cela génère des volumes parfois considérables, allant sur des grosses journées jusqu'à 100 000 bitcoins échangés. Ce sont ces plateformes qui ont contribué en grande partie à faire de Bitcoin la monnaie étalon des cryptomonnaies.

Reprenons ici notre tour d'horizon. En 2013 naquirent plus d'une cinquantaine d'altcoins dont certaines vraiment innovantes et reflétant des désirs et mécanismes nouveaux.

RipplePay, une entreprise fondée des années plus tôt et qui avait mis en place un système de services financiers à l'échelle mondiale, avec l'ambition de créer un réseau international d'échange de valeur Ripple, créa en mai 2011 un système de monnaie numérique, inspiré de Bitcoin, dont le consensus ne reposait pas sur une preuve de travail mais sur une toile de confiance restrictive. On peut dire que la blockchain de cette monnaie est restrictive (*permissive*) car tous les utilisateurs ne peuvent pas jouer le rôle de mineurs validateurs. De ce fait, le réseau est certes plus rapide, mais on peut le considérer comme moins fiable. De plus, il est généralement discrédité parce que sa monnaie a été « préminée » : tous les jetons ont été créés d'un coup et sont distribués gratuitement ou vendus au fur et à mesure sur les marchés, sachant que les créateurs ont conservé 20 % de la masse monétaire globale.

Ripple se veut une monnaie passerelle, permettant l'émulation de n'importe quelle monnaie ou valeur. Altcoin un peu particulière, les banques l'ont rapidement appréciée pour son aspect fermé et contrôlable. On peut objecter qu'il ne s'agit en fait que d'une simple base de donnée distribuée privée classique sans réelle innovation, mais l'engouement reste fort chez les banquiers : beaucoup la testent et l'implémentent comme *UBS*, *Unicredit* ou *Santander*. La capitalisation du jeton de Ripple s'établit au printemps 2017 autour d'un milliard de dollars.

L'année 2013 fut aussi celle de la naissance du ByteCoin, monnaie utilisant CryptoNight, un nouvel algorithme de hashage tranchant radicalement avec celui de Bitcoin, car résistant à l'extraordinaire puissance de calcul des ASIC (*application-specific integrated circuit*). Il est implémenté dans le protocole qui fonctionne à l'aide de signature de Cercle. C'est un algorithme de hashage bien plus jeune, ce qui est assez mal considéré dans la cryptographie où l'on a tendance à choisir les algorithmes les plus éprouvés, mais qui a l'avantage de permettre un minage plus égalitaire et (par la signature de cercle) un anonymat total. C'est une chose qui sera bien exploitée par son *fork* Monero dont nous reparlerons.

Vinrent également la même année GridCoin et PrimeCoin, qui essayaient de pallier le supposé gaspillage de puissance de calcul de Bitcoin. Le PrimeCoin utilise un mécanisme de preuve de travail utilisant des algorithmes différents qui permettent de trouver des nombres premiers à l'aide de chaînes de Cunningham. C'est une belle avancée, qui montre qu'il serait possible de sécuriser la monnaie tout en effectuant une tâche de calcul « utile ».

Le GridCoin fut encore plus ambitieux car il voulait permettre le calcul parallèle tout en sécurisant la monnaie à l'aide de BOINC (*Berkeley Open Infrastructure For Network Computing*) qui permet notamment le déchiffrage des signaux écoutés par le programme SETI ou bien le séquençage d'Ebola. Son algorithme de consensus est une hybridation entre la simple preuve d'enjeu et la « preuve de BOINC », un système permettant de récompenser les mineurs en fonction de la puissance de calcul attribuée au réseau BOINC.

La même année naquit une monnaie qui devait percer le mur des médias traditionnels : le Dogecoin, monnaie purement communautaire basée sur le charme d'une image à diffusion virale sur Internet, un « mème »

celle d'un chien Shiba Inu nommé *Doge*. Cela peut sembler absurde. Mais la communauté de cette monnaie était si importante que cela créa très vite une infrastructure de services assez impressionnante. Dogecoin devint très populaire alors qu'elle n'avait rien de spécial : c'était juste une copie du Litecoin, avec une création en perpétuelle inflation (choisie a posteriori par un fork) ! Elle se nicha pourtant quelques jours juste derrière Bitcoin en termes de capitalisation de marché. Sa capitalisation était encore, fin 2016, d'une vingtaine de millions de dollars et elle connut un rebond en mars 2017, à plus d'une quarantaine de millions de dollars.

L'année 2013 vit également naître le premier jeton en surcouche de Bitcoin. Le Mastercoin est intrinsèquement lié à Bitcoin, puisqu'il est émis sur une plateforme en surcouche permettant elle-même d'accueillir des protocoles décentralisés comme Maidsafe ou Factom. Cette altcoin marqua l'histoire en étant l'objet de l'une des premières *Crowdsale* ou *Initial Coin Offering* (ICO) permettant d'acheter en Bitcoin les premiers jetons distribués, et l'opération leva ainsi plus de 5 000 bitcoins valant à l'époque 500 000 $. Cet exemple montre aussi que les altcoins ne sont pas nécessairement de nouvelles cryptomonnaies avec leur propre blockchain mais peuvent aussi utiliser la blockchain de Bitcoin comme noyau, avec cependant des applications limitées.

Le phénomène d'ICO s'est rapidement développé. Il y eut notamment à l'été 2014 celle d'Ethereum qui leva 18 millions de dollars en bitcoin [130] et dont la valorisation dépasse au printemps 2017 les 4 milliards de dollars. Il y eut aussi l'ICO de NXT, valorisée fin avril 2017 autour de 15 millions de dollars et qui n'avait alors levé que 7 000 dollars en bitcoin [131].

Le bitcoin, malgré sa volatilité jugée excessive à l'extérieur de la communauté, est considéré comme plutôt stable en terme de prix par la majorité de ses utilisateurs et les altcoins ont, elles, eu des volatilités complètement folles allant parfois jusqu'à 15 000 %. De ce fait, un véritable marché s'est développé avec évidemment son lot d'arnaques, de levées de fonds frauduleuses ou des jetons préminés cachés par le protocole. La prudence est de mise dans le monde des altcoins et il vaut mieux être un minimum expérimenté avant de s'y lancer. Toutefois il est intéressant de constater la capacité d'autofinancement du monde des méta-monnaies, aidée par la fluidité et la sécurité du Bitcoin. Il est très facile de lever des sommes considérables d'argent, car tout est plus facile qu'une levée de fonds ou une entrée en Bourse classique. Par exemple, sur les trois premiers trimestres de 2016, plus de 200 millions de dollars ont été levés dans la cryptosphère en bitcoins (moins de 1 % en ether) face aux 376 millions de dollars par les circuits classiques de l'investissement. [132] C'est ce qui explique la prolifération croissante des altcoins, avec tout de même un ralentissement après 2014-2015 (plus de 300 nouvelles monnaies.). Aujourd'hui il existe plus de 675 monnaies cotées [133].

Concluons ce tour d'horizon par une rapide typologie. Il y a les monnaies non novatrices (les *shitcoins*), ou les monnaies pour rire comme le LuckyCoin (avec une création monétaire aléatoire à chaque bloc). Il y a aussi des monnaies représentant de nouveaux noyaux, comme Bitcoin, et qui sont des refontes complètes fondées sur d'autres systèmes. Nous avons vu Ripple, mais il y a aussi NXT, créée en 2014 par l'anonyme BCnext et qui propose directement dans son *wallet* de voter, de vendre des objets, de créer des actifs cryptographiques et de les échanger et une multitude d'autres services. Il y a enfin Ethereum que tout le monde connait depuis que la grande presse a présenté son ether comme la monnaie qui allait ringardiser Bitcoin : c'est un protocole de type dit « *Turing complete* » qui permet une liberté totale de code sur sa blockchain. Le projet créé par le jeune génie Vitalik Buterin en 2015 vise ni plus ni moins qu'à être un « ordinateur-monde ». La capitalisation de sa monnaie, l'ether, est la seconde derrière celle du bitcoin, et cette monnaie est encensée par tous les détracteurs de Bitcoin et par les amateurs de la « technologie blockchain ».

On peut aussi nommer Monero, valorisée à près de 300 millions de dollars en avril 2017, la seule cryptomonnaie véritablement anonyme grâce à la technologie *CryptoNote* et dont la force réside dans le fait que tout le monde étant obligé d'être anonyme sur son réseau, il n'y a pas de fuite d'informations possibles.

Plus récemment il y a eu Zcash, dont les méthodes sont discutables, car ils récupèrent temporairement une partie des fruits du minage et certaines zones du code ne sont pas libres et transparentes. Le projet paraît bancal car il n'est pas obligatoire d'être anonyme sur son réseau, ce qui fait que l'anonymat des uns peut être compromis par les non-anonymes. [134] Enfin on peut aussi nommer BitShares, un système à preuve de participation avec des délégués élus au nombre de 101. Cela permet de résoudre de nombreux problèmes de mise à l'échelle et d'avoir pour son offre d'applications des outils permettant une mise en place plus facile. Cette monnaie est valorisée aujourd'hui à 70 millions.

Enfin il y a les altcoins qui ont réellement un usage précis. On pourra citer celles qui ambitionnent d'être des plateformes de cloud décentralisées comme StorJ ou SiaCoin, valorisées à 10 et 15 millions. Chacun peut obtenir des jetons en fournissant une partie de son disque dur à ces réseaux. On peut aussi citer celles prônant l'anonymat comme Dash, valorisé à près de 500 millions de dollars (en avril 2017) bien que souffrant de problèmes d'architecture en ce qui concerne l'anonymat ; Monero, Zcash ou ShadowCash qui utilise aussi la signature de cercle sans être *CryptoNote*.

Il y a le jeton de la plateforme de marché prédictif, Augur, valorisée à 120 millions et fonctionnant comme un jeton sur Ethereum. Des monnaies dédiées au notariat comme Factom, valorisée à 379 millions, ou Stratis, valorisée à 41 millions. Des monnaies voulant être la base de réseaux sociaux comme Steem, dont la valorisation était montée jusqu'à 300 millions de valorisation avant de redescendre à 16 millions, ou Synéreo valorisée à 6 millions à la fin de 2016 (et le double en avril 2017).

Début 2017 le marché des altcoins a trouvé une seconde jeunesse avec des capitalisations en hausse comme on vient d'en dresser le constat. L'histoire semble se répéter car la même folie des altcoins eut lieu en 2014 après la hausse du bitcoin et le regain d'intérêt pour celui-ci. À l'époque on invoquait comme raison le fait que les altcoins semblaient plus accessibles psychologiquement aux nouveaux-entrants. Comprendre ici que lors d'un achat de 100 euros il est impossible d'avoir plusieurs bitcoins mais uniquement une fraction alors que les altcoins vont souvent permettre de s'affranchir de cette limite en ayant des dizaines voire des milliers d'unités pour la même somme. De nos jours la raison invoquée est la congestion du réseau Bitcoin : ceux qui utilisent vraiment bitcoin pour payer seraient embêtés par les frais et se verraient obligés de passer par des réseaux secondaires. Cette hypothèse de la nécessité par l'usage doit être prise avec des pincettes et il est tout à fait possible que nous soyons aussi dans une sorte de ruissellement à la Reagan version 2.0. Ceux qui s'enrichissent avec le bitcoin quand son cours monte choisissent de vendre avec parcimonie et diversifient leurs actifs en altcoins, faisant alors monter mécaniquement celles-ci tout en faisant une petite part d'ombre à Bitcoin au sein de ce marché. Cela semble montrer en tout cas que les acteurs ne sortent pas nécessairement du marché bitcoin en monnaies classiques mais plutôt en altcoins, la capitalisation cumulée de toutes les crypto-monnaies, elle, ne cessant d'augmenter.



Bitcoin et Altcoins, les cours en temps réel (expérience)

Le lecteur l'aura compris, les altcoins sont un laboratoire infernal. Parfois des conceptions échouent, d'autres fonctionnent mais sans jamais avoir d'impact direct sur Bitcoin et son code. C'est leur principale qualité : il est très difficile de changer un protocole, alors pour innover il faut proposer d'autres monnaies, et certaines ont essuyé des plâtres. En terme de valorisation, elles ont oscillé pendant très longtemps entre 5 % et 25 % de la capitalisation totale des cryptomonnaies. Cependant nous devons souligner que ce chiffre est en avril 2017 aux alentours de 30 % en raison de la hausse globale des altcoins et surtout de la forte hausse d'Ethereum. Pic temporaire ou non, seule l'histoire nous le dira. Il nous semble difficile de dégager une tendance avec si peu de recul. Quoi qu'il en soit, ces chiffres montrent bien la supériorité de Bitcoin dans cet écosystème, et en tant qu'étalon. Cette diversité parfois un peu loufoque, voire marquée par des tentatives de réinventer la roue, semble cependant bénéfique et nécessaire à l'écosystème. L'avantage de celui-ci est sa capacité d'autofinancement. Le but est désormais de réussir à concentrer les efforts sur Bitcoin à l'aide de nouveaux protocoles en surcouche du protocole Bitcoin et fonctionnant grâce à des mises à jour de ce dernier comme les sidechains et le réseau Lightning dont il va être question d'abord pour les problèmes qu'il peut résoudre puis pour décrire son fonctionnement.

Le « code » : un texte sacré

Changer un protocole est loin d'être une mince affaire, surtout quand celui-ci comporte un enjeu monétaire. Pour Bitcoin, il y a une difficulté supplémentaire : il est totalement décentralisé et n'a pas de leader depuis que son

créateur anonyme a disparu en 2011, bien qu'il ait en quelque sorte désigné Gavin Andresen comme son successeur.

Depuis ses débuts, Bitcoin n'a cessé d'être amélioré sur différents points [135]. Cependant une mise à jour y est plus compliquée qu'une mise à jour de protocole classique, qu'il s'agisse de ce que l'on appelle un *soft fork* (ou embranchement doux), à savoir une mise à jour qui change des paramètres réduits et qui ne compromet par la compatibilité entre la nouvelle et l'ancienne version, ou de ce que l'on nomme un *hard fork* (ou embranchement dur), à savoir une mise à jour qui change des paramètres généralement plus capitaux (taille des blocs, masse monétaire ou autre) et qui fait que les différentes versions ne seront plus compatibles entre elles. Beaucoup de *soft forks* ont déjà eu lieu dans Bitcoin sans aucun problème. En revanche il n'y a pas eu beaucoup de *hard forks*. [136]

Comme il n'y a pas de leader dans Bitcoin, les décisions doivent être prises de manière démocratique. Personne ne peut imposer sa vision. Par l'essence même de la blockchain, il serait possible que la blockchain de Bitcoin se scinde un jour en deux lors d'un *hard fork*. Ce risque est dû au mécanisme de sécurité du Bitcoin, qui fait que la chaîne la plus longue l'emporte. Dans le cas d'un *hard fork*, comme les deux protocoles ne seraient plus compatibles, si la communauté était réellement divisée, deux systèmes pourraient se mettre à coexister. Si l'on se représente la Blockchain comme une route linéaire, il faut voir le moment d'un *hard fork* comme une patte d'oie. Si différents mineurs restaient en concurrence sur les deux nouvelles sections de blockchain, ils deviendraient totalement indépendants les uns des autres. Dans ce cas, les deux chaînes partageraient un passé commun jusqu'à l'instant du *fork*. Une autre conséquence, un peu étrange, c'est que les bitcoins seraient dédoublés : il y aurait désormais des bitcoins de l'ancien protocole sur une chaîne et des bitcoins du nouveau protocole sur l'autre. Autant dire que ce n'est pas un scénario enviable.

Ce genre de *fork* durable s'est pourtant produit dans l'histoire des cryptomonnaies, avec un cas célèbre qui fait qu'il existe depuis l'été 2016 deux chaînes d'Ethereum [137]. Il est difficile de résumer simplement l'affaire, tant pour ses circonstances que pour son dénouement. Un « contrat intelligent » sur Ethereum, destiné à financer une sorte de véhicule d'investissement à organisation autonome et décentralisée (*TheDAO*) avait été mal codé. Ce *bug*, repéré peut-être par un proche, a permis un détournement d'ethers équivalent à 60 millions de dollars. Plutôt que d'admettre le *bug* et la perte, la communauté Ethereum s'est majoritairement décidée en faveur d'un *fork* permettant de rendre sans effet l'opération frauduleuse.

Ce *fork* permettant de facto de réécrire l'histoire a cependant été considéré par une minorité agissante comme une véritable hérésie vis-à-vis de l'essence même des cryptomonnaies qui sont linéaires, fiables, infalsifiables, éternelles et incensurables.

De ce fait si la version majoritaire d'Ethereum a suivi le fork, certains nœuds continuent de faire tourner la blockchain d'origine, et il y a donc deux versions de l'ether cotées depuis l'été 2016. On peut penser que la résistance s'épuisera (le cours de l'éther dit « classique » n'excédant pas 10 % de l'autre) mais les conséquences sont lourdes pour la (double) communauté et pour son image.

Une des raisons de la situation a été la puissance de la fondation Ethereum qui, même si son leader Vitalik est resté assez discret, a tout de même clairement penché vers le *fork*, influençant forcément l'opinion. La vérité est qu'il y avait dans cette affaire beaucoup d'argent en jeu, y compris d'énormes sommes appartenant aux développeurs, et que cette aventure a fait ressortir d'importants clivages philosophiques entre Ethereum et Bitcoin.

Bitcoin, quant à lui, fait face depuis ses débuts à divers problèmes d'ordre économique, sociologique, politique ou autre. L'absence du fondateur fait que leur résolution peut paraître lente.

Il y a le problème de la consommation d'énergie : très rapidement, des développeurs ont fait en sorte que Bitcoin en consomme le moins possible, ou du moins de façon optimisée, et plusieurs idées d'adaptation du protocole ont aussi été émises.

Il y a ensuite le problème du délai d'attente des transactions. Un bloc Bitcoin est censé mettre 10 minutes à être validé. Cependant, avec un réajustement tous les 15 jours et une puissance de calcul sur le réseau assez variable, la régularité des blocs laisse parfois à désirer. Ce problème n'est pour l'instant guère abordé car il reste mineur par rapport à d'autres. D'autres cryptomonnaies l'ont corrigé et Bitcoin le fera peut-être un jour. Mais réduire le temps de confirmation à la façon de Litecoin est inutile, car l'assurance d'avoir une transaction valide demande alors plus de profondeur. Bitcoin est sur le point de résoudre ce problème avec l'intégration d'alertes à la

double dépense par les différents portefeuilles qui permettent d'avertir en moins de 30 secondes s'il y a un doute possible sur la transaction, ou bien grâce au réseau Lightning.

Viennent ensuite les problèmes du pseudonymat. L'idée de Bitcoin était tout de même de jouer le rôle du cash électronique. De ce fait, sa non-fongibilité est devenue un problème qu'on ne peut éluder. Pour beaucoup, Bitcoin se doit donc d'être anonyme et c'est même comme cela qu'il a été imaginé. Il existe quelques pistes que nous n'allons pas décrire ici et l'anonymisation a déjà été assez brillamment résolue par les monnaies *cryptonote* comme Monero. À cet égard, le lecteur peut commencer à se demander pourquoi Bitcoin n'adopte pas les améliorations des autres cryptomonnaies. Mais ces modifications profondes de Bitcoin, qui demanderaient beaucoup d'expertise technique, seraient *de facto* plus dures à faire accepter dans un consensus général pour éviter un *fork* de la blockchain. En outre, les gens travaillant sur Bitcoin avec une expertise technique suffisante sont en nombre relativement limité. Les *sidechains* pourraient résoudre éventuellement ce problème.

Le nombre de nœuds du réseau Bitcoin constitue un autre problème. Ceux-ci sont en 2016 au nombre de 6 000 dans le monde entier [138]. Cela veut dire qu'il y a 6 000 relais de Bitcoin et 6 000 copies du protocole et de la blockchain dans le monde. Il serait important que, si Bitcoin croît, le nombre des nœuds croisse aussi, tout en gardant un niveau de qualité élevé en fonction de la bande passante, de la puissance de l'ordinateur et de sa capacité de stockage. Mais personne n'a intérêt au quotidien à gérer un nœud complet, car ceux-ci sont des portefeuilles bien moins pratiques d'usage pour le moment. De ce fait, les nœuds sont entretenus actuellement par des militants indépendants et des entreprises du secteur. Le problème est que cela ne laisse pas beaucoup de marge d'erreur et dans une certaine mesure la solution serait d'avoir une concurrence et un système de récompense similaire au minage. Certes c'est impossible pour l'instant car les nœuds ne produisent pas de preuves de travail et pourraient donc effectuer des attaques de Sybil, mais on peut penser qu'une rémunération deviendra possible s'il s'avère extrêmement cher d'entretenir un nœud.

Le problème suivant, celui de la divisibilité et des unités de compte, est largement un faux problème : quand bien même Bitcoin vaudrait plus d'un million de dollars et que ses décimales seraient insuffisantes, il suffirait, même si c'est peut-être plus compliqué que certains ne le disent, de faire une évolution du code vers plus de divisibilité, et il n'y aurait aucune raison que cela ne soit pas accepté par le consensus décentralisé. Mais cela peut aussi être résolu avec Lightning qui peut permettre l'exécution de transactions inférieures à 1 satoshi.

Le problème dit de « l'attaque de 51 % », par un pool de « mineurs égoïstes » qui prendrait le contrôle de plus de la moitié de la puissance de calcul du réseau, ou encore de l'attaque « Goldfinger » visant à détruire le système (sans nécessairement s'emparer de sa valeur), est assez illusoire en termes monétaires, même s'il reste dans les moyens de certains riches « ennemis » comme des États ou des GAFAM. Cependant, ce risque qui, comme tous les risques d'attaque contre la blockchain, fait l'objet d'abondantes études [139], est assez improbable car la blockchain est suffisamment transparente pour que tout le monde voie les malversations. L'attaque serait extrêmement dure à réaliser par surprise et à mener dans un laps de temps de 10 minutes.



Une épée de Damoclès sur Bitcoin (article de Jean-Paul Delahaye)

Enfin, la communauté, qui vit avec l'idée qu'une attaque pourrait se produire, a développé diverses stratégies de réaction et des mesures de sauvegarde. Moins massive que l'attaque « 51% », l'attaque *éclipse* a également fait l'objet d'une réflexion approfondie [140].

En revanche, la centralisation du minage par les pools est un problème d'un point de vue démocratique car il n'est plus possible aujourd'hui en étant un non-professionnel de miner à une échelle raisonnable. Les mineurs ont le pouvoir sur l'application des mises à jour du protocole, malgré le savant équilibre entre eux et le reste de l'écosystème. L'autre problème de cette centralisation est physique et politique, en raison de l'attractivité de la Chine pour ce qui est du prix de l'énergie autant que de l'assemblage. Ainsi la quasi totalité du minage industriel est aujourd'hui situé en Chine, à la possible merci des sautes d'humeur du gouvernement chinois. De même en ce

qui concerne les brevets et les constructeurs d'ASIC qui sont aussi tous chinois de nos jours. Bien que des fonds étrangers soient présents dans le capial de ces mineurs ou de ces fabriquants, cela demeure un problème quant à l'ambition de décentralisation qui est celle de Bitcoin. Plusieurs altcoins ont essayé de garder une certaine équité dans le minage en empêchant le minage spécialisé à l'aide d'algorithmes insensibles aux ASIC. Une autre solution serait de donner le droit de vote aux nœuds, mais de nouveau ils ne produisent pas de preuve de travail et les nœuds honnêtes seraient exposés à l'attaque de Sybil. Ce problème est donc partiellement résolu par la structure même de Bitcoin et son écosystème.

Un autre problème s'est fait jour progressivement : celui de la taille de la blockchain, taille croissante, voire exponentielle si la limite de la taille des blocs est elle-même changée. Pour cela il existe de nombreuses solutions et idées. Tout d'abord, il y a des compressions plus grandes des données et des signatures, comme la méthode dite des signatures de Schnorr [141] qui ont aussi l'avantage de protéger un peu plus les données privées. Autre solution : écrire des données à l'extérieur de la blockchain en *off-chain*. Cela pourra être fait grâce au réseau Lightning. On trouve aussi des techniques d'optimisation de la lecture de la blockchain que nous ne détaillerons pas ici mais qui pourraient permettre à n'importe qui d'installer un nœud complet très facilement sans avoir une blockchain d'une taille conséquente. Cependant, même avec ces solutions théoriques, ce problème n'a pas été résolu et il a été dans la pratique mis de côté du fait de celui sur la taille des blocs.

Cela induit le problème de la *scalability*, de la mise à l'échelle. C'est le fait que le système Bitcoin puisse fonctionner correctement à très grande échelle en termes d'utilisation. On entend parfois mentionner l'objectif de pouvoir gérer le même nombre de transactions par seconde que Visa, soit 2000 en moyenne. Alors que, pour l'instant, avec la taille d'un bloc fixée à 1 MB (mégabyte = 1 000 000 bytes) sur le réseau Bitcoin, avant Lightning ou une taille agrandie des blocs, le nombre de transactions par seconde est limité à 7 en moyenne. Au début de Bitcoin, en 2010, le réseau a été victime d'attaques dites de *spam*, qui consistent en l'envoi de milliers de transactions en continu de sorte à faire saturer le réseau. Pour pallier cela Satoshi Nakamoto brida la taille des blocs à 1 MB [142]. De cette manière, les mineurs ont commencé à prendre des frais de transactions et seules les transactions avec le plus de frais allaient être traitées. Cela deviendrait donc coûteux à un attaquant. Bien sûr, ce problème est né très tôt, mais c'est en 2015, lorsque le réseau commence à voir ses premiers blocs saturés que Gavin Andresen et Mike Hearn, deux développeurs historiques de Bitcoin, proposèrent une nouvelle version du protocole Bitcoin, nommé Bitcoin XT, où la limite de bloc passerait à 8 MB en 2016 puis doublerait chaque année. Cette proposition provoqua un véritable tollé. On vit la nouvelle abordée dans les médias généralistes qui se repaissent de n'importe quelle polémique sur Bitcoin.

Plutôt que de critiquer ces tâtonnements, on peut voir énormément de positif dans ces démarches : Bitcoin est véritablement une démocratie active. Du fait du processus de consensus décentralisé et de l'impératif du prix qui dépend de tout le monde et non uniquement des mineurs, on échange avant de trouver un accord sur la résolution d'un problème.

Mais le conflit sur la mise à l'échelle a plus ou moins suscité des clans au sein des développeurs Bitcoin, qui n'ont personne vers qui se tourner. Gavin Andresen déclara à la fois que « l'argument d'autorité est ici invalide » [143], quel que soit le respect dû à Satoshi, mais que la fidélité à l'idéal créateur est extrêmement importante. Quand on perd le créateur ou le leader, arrive un temps où ses successeurs s'approchent de la glose religieuse. On cita régulièrement sur les forums où les réseaux diverses citations de Satoshi appuyant l'assertion qu'il était pour un camp ou pour l'autre.

La proposition de protocole Bitcoin XT n'a pas fonctionné, elle n'a guère été très adoptée. Désormais, au début 2017, on compte 4 propositions de Bitcoin assez fortes [144] : Bitcoin Core, le logiciel héritier qui compte une équipe de trois mainteneurs et de 14 contributeurs anonymes ou non, soutenus par les mineurs chinois notamment et bitcoin.org (85 % des nœuds) ; Bitcoin Classic qui prône un passage à 2 MB, maintenu et développé par une équipe d'une dizaine de personnes dont Gavin Andresen et Jeff Garzik (2 % des nœuds) ; Bitcoin Unlimited avec une trentaine de volontaires menés par Andrew Stones, qui supprime la limite de taille et la remplace par un vote dynamique des mineurs, soutenu par Roger Ver de bitcoin.com (11 % des nœuds) ; et enfin Bitcoin XT tout de même soutenu par de grosses entreprises du secteur (0,5 %) mais sans Mike Hearn, qui fit en 2016 un véritable fiasco en sortant de l'écosystème par dépit tout en écrivant un article rageur contenant la phrase : « Why has Bitcoin failed ? » [145] qui fit le tour de la toile.

Au total, tout avance très lentement par peur d'un *fork* malencontreux. Cela a fait prendre conscience à tout le monde de l'horizontalité du réseau, et donc de la nécessité de la discussion pour arriver à une solution. Il

semblerait que la communauté Bitcoin soit plus dans une logique de faire les choses avec parcimonie pour que tout reste stable, même si le début de l'année 2017 a pu montrer le pouvoir des sociétés de minage avec des prises de positions risquées et parfois assumées. Or il est évident que les mineurs ne peuvent jouer seuls, car leur revenu est dépendant de la réussite de Bitcoin sur un plan général. Pour tenter soit de trouver un consensus, soit de faire un passage en force, de nombreuses autres solutions sont et ont été proposées comme le UASF (*User Activated Soft Fork*). Cette solution permettrait aux plateformes d'échange et aux portefeuilles de jouer un rôle encore plus grand dans le rapport de force. Encore une fois, nous ne pouvons tout détailler ici en raison de la nature changeante et complexe des propositions d'améliorations de Bitcoin.

Il faut tout de même énoncer ici quelques arguments des deux clans, *big blockist* et *small blockist*. Pour résumer, l'agrandissement de la taille des blocs avantage les mineurs ayant beaucoup d'infrastructure et un excellent accès à Internet (ce qui n'est pas forcement le cas des chinois) car il augmente théoriquement leur revenu par bloc du fait du nombre croissant de transactions, mais c'est discutable. Il est bénéfique pour l'adoption de masse de Bitcoin, mais aussi pour laisser le consensus de la taille des blocs aux mineurs sans pour autant faire des *hard forks* par la suite. Cela donne aussi des blocs moins censurés (parce que non-surchargés) car tout le monde pourrait y être inclus. Il faut néanmoins garder en tête le fait que le pouvoir au sujet de la taille des blocs est alors laissé aux mineurs.

Mais des blocs réduits pourraient aussi créer davantage de revenus pour les mineurs, en raison d'une concurrence pour entrer dans la blockchain, et donc de frais plus élevés. Cela permettrait à Bitcoin de valider son statut d'or numérique et de réserve de valeur : rare et cher, mais transportable. Enfin des blocs plus petits empêcheraient la centralisation excessive causée par l'injustice matérielle et infrastructurelle. Bref ce débat est encore en cours et ce problème pourra être résolu avec la surcouche Lightning, les sidechains ou une autre alternative. Nous avons pris ici le parti de Lightning, non de manière prophétique, mais parce que c'est la solution qui semble la plus aboutie, largement plébiscitée par les autorités scientifiques ainsi qu'au sein de la communauté. Celle-ci pourra en outre être accolée à de nombreuses autres améliorations comme MimbleWimble, que nous ne pouvons pas raisonnablement énumérer et expliquer dans cet ouvrage qui se veut certes complet mais qui souhaite rester généraliste et accessible.

Nous souhaitons pour terminer aborder trois problèmes qui, pour l'instant, ont été un peu mis de côté.

D'abord la rémunération par création monétaire, qui va baisser jusqu'à atteindre zéro. Il va falloir que le cours du bitcoin augmente énormément ou qu'un marché de frais de transactions rentables se développe pour que les mineurs continuent d'être incités [146].

Ensuite les bitcoins de Satoshi, perdus ou endormis. Certains seraient favorables à un recyclage des bitcoins après une très longue période sans mouvement, pour reprendre les bitcoins dont les clefs sont perdues et inciter Satoshi à bouger les siens.

Enfin la difficulté du protocole Bitcoin, écrit dans un langage moins attrayant que d'autres plus modernes comme celui d'Ethereum, ce qui rend Bitcoin très peu attractif pour les développeurs. À ce propos des nœuds de Bitcoin complets écrits dans d'autres langages et ne changeant rien à sa structure existent déjà, comme Bitcore de Bitpay qui permet aux développeurs d'utiliser des API Bitcoin plus facilement (2 % des nœuds) ou bien Btcd, une version de nœud écrite en Go qui est le langage populaire lancé par Google. Cette difficulté pourra aussi être arrangée par le projet Rootstock qui devrait permettre la même flexibilité qu'Ethereum tout en étant rattaché à Bitcoin.

Nous le voyons, Bitcoin est fondamentalement une communauté, même en ce qui concerne son code. Tout le monde est concerné et il faut donc trouver des solutions qui conviennent à une large majorité. Toutes les décisions sont prises après de longues discussions et de très nombreux tests. Bitcoin est déjà plus ou moins responsable et ne peut pas se permettre de subir le schisme d'un *hard fork*. Motivés par l'envie de faire progresser Bitcoin comme un noyau ouvert, les développeurs trouvent tout de même des façons de le développer sans pour autant prendre de risques. Nous allons voir tout de suite ces jeunes ou futures implémentations qui offrent de nombreuses possibilités et solutions.

Bitcoin effleure le monde réel

Bitcoin est déjà riche de possibilités et devrait l'être encore davantage. Parlons dans un premier temps de la représentation d'un actif tangible par un actif numérique à l'aide des *colored coins* que nous avons évoqués dans le point II, 1. Grâce à cette surcouche, on peut créer des *assets* (fonds) en émettant des jetons de même nature, mais différenciés et identifiables sur la blockchain Bitcoin. De cette manière il est possible, comme nous l'avons dit, de *représenter* des actions ou d'autres actifs tangibles même si le lien est difficile à créer.

Au-delà, il est possible d'émuler assez facilement, voire de remplacer les monnaies privées qui sont déjà en circulation comme les *miles* ou les points de fidélité valables chez certaines enseignes. L'avantage de ces actifs, c'est qu'ils sont déjà numériques, il est donc possible de les remplacer intégralement par des *colored coins* pour que ceux-ci bénéficient de la fiabilité, de la fluidité et de la sécurité de Bitcoin.

On sait aussi que de nombreuses institutions financières ou boursières aimeraient utiliser une blockchain pour représenter ou tracer leurs transactions : les *colored coins* semblent encore ici représenter une solution. Et tout cela est d'ores et déjà possible avec Bitcoin et à très faible coût. Mais l'idéal serait de pouvoir représenter les actuelles monnaies non-programmables dans la blockchain, à défaut d'y émettre leurs remplaçantes.

C'est un challenge de taille. Les monnaies « fiat » actuelles étant non programmables sur les livres bancaires où elles sont inscrites, il faut passer pour le moment par un tiers. On avance actuellement la solution du blocage d'un fond par une institution et l'émission de *colored coins* à due concurrence. Ainsi, il serait possible d'avoir des e-dollars ou des e-euros représentés par des jetons en *colored coins*. Mais il reste quand même une difficulté, qui tient à la centralisation de ce fonds en monnaie fiduciaire, laquelle ne peut pas être informatisée et décentralisée. S'ajoute à cela le problème de la montée en charge de Bitcoin, dont pour l'instant le réseau ne peut supporter des milliers de transactions à la seconde.

Pour pallier cela, deux alternatives se présentent pour le moment à Bitcoin, comme nous venons de le voir. En ce qui concerne la mise à l'échelle, il y a d'abord Lightning qui permet de ne pas toucher à la taille des blocs et donc d'éviter un *hard fork* à ce sujet. Et il existe, au-delà, une autre solution, qui serait d'augmenter voire de supprimer la limite de la taille des blocs. Nous allons parler ici de l'alternative Lightning, car c'est celle qui a pour le moment le plus de chances de s'imposer et qu'elle implique des mécanismes nouveaux contrairement à l'augmentation de la taille des blocs.

Nous allons essayer d'expliquer cela assez simplement. Il faut d'abord rappeler que Lightning utilise une technique incluse dans le protocole Bitcoin, à savoir les canaux de paiement. Encore une fois, on voit que Satoshi Nakamoto avait une vision à long terme, car le Bitcoin est étonnamment riche de fonctionnalités pouvant permettre son amélioration.

Lightning est proposé pour la première fois dans un livre blanc par Joseph Poon et Thaddeus Dryja début 2015[147]. L'idée plaît rapidement à la start-up Blockstream qui embauche dans la foulée Rusty Russell (un développeur connu pour son travail sur le noyau de Linux) pour s'occuper de travailler à ce sujet. En 2016, l'équipe de Bitcoin Core met en place le concept *Segregated Witness* pour permettre plus aisément l'implémentation de Lightning. D'après Nicolas Bacca de la société française Ledger, il s'agit « d'une remise à plat des structures de données utilisées aujourd'hui dans le protocole Bitcoin pour aboutir à un design plus propre : on sépare les données utiles (ici, les informations d'une transaction) de ce qui permet à un observateur de s'assurer qu'elles sont valides (ici, les signatures). Cela a pour effet immédiat d'augmenter la capacité utile d'un bloc : en stockant la signature des transactions séparément, on gagne beaucoup de place. » Fin 2016, la version de Bitcoin intégrant *Segwit* est proposée au consensus.

Le réseau Lightning utilise un protocole en surcouche de Bitcoin et permet à des acteurs tiers d'utiliser la blockchain comme une chambre de compensation périodique.

Un réseau utilisant Lightning peut présenter quelques nuances et il peut y avoir différentes implémentations. Ainsi, une implémentation française qui se nomme Eclair est développée par la start-up Acinq. Lightning consiste en un réseau décentralisé (ou plus ou moins centralisé) au-dessus de Bitcoin. Ce réseau pourra être proposé par des entreprises ou bien par des pairs, tout comme Bitcoin. Les échanges sur ce réseau s'effectuent dans ce que l'on appelle *des canaux de paiements*. Ceux-ci utilisent peu de place dans les blocs Bitcoin, car ils représentent juste les soldes des utilisateurs du réseau.

On estime que l'on peut quasiment couvrir l'humanité entière avec tout au plus six degrés de connexion entre les personnes[148]. Il est donc possible par un semblable effet de réseau d'inclure tout le monde dans le réseau

Lightning. Car un réseau Lightning étant une surcouche de Bitcoin, il va falloir que les « pairs » dans ce réseau y établissent le consensus pour que celui-ci fonctionne. On peut alors penser à toutes les transactions sur des plateformes d'échanges ou sur des wallet centralisés de type Xapo qui pourraient être facilitées et surtout plus sécurisées grâce aux réseaux Lightning. Toutes ces transactions *off-chain* auraient une existence *on-chain*, sans pour autant surcharger le réseau Bitcoin. De la sorte les plateformes d'échange n'auraient plus besoin de stocker les actifs de leurs utilisateurs mais seulement d'ouvrir un canal de paiement avec eux, canal qu'ils fermeraient à chaque exécution d'ordre.

L'avantage de délocaliser les transactions *off-chain* et de garder les soldes *on-chain* est de permettre une mise à l'échelle quasi définitive de Bitcoin, ne dépendant plus de son protocole mais des infrastructures Lightning. Ainsi, des milliers de transactions qui ne nécessiteraient pas de confirmation pourraient être effectuées sur la surcouche. Lightning permettrait donc aussi ce que l'on appelle le « *zeroconf* », c'est-à-dire des transactions sans délai, car sans le handicap de l'attente de confirmation de 10 minutes sur le réseau Bitcoin. En effet, sur un réseau Lightning, on trouverait des « pairs » qui se font mutuellement confiance et ne valident que des soldes de séries d'opérations, soldes enregistrées régulièrement sur la blockchain de Bitcoin. Pour inscrire ces soldes dans la blockchain, les « pairs » useraient d'une multisignature rendant impossible de tricher, tous les pairs devant être satisfaits de la transaction. En outre, il sera toujours possible d'utiliser les fonctions de Bitcoin décrites plus tôt, la monnaie restera donc sur Lightning totalement programmable.

Ce réseau pourrait permettre à des acteurs comme Visa ou Mastercard, ou comme les banques, de mettre en place un réseau en surcouche de Bitcoin. Ils pourraient ainsi rapidement implémenter ceci pour leurs clients. Ce serait extrêmement bénéfique en un sens pour Bitcoin car cela marquerait le début d'une utilisation à grande échelle.

Mais si cela résout le problème de la mise à l'échelle nécessaire pour proposer un jour l'émission de monnaie classique programmable sur la blockchain, cela ne résout pas le problème lui-même : ce sont encore des bitcoins qui sont échangés.

Une autre solution a été proposée fin 2014 pour améliorer également la mise à l'échelle de la blockchain Bitcoin et permettre des services comme l'émission de monnaies programmables. Le *whitepaper* de cette solution intitulé « Permettre des innovations de la blockchain avec des chaînes latérales à lien fixe » (*Enabling Blockchain Innovations with Pegged Sidechains* [149]) est écrit par plusieurs grands noms du Bitcoin (Adam Back, Peter Wuile, Maxwell) et il est soutenu par la start-up Blockstream déjà mentionnée qui a levé 20 millions en fin 2014 et 55 millions en février 2016.

Le principe des *sidechains* est de permettre la création de crypto-jetons sur des petites chaînes tangentes à la blockchain de Bitcoin. Ainsi, au lieu d'avoir des milliers de cryptomonnaies différentes, totalement autonomes mais de ce fait non interopérables, on fait en sorte que l'interopérabilité de cette grande diversité de jetons cryptographiques soit assurée au niveau du réseau de Bitcoin, en bénéficiant si besoin de sa sécurité sans égale. Le principe adopté est de faire un *2-way peg* (rattachement à 2 voies) entre deux blockchains (l'une des deux pouvant être la blockchain de Bitcoin, ou une autre *sidechain* déjà rattachée).

La technique est finalement assez simple et consiste dans le rattachement des deux blockchains par le séquestre préalable de jetons de la première chaîne pour débloquer d'autres jetons sur la seconde. Ainsi, si quelqu'un veut utiliser une chaîne latérale à Bitcoin, il aura juste à prouver qu'il a bloqué un certain nombre de bitcoins pour déverrouiller des jetons sur l'autre chaîne. Cela peut paraître anodin mais avec cette amélioration il devient possible de se passer d'intermédiaire de change, et même de renforcer la mise à l'échelle et les possibilités de Bitcoin. Tout peut être entièrement décentralisé.

Il serait dès lors imaginable d'émettre des devises électroniques particulières sur une chaîne avec des nœuds privés ou non, tout en bénéficiant de la sécurité de Bitcoin. Il sera nécessaire pour ce genre d'opérations (et sans doute inévitable si la technique se développe) que le bitcoin devienne une unité de compte de référence comme le dollar ou l'euro pour que cela soit plus aisé. En ce sens que le séquestre est dans le cas d'une *sidechain* exprimé en bitcoin. Mais ici les jetons émis peuvent être des e-dollars !

Les possibilités deviennent donc quasi infinies, car comme nous l'avons vu il y a peu, Bitcoin a provoqué un élan de créativité incroyable qu'il serait vraiment dommage de stopper.

Un des projets les plus ambitieux à se sujet est *Rootstock*, qui ambitionne de permettre sur Bitcoin tout ce qui est possible sur Ethereum, notamment en termes de « contrats auto-exécutables », à l'aide d'une *sidechain* et d'un jeton particulier, le *RSK*. Toutes les critiques formulées contre Bitcoin en raison de sa faible capacité de programmation par rapport à Ethereum tomberaient à l'eau si le RSK était programmable et conservait de surcroît la sécurité de Bitcoin sur sa chaîne principale, tandis que les possibles problèmes dus au langage « *Turing complete* » ne pourraient apparaître que sur la chaîne latérale. On peut dès lors imaginer qu'une grande partie des cryptomonnaies existantes pourraient basculer sur ce modèle pour des raisons de sécurité et de facilité pour les utilisateurs.

Nous n'avons fait ici que passer rapidement sur deux projets immenses pour Bitcoin, qui ne sont pas dénués de challenge. Mais nous devons également rappeler que rien ne nous assure leur mise en service ni même qu'ils seront adoptés. Peut-être qu'à l'heure où le lecteur lira ces pages, ces projets auront été totalement rejetés ou abandonnés. Cependant nous ne sommes pas inquiets, car toute la communauté, qui est au cœur même des innovations dans la cryptosphère, réfléchit sans relâche pour améliorer le système. Et l'on voit fleurir très fréquemment des idées ou des projets que nous ne pouvions évidemment pas tous décrire ici. Il faudra alors garder à l'esprit que Bitcoin peut devenir la méta-monnaie centrale par des améliorations successives de son protocole, profitant alors d'une mise à l'échelle digne des plus grands réseaux de paiements et d'une richesse de possibilités telle que celle proposée aujourd'hui par les altcoins.

Le bitcoin et la finance : « je t'aime moi non plus »

Il fut très longtemps et il reste hélas parfois de bon ton, chez les financiers, d'afficher à la fois son dédain du bitcoin et, fût-ce contre toute vraisemblance, un enthousiasme précoce pour la « technologie de la blockchain ». En réalité, de même que le bitcoin fut longtemps sans réelle valeur, il fut longtemps confidentiel, ceci expliquant largement cela, ce qui n'excuse pas pour autant le manque de curiosité et de rigueur intellectuelle de certains.

Bien évidemment, les premiers investisseurs, qu'il s'agisse de ceux, *family and friends,* qui apportent de la *love money*, puis des *business angels* et enfin les *venture-capitalists* les plus au fait de la nouveauté, presque tous sont implantés au cœur ou à proximité immédiate des centres de l'innovation technologique et informatique, au premier rang desquels se situe la Silicon Valley dans la partie Sud de la baie de San Francisco. *Geeks*, entrepreneurs ou investisseurs initiés s'y rencontrent dans des espaces de *co-working* ou pour des *meetups* où l'on communie dans le sentiment d'une révolution encore tout à fait confidentielle, même à San Francisco. Les premiers *meetups* se tiennent à partir du début 2012, dans l'emblématique local à l'angle de la 20e rue et de celle de la Mission.

C'est aussi au tout début de 2012 qu'a lieu l'un des premiers investissements portés à la connaissance du public, celui qu'un fonds d'incubation et d'amorçage de Portland réalise à hauteur de 30 000 dollars dans une place de marché communautaire permettant le règlement sur mobile en bitcoin, Gliph, qui existe toujours 5 ans après.

En septembre 2012 ce sont 600 000 dollars qui sont investis par divers californiens dans la plateforme d'échange Coinbase, créée trois mois plus tôt à peine par Brian Armstrong et Fred Ehrsam. Cette première levée de fonds est réalisée auprès d'entrepreneurs activistes ainsi que des fonds californiens, Y Combinator et FundersClub. Un délai aussi court est proprement impensable en France. Mais la suite ne le serait pas moins. Au 31 décembre de l'année suivante, soit en à peine 18 mois, Coinbase aura levé en tout près de 32 millions, dont 25 auprès du fonds de deux anciens de Netscape, Marc Andreessen et Ben Horowitz.

On est encore tout au début. Dans le milieu que Bitcoin intéresse, la spéculation commence (le cours est passé de 5 à 15 $) mais ce milieu s'étoffe encore lentement et les échanges n'ont dépassé le million de dollars que 20 fois dans l'année 2012. Dans ce petit milieu on va voir des opérateurs plus ou moins professionnels, car souvent liés entre eux par des relations familiales ou communautaires. C'est ainsi, par exemple, qu'on voit au début de l'année 2013 les jumeaux Tyler et Cameron Winklevoss, co-fondateurs de Facebook (qui avaient révélé en avril 2012 posséder 1 % des bitcoins en circulation), franchir un cap symbolique en investissant 1,5 M$ dans Bitinstant, le processeur fondé en 2011 par un ami new-yorkais, Charlie Shrem. Bitinstant employait déjà seize personnes et permettait à ses clients de régler leurs dépenses dans 70 000 commerces. Cependant les plaintes de clients se multiplient, une *class-action* est intentée et finalement Bitinstant disparait du paysage en 2014, tandis que son fondateur est mis sous les verrous, accusé d'avoir largement contribué au développement de la *Silk Road* car peu regardant sur l'origine des fonds échangés. Il est aussi accusé d'avoir accepté délibérément de convertir de grosses sommes tout en étant conscient de l'usage illégal de ces sommes une fois converties. Enfin, comme Ross Ulbricht, il fut défendu en grande partie par la communauté libertarienne trouvant cet emprisonnement totalement injuste et contraire à la liberté des affaires.

Plus conventionnel est l'investissement de 510 000 $ réalisé au début de janvier 2013 par des bitcoineurs comme Barry Silbert, Roger Ver et d'autres *early birds* dans un autre processeur, Bitpay. Ils sont rejoints dès mai 2013 par le Founders Fund et Heisenberg Capital qui injectent 2 nouveaux millions.

Les premiers investissements à six chiffres commencent vers la fin de l'hiver 2013 : Bridgescale Partners et quelques privés mettent 2 M$ dans BitGo, tandis qu'un ensemble de fonds spécialisés (déjà !) réunissant Andreessen-Horowitz déjà mentionné mais aussi Bitcoin Opportunity Fund, Lightspeed Venture Partners ou Vast Ventures mettent 2,5 M$ dans Ripple Lab qui développe une solution de paiement concurrente historique de Bitcoin, destinée au monde bancaire car semi-décentralisé et plus hiérarchique. Ils sont rejoints en avril par Camp

One Ventures, Core Innovation Capital, Google Ventures, IDG Capital Partners, Individual Investors, Venture51 qui ajoutent 3 nouveaux millions.

En avril 2013, Ribbit Capital, Union Square, Red Swan, Interplay et FundersClub remettent un peu plus de 6 millions dans Coinbase, et ceci un peu plus de six mois après le premier tour d'investissement réalisé au bénéfice de cette plateforme.

L'été 2013 est bien occupé à Palo Alto : en août, Centralway, Floodgate, Google Ventures, Y Combinator et quelques personnes physiques y investissent 1,25 M$ dans Digital Currencies Fintech. En septembre, Boost Fund met 2 M$ dans Vaurum (une plateforme d'échange plus tard rebaptisée Mirror) et on voit Centralway, Floodgate, Google Ventures, Rothenberg Ventures et Y Combinator mettre la même somme dans Buttercoin, une plateforme dont la fermeture 18 mois plus tard sera interprétée comme une « preuve » de la perte d'attractivité du Bitcoin par les « docteurs Tant-pis » de la cryptosphère.

Fin octobre, changement de braquet : c'est une mise de 9 M$ qui est annoncée par Accel Partners, General Catalyst Partners et divers investisseurs individuels dans la firme Circle de Boston. En même temps, à Londres, Pantera Capital investit 10 M$ dans la plateforme slovène Bitstamp. Et en toute fin d'année, les 25 M$ déjà évoqués investis dans Coinbase par les fonds Andreessen-Horowitz, Ribbit Capital, Union Square et QueensBridge, ainsi que par quelques particuliers, interviennent à un moment où le cours du bitcoin semble devoir monter « *to the moon* ».

Une donnée amusante se fait jour à partir de ce moment. On réalise que la cryptomonnaie, accusée d'être une pyramide de Ponzi, permet en réalité un autofinancement. En effet beaucoup de *early adopters* ont fait des fortunes grâce à l'envolée du cours et cela permet de financer leurs projets personnels mais aussi de financer les projets des autres. Nous pensons que c'est une donnée à prendre en compte pour comprendre le très rapide essor du capital dédié à la création d'entreprises dans le milieu, que ce soit en matière de financement salarial ou en matière de R&D. On a dit souvent de l'écosystème d'entreprises qu'il est presque prêt « trop tôt ». En effet les services de base du Bitcoin existent déjà avec des « mastodontes » à leur échelle : en ce qui concerne les processeurs de paiement pour commerçants, Bitpay ou Coinbase semblent déjà prêts pour une adoption de masse. Bitcoin a en quelque sorte déjà son ou ses PayPal grâce au pouvoir extrêmement rapide de cet investissement.

C'est aussi la raison pour laquelle le business qui se cherche autour de la « technologie blockchain » pourrait ressembler davantage à une bulle que celui fondé sur Bitcoin, dont les premiers investisseurs sont des personnes très au fait de ce qu'est Bitcoin. C'est loin d'être le cas des investissements dans la « technologie blockchain » qui sont davantage le fruit d'une excitation marketing et du sentiment qu'il ne faut pas « rater le coche » comme à l'époque de la pré-bulle Internet.

Avec l'engouement croissant pour Bitcoin, les choses se structurent, les fonds d'investissement, voire les fonds de fonds, se font toujours plus présents. Il n'est plus question, à compter de 2014, de mentionner une à une toutes les opérations, surtout les « petites » (qui seraient célébrées comme des exploits en France), mais il faut noter que la déprime du cours de la devise elle-même ne semble pas refroidir l'enthousiasme. Durant le seul mois de mars 2014, la plateforme Kraken lève 5 M$, Bitreserve autant, OK Coin lève 10 M$, Circle 17 M$ et Xapo 20 M$ (cette tranche-ci auprès de Benchmark, Fortress Investment, Ribbit Capital et Slow Ventures). Au milieu d'innombrables petits deals à 100 000 euros, le processeur de paiement Bitpay (une société fondée en mai 2011 pour commercialiser des solutions d'acceptations du bitcoin et qui annonçait déjà 12 000 clients commerçants) annonce en mai une levée de 30 M$ tandis que Bitfury (entreprise spécialisée dans le minage de bitcoins) lève 20 M$. En mai également, on voit des levées de 10 M$ en Chine (Huobi) et en Israël (Simplex). Les affaires les plus prometteuses multiplient les levées, espacées parfois de quelques semaines seulement. Ainsi en juillet Xapo lève-t-il une nouvelle tranche de 20 M$ (cette fois auprès d'Index Ventures, Greylock Partners, Emergence Capital, Winklevoss Capital et Crypto Currency Partners). En août, Chain lève 14 M$ et en octobre, tandis que Bitfury réalise une nouvelle levée de 20 millions, Blockchain.info en lève 30.

Arrêtons-nous un instant sur ce nom : jusqu'en 2014, Bitcoin a été « le » sujet, et son registre, que l'on appelait plutôt le *Ledger* ne s'était pas autonomisé. La blockchain, c'est un mot qui apparaît progressivement, pour désigner d'abord (en deux mots) le chainage des blocs par le hashage, une pure description technique d'un mécanisme de Bitcoin donc, puis par une sorte de métonymie troublante, tout le registre et son fonctionnement, le protocole et l'algorithme.

On va y revenir longuement au point suivant pour montrer comment, dédain ou mauvaise foi, la finance institutionnelle va s'emparer de « la technologie blockchain » pour retourner l'arme qui la visait. C'est progressivement que l'on voit apparaître le mot *Blockchain* plutôt que *Bitcoin* dans les articles de presse et d'une manière générale dans tout le monde extérieur à la sphère Bitcoin. Ainsi, on peut dater de la fin 2014 le début du phénomène. Le petit monde de Bitcoin va devoir composer tant bien que mal avec ce nouveau *buzzword* qui trouvera son paroxysme avec la couverture de *The Economist* de novembre 2015 « *The trust machine, how the technology behind Bitcoin could change the world* »[150]. En novembre 2014 la start-up canadienne *Blockstream* annonçait une levée de 21 millions marquée par la présence de Reid Hoffman, co-fondateur de LinkedIn : parmi ses projets, le développement de sidechains (évoquées au point III, 2) qui impliquent une fondation bitcoin très solide, mais le tout avec un nom qui certes se justifie (l'entreprise axe principalement son développement sur la blockchain de Bitcoin) mais qui a sûrement été jugé plus… convenable !

Le monde financier, n'est cependant pas monolithique. Ce qui hérisse ou menace les banques peut sembler attractif à des investisseurs individuels hardis ou innovants comme Richard Branson, fondateur du groupe Virgin, ou Jerry Yang, co-fondateur de Yahoo, qui participent en mai 2014 à la levée de fonds de 30 millions de dollars au profit de Bitpay. Quant aux investisseurs en capital, ils avaient déjà pris l'habitude, en finançant les « Fintechs », de nourrir de futurs oiseaux de proie qui s'en iraient un jour chasser le gibier des banques. Une certaine forme de schizophrénie peut donc exister. On le vit en France (avec un zéro de moins !) quand la société Ledger, qui gère la « Maison du Bitcoin » à Paris mais a aussi mis au point des portefeuilles Bitcoin sécurisés dotés d'une carte à puce parmi les plus sûrs du monde, parvint à lever 1,3 million d'euros auprès de quelques *business angels* mais aussi de XAnge, la filiale d'investissement de La Banque Postale que cela n'empêchait pas de poursuivre les clôtures (et même les gels) de comptes de divers bitcoineurs (dont l'un des auteurs de ce livre). La rumeur prétend que XAnge s'était fait à l'époque taper sur les doigts par La Banque Postale pour avoir réalisé ce financement. Ils devraient s'en être remis sachant que Ledger (qui a réussi en avril 2017 une seconde levée de fonds sur laquelle nous allons revenir) est une des plus belles entreprises du monde Bitcoin…

À partir de la fin 2014, du côté occidental de l'Atlantique, les investisseurs s'organisent dans ce secteur très spécifique et on remarque désormais les plus grands. Ainsi, en décembre 2014, la quasi-totalité des bitcoins saisis et mis aux enchères par le *United States Marshals Service* sont remportés par le *Bitcoin Investment Trust*. Et en avril 2015, ce sont Goldman Sachs et IDG Capital Partners (une société d'investissement implantée en Chine) qui mènent la nouvelle levée de fonds de Circle.

Bien avant qu'en France (où une seconde levée de fonds du secteur était annoncée en septembre 2015, au bénéfice de la plateforme Paymium et à hauteur de 1 million d'euros) les officiels ne se soucient seulement de la chose et n'organisent de timides rencontres sur le thème de « la blockchain », le bitcoin était bien tenu en main, quant au développement de son écosystème, par le capital américain. Le *Digital Currency Group* de Barry Silbert, impliqué notamment dans Bitpay, Bitpesa, Chain, Changetip, Circle, Coinbase, CoinDesk, Coinsetter, Colu, Kraken, Ripple Labs, Safello ou Xapo s'était imposé comme le plus puissant groupe d'investissement du secteur.

Cette arrivée des capitaux-risqueurs (*ventures capitalists*) ne pouvait pas rester sans conséquences. L'investissement n'est ni une marque d'intérêt passive ni un geste d'encouragement à la recherche fondamentale. Toute société qui reçoit ce type de monnaie se voit engagée dans une course à la croissance, sur un tempo généralement court-termiste, sauf peut-être en Californie où les rounds de *funding* sont tellement proches et élevés qu'ils peuvent permettre à des sociétés de survivre extrêmement longtemps sans bénéfice (20 ans pour Amazon[151], 5 ans pour Facebook[152], ce temps n'est pas encore arrivé pour Twitter[153]). Ces exemples ne sont qu'un minuscule échantillon des sociétés californiennes vivant sans bénéfice et affichant des capitalisations pourtant monstrueuses. Au moins offrent-elles « de la traction ». Le décalage entre le caractère encore très expérimental de Bitcoin (chose pourtant rappelée du soir au matin) et les attentes de croissance des performances concrètes, ce que l'on appelle la *scalability* (le passage à l'échelle supérieure) a entraîné le débat déjà évoqué au point III, 2 sur la taille des blocs, débat très vif et parfois acrimonieux car mêlant des considérations politiques et morales à des intérêts très palpables.

Car Bitcoin a sa logique propre. Et tandis que les *venture capitalists* investissaient tous ensemble un bon milliard autour du jeune bitcoin, l'algorithme continuait d'en créer 50 unités (jusqu'en 2012) puis 25 toutes les dix minutes, que le marché absorbait tant bien que mal, et plutôt bien : la capitalisation totale des jetons en circulation, qui était de 3 petits milliards de dollars en début 2015 avait refranchi la barre des 5 en octobre. Devant l'abondance de presse sur le moindre pari d'un *venture capitalist* recyclant sa pelote ou d'un consortium de banque misant quelques millions[154], il convient de rappeler ces chiffres. Les premiers investisseurs du monde

bitcoin, ce sont les bitcoineurs qui, en année pleine, ont « acheté » aux mineurs 1 362 000 nouveaux bitcoins en 2015 et 1 471 000 en 2014, et les mineurs eux-mêmes qui les ont produits non sans investissement, et en ont gardé une part. En affectant tous ces bitcoins (de la façon la plus grossière) d'un cours moyen de l'ordre de 500 euros sur la période, on est autour de 1,4 milliard de dollars d'argent frais.

Dans ces conditions la production de bitcoins, le « minage », est progressivement devenue une industrie lourde. Sa seule mesure publique et incontestable est celle du *hashrate*, c'est-à-dire du nombre (en milliards) d'opérations que l'ensemble des *nodes* effectuent à chaque seconde. Au cours de l'année 2012, elle était passée de 9 à 24 milliards de hash par secondes (TH/s), au cours de l'année suivante, la courbe entamait son envol hyperbolique, franchissant les 500 TH/s à la fin de l'été pour achever l'année à 20 fois ce niveau. La puissance de feu du réseau était ensuite multipliée par 32 en 2014, pour s'établir autour 320 000 TH/s au début 2015. À noter qu'elle a ensuite pratiquement doublé en 2015 et de nouveau en 2016. On voit que l'effort d'équipement a été particulièrement puissant sur les deux années 2013 et 2014 et s'est poursuivi. La presse, qui orne rituellement tout article sur le bitcoin d'un graphique concernant son cours réputé anormalement erratique, ne montre pratiquement jamais la courbe du *hashrate* et celle du nombre d'opérations, dont les hyperboles seraient autrement plus inquiétantes pour le système classique. D'autres graphiques sont édifiants en ce sens, ceux du nombre de nouvelles adresses détectées chaque jour sur le réseau, du volume de transactions journalières et d'autres encore. [155]

En septembre 2015, la firme de minage BitFury investit 100 millions de dollars dans un nouveau *data center* à Tbilissi, la capitale de la Géorgie. Mais le minage est déjà devenu une industrie largement chinoise, ce qui a, parmi ses nombreuses conséquences, entretenu un grand flou sur les chiffres de celui-ci.

Ce qui sera régulièrement dénoncé comme un « problème de gouvernance » de Bitcoin provient moins d'une absence de banque centrale gouvernant cette monnaie que de la divergence épisodique des intérêts ou des affects des utilisateurs, des mineurs, des investisseurs et des développeurs de ce qui est bien plus qu'une monnaie.

Quoiqu'il en soit, malgré le brutal dégonflement de son cours sur toute l'année 2014 et près d'une centaine de faire-part de décès [156], Bitcoin s'était fait sa place en 2015 dans le paysage. En mai 2015, le *New York Stock Exchange* annonçait qu'il intégrerait désormais le cours du bitcoin en dollar, une fois par jour, à 11 h, sous l'indice *NYXBT*. L'autre marché new-yorkais, le NASDAQ, a aussi adopté bitcoin. Des firmes d'investissement liées au bitcoin, mais aussi des *trackers* (actions reflétant le cours du bitcoin) y sont inscrites à la suite du Bitcoin Investment Trust de Grayscale. Mais là, on va vite comprendre qu'au-delà de la devise bitcoin, c'est la capacité de sa « technologie blockchain » de gérer les opérations de règlement, de livraison et de compensation qui intéresse le NASDAQ. Dès mai 2015 celui-ci annonçait qu'il envisageait d'utiliser cette « technologie » afin de faciliter les échanges sur un marché entre sociétés privées, notamment par la mise en place d'un protocole assez voisin et nommé l'*Open Assets Protocol*, qui ne serait pas utilisé pour créer une monnaie mais pour garder la trace des transactions sur ce marché privé. L'année 2015 est aussi celle où la « technologie blockchain » tente de ravir au Bitcoin la place d'innovation fondamentale qui est la sienne.

La solution, c'est de taire son nom

On a daté de la crise chypriote du printemps 2013 la première apparition du Bitcoin sous les projecteurs. Il n'est alors pas mis immédiatement en accusation, bien au contraire, ni par les autorités, ni par le business.

Fin juillet 2013 est créée aux USA la *Digital Asset Transfer Authority* qui se fixe pour tâche de produire des normes pour que les crypto-devises évoluent en conformité avec la législation et la réglementation. Le 6 septembre le patron de la Fed présente Bitcoin comme un système de paiement rapide et sûr. Quelques semaines plus tôt, l'Allemagne lui avait donné le statut de monnaie privée. Encore en novembre, le Département de la Justice américain le qualifiait de monnaie « légitime » et Ben Bernanke disait qu'il avait du « potentiel ».

Mais après le scandale de la *Silk Road* (dont la première fermeture date d'octobre 2013) vint la bulle chinoise, et le 5 décembre les autorités chinoises se fâchent, vite suivies des autorités américaines puis de bien d'autres. C'est vers décembre 2013 que la guerre est déclarée par les banques, partout dans le monde, d'abord de façon très concrète, en fermant les comptes dès que bitcoin est en cause, que ce soit pour du *trading*, de la *remittance* ou du minage, et ceci tout en commençant à créer des *task forces* de recherche sur le sujet. Les banques s'avèrent être l'un des secteurs le plus avisés sur la question, malgré leur revirement opportuniste (et peut-être

apparent) vers la « technologie blockchain ». On en voit qui pourraient bien switcher de *business model* une fois la régulation actée et favorable.

Mais les banques mettent aussi en avant l'asymétrie que représente l'existence de ce système radicalement non régulé alors qu'elles-mêmes sont astreintes à de lourdes obligations. Les autorités y répondent dans le plus grand désordre, et parfois sans grand sérieux, quand l'opinion de banquiers menacés dans leur monopole et de juristes encore peu formés à la chose sert de « consultation ». On voit des régulateurs parler de « comptes en bitcoin », exiger des « adresses transparentes » voire des clefs cryptographiques réservées aux autorités. Les institutions les plus diverses expriment les opinions les plus erratiques.

En mars 2015, la BCE [157] juge le bitcoin « intrinsèquement instable (mais) novateur ». Ouf ! La Fed juge que c'est « un coup de génie sans avenir » mais qui peut inspirer la Fed [158]. L'idée du plagiat ne gênera jamais les grands défenseurs de la propriété privée. Toujours aux USA, la *Commodity Futures Trading Commission* déclare en septembre 2015 que Bitcoin et les autres crypto-monnaies sont des « matières premières », comme l'or, le pétrole, ou le blé tandis que c'est officiellement une « propriété » pour les impôts (IRS) et une « monnaie » pour la SEC, le gendarme de la Bourse. Il y a eu à ce propos une demande très sérieuse à la SEC de la part des Winklevoss pour intégrer un ETF (Index) Bitcoin au BATS Global Exchange (troisième place boursière américaine après le NYSE et le NASDAQ) après plus de trois ans de demande pour intégrer le NASDAQ. [159] Sans succès, cette fois.

Les choses ne sont pas plus claires en Europe où l'eurodéputé lituanien Antanas Guoga, finit par le dire fort honnêtement et fort justement en avril 2016 : « nous tentons de faire des lois sur quelque chose que nous ne connaissons pas et que nous ne comprenons pas vraiment. Je suggère à tout le monde de se procurer des bitcoins afin de se familiariser avec le système ».

L'attention s'est longtemps focalisée sur la volonté manifestée à New-York dès novembre 2013 de réguler la nouvelle crypto-finance, en l'assujettissant à l'octroi d'une licence. Le terme de *NY BitLicense* fait son entrée dans le vocabulaire des cryptos, avec le nom de Benjamin Lawsky, superintendant du *New York State Department of Financial Services* (NYDFS) qui, au moins, était bon connaisseur de la chose.

L'histoire de l'élaboration des textes est édifiante. Au-delà d'une dramaturgie toute américaine et des menaces classiques que suscite toute tentative de régulation, surtout quand elle ne doit s'appliquer qu'assez localement, on distingue deux éléments importants dans les échanges entre les autorités et les professionnels durant la *public comment period* courant jusqu'en octobre 2014. D'une part un débat de fond chez les supporters des monnaies libres quant à l'opportunité d'admettre une régulation (aussi légère que possible) de nature à faciliter l'adoption de masse au prix d'une renonciation à certaines dimensions libertaires du projet d'origine. Naturellement les investisseurs inclinaient dans un sens, les *geeks* restés fidèles à la philosophie *cypherpunk* des origines dans l'autre. D'autre part, le fonctionnement propre du bitcoin, sans réel équivalent, rendait particulièrement ardue l'élaboration d'une régulation spécifique à cette monnaie au-delà des règles s'appliquant par métiers ou par usages.

Passée la période des commentaires sur sa première et très sévère version, Ben Lawsky entra dans la période des marchandages : la NY Bitlicense pourrait ne pas s'appliquer entièrement ou immédiatement aux plus petites startups ni à ceux qui développeraient une blockchain pour faire autre chose que du paiement ou des wallets à usage personnel. De plus les choses continuaient de bouger hors de New York : au niveau fédéral on vit en début 2015 une proposition de loi pour un moratoire de 5 ans en matière de législation sur la cryptomonnaie, opinion assez raisonnable également formulée en Europe : comment réguler quelque chose qui n'existe encore qu'à l'état d'expérience et dont le régulateur ou le législateur ne comprend qu'à grand peine les implications ? Dans d'autres États américains, comme le Vermont en février 2015, on émettait des doutes sur l'opportunité d'une régulation spécifique. La difficulté principale, comprise par certains législateurs, étant de réussir à établir un cadre dynamisant le business et rassurant les entreprises tout en étant assez sévère pour ne pas être accusé d'irresponsabilité ou de laxisme. 18 mois après les premières annonces, le débat faisait encore rage, impliquant les ténors de l'industrie ou le MIT. Quand la nouvelle régulation entra en vigueur, les plateformes Kraken et Bitfinex, deux majors de l'industrie cessèrent leurs activités à New-York, mais le NYDFS reçut 22 demandes officielles d'attribution de licence. La première fut attribuée enfin en septembre 2015 à Circle, la seconde ne vint que six mois plus tard, en juin 2016, attribuée à Ripple c'est à dire à un concurrent très « bancaire » de Bitcoin. Au total, sans doute *beaucoup de bruit pour rien.* Pour rien ? Non : M. Lawsky créait ensuite, dès la fin 2015, sa firme d'aide et d'accompagnement réglementaire aux entrepreneurs du secteur.

En Europe le fait majeur fut l'arrêt de principe, déjà évoqué, rendu en octobre 2015 par la Cour de Justice de l'UE[160], déclarant que les prestations d'échanges de bitcoins contre une devise traditionnelle sont une activité de prestation de services, et que ces opérations sont exonérées de la taxe sur la valeur ajoutée. C'est le critère d'*usage* qui fonde l'appréciation du juge, indépendamment du caractère légal ou non ; ce n'est pas la loi mais l'acceptation par les parties qui, s'agissant d'autre chose que la devise officielle, suffit à qualifier un « moyen de paiement » dont l'émission, l'acquisition et la gestion constituent des services de paiement. Certes il s'agit d'un arrêt de droit fiscal, lequel est un droit autonome, mais le juge a dû déterminer si l'usage du bitcoin correspondait ou non à la définition du service de paiement et en ce sens l'arrêt n'est pas spécifique au droit fiscal et éclaire sur le mécanisme de qualification des services de paiement. Façon de dire qu'il s'impose largement. On entendit des dirigeants de banque s'enrouer de colère.

La volonté de doter les choses d'un cadre légal et de réglementer (fureur toute européenne) se porta alors sur le sujet de conversation qui, entre temps, s'était imposé : celui de la blockchain. Que ce soit par indifférence ou par mauvaise foi, il fut en effet proclamé *urbi et orbi* que le Bitcoin n'était qu'un détail et que la chose intéressante n'était « que la blockchain ». Ceci est en soi un élément d'histoire assez significatif.

L'effondrement du cours dès janvier 2014 est suivi en février de la faillite de MtGox présentée comme la preuve du caractère dangereux de la nouvelle monnaie, non garantie, non protégée, n'attirant finalement que des escrocs et des naïfs. Désormais il n'y aura plus un article, plus un discours, sans qu'un mélange de MtGox et de *Silk Road* ne serve d'introduction, de développement pittoresque ou d'étayage à des démonstrations convenues. Le vent tourne, d'autant que le cours baisse et comme chacun sait, un actif qui baisse a peu de supporters, même si les bitcoineurs restent tenaces et confiants. La corrélation de la courbe de recherche « Bitcoin » sur Google avec celle de son prix va alors être quasiment parfaite.

Soudain, à l'automne, Bitcoin fut *out*. Pour une part, ce furent les entreprises du secteur elles-mêmes qui initièrent la manœuvre. Après 18 mois d'investissements massifs elles commençaient à réaliser que l'adoption par le grand public d'une technologie, aussi utile soit-elle, et même à l'ère de la globalisation, n'allait pas se faire en quelques mois. Plusieurs avaient fondé leur business model sur une croissance un peu trop optimiste du taux d'adoption. N'ayant rien de plus à vendre, la tentation fut grande de vendre la même chose sous un autre nom. Progressivement, le mot blockchain fit son apparition. Au début pour parler de Bitcoin sans prononcer un mot qui fermait déjà les portes de l'univers bancaire, alors même que tant de gens entendaient vendre auxdites banques des copies plus ou moins réussies d'un protocole libre. Puis pour vendre un peu n'importe quoi, voire de la fumée.

La grande finance et ses chantres ordinaires avaient aussi été à la manœuvre. Prises entre la menace des GAFAM et celles des start-up de la *fintech*, les banques trouvèrent là le remède miracle à leur obsolescence informatique. En juin 2015, les experts de Santander (des consultants recrutés par appel d'offre) avaient promis *de 15 à 20 milliards de dollars par an d'ici à 2022 en coûts d'infrastructures liés aux paiements internationaux, au trading et à la mise en conformité.* Les 20 milliards seront indéfiniment répétés, sans détail, de conférence en conférence.

Il revint à Madame Blythe Masters de cristalliser la chose. Le 1er septembre, cette britannique de 46 ans, entourée de ses trois molosses dans son penthouse de Manhattan, avait distillé pour Bloomberg que *the Blockchain changes everything*[161]. Or Madame Masters n'est pas n'importe qui. Mathématicienne entrée à 17 ans chez JP Morgan, elle y avait fait une carrière fulgurante dont l'apothéose fut l'invention des contrats d'échange sur défaut de crédit, dont la montagne estimée à 58 000 milliards de dollars hors bilan avait, en septembre 2008, sérieusement ébranlé la planète. En septembre 2013, elle s'était retrouvée dehors de Morgan. La « technologie Blockchain », qu'elle semble n'avoir découverte que dans le courant 2014, allait être aussi son rebond.

Le 6 octobre 2015, Blythe Masters cisèle la formule que tous les financiers suiveurs répétèrent pendant près d'un an : *Forget Bitcoin, Embrace the blockchain.* Techniquement, ce serait soit une imbécillité soit une imposture. Mais en termes de marketing c'est un coup de génie. Quand Mme Masters poursuit en déclarant que « dans sa structure la plus simple, une blockchain n'est guère grand-chose de plus qu'une drôle de base de donnée » on perçoit trois choses qui seront les marqueurs de tous les discours sur « la blockchain » durant des mois : une totale indifférence à la complexe vérité de l'agencement réalisé en 2008 par Satoshi Nakamoto, une solide absence de scrupule et un fort cynisme permettant d'asséner autoritairement les choses sans les démontrer, le tout couplé, il faut le dire, à une erreur linguistique capitale.

Parce que, dès lors, le mot *blockchain* devient incontournable pour un an au moins chez les start-ups de la *fintech*, qui durent vendre de la blockchain, chez les banques (où les plus cyniques comparaient en privé ce sujet à celui de la sexualité chez les préadolescents) et chez les consultants, les juristes et les journalistes qui se disent spécialisés, parce qu'en fait c'est seulement un mot pour un autre dans un discours controuvé, il nous parait important de l'analyser d'abord comme tel : un mot qui tombe mal.

Nous avons parlé de métonymie (on peut aussi parler de synecdoque) au sujet de cet usage du mot « blockchain ». Mais par rapport à celle du « verre » qui est nettement moins dénaturante (bien que fonctionnant syntaxiquement de la même façon nom / complément du nom), une différence de taille existe : « la blockchain » ne peut pas être précédée d'un article défini au singulier et c'est là que se pose tout le problème de cette métonymie. Nous pouvons dire un verre à la place d'un verre de quelque chose parce que le verre en question est indifférencié. En revanche pour ce qui des blockchains c'est tout différent. On peut dire « la blockchain de Bitcoin », car la blockchain de Bitcoin est unique et identifiée ; ici le mot blockchain est déterminé par le mot Bitcoin. Donc la métonymie « la blockchain » ne peut sémantiquement être défendue. Son extension, qui amène à parler de « la technologie de la blockchain » (peut-être parce que le non-sens est inconsciemment ressenti), fait que c'est la technologie qui vient être déterminée par la blockchain. On s'enfonce : cet apparat trompeur focalise sur le noyau « la technologie » alors que son complément du nom ne veut en réalité rien dire. Décidément la métonymie de « la blockchain » ne peut pas fonctionner ; c'est comme si nous choisissions arbitrairement de dire « la technologie » comme métonymie de « la technologie de X » et donc de ne faire porter qu'un sens à ce mot qui a besoin d'être complété pour être pleinement déterminé, mais qui peut l'être de différentes manières tout comme le mot « blockchain ».

Le mot est au demeurant rarement utilisé pour désigner ce pour quoi il a été formé : un registre décentralisé enregistrant des transactions. Ce qu'on nomme dans ou pour les banques la « technologie blockchain », c'est parfois non seulement ce registre, mais aussi tous les mécanismes qui permettent de valider des transactions et d'inscrire et de nouveaux blocs dans ce grand livre. En ce cas, ce que les banques tentent de reproduire, d'édulcorer, parfois de breveter et au final de privatiser ce n'est ni plus ni moins que la « technologie Bitcoin ». Mais parfois on décortique la chose : comme les banques ne veulent pas d'une blockchain dotée d'un jeton intrinsèque valorisable ou public, on le supprime, et du coup on supprime aussi l'*incentive* de la preuve de travail, etc.

Oubliant que l'invention de 2008 (année où les banques ne se faisaient plus confiance du tout entre elles !) a surgi pour créer une nouvelle forme de confiance sans autorité centrale ni reconnaissance bilatérale, on crée des « blockchains » bancaires où la validation des écritures se fait pourrait-on dire autour de la table. On oublie aussi le problème dit « des généraux byzantins », la possibilité d'une tricherie ou d'un consensus par fusion-acquisition. Il est évidemment malséant de rappeler le scandale du Libor[162] qui vit, durant quatre ans au moins, une bonne demie douzaine de grandes banques manipuler de concert le cours de cet indice phare…

À la fin il reste une base de donnée (faiblement) distribuée et bien plus « virtuelle » que celle de Bitcoin, autant dans son existence que dans sa substance. Comme elle ne comporte pas de jeton valorisé, on imagine d'y inscrire un jeton représentatif de « vraie » monnaie. Mais justement ce jeton ne serait qu'une forme virtuelle de la vraie monnaie. C'est le problème avec les cryptomonnaies imaginées pour le règlement des opérations de marché : les opérateurs ne sont pas payés plus vite, ils ont plus vite leurs jetons, qui représentent la vraie monnaie à la façon dont un cube en bois représente un hôtel au Monopoly. Alors on imagine aussi d'y inscrire des titres, en obtenant des autorités la validité juridique de l'opération : c'est le sens de l'ordonnance signée par M. Macron le 28 avril 2016 et permettant l'inscription de mini-bons de caisse sur une mini-blockchain, projet expérimental sans grand intérêt mais célébré comme révolutionnaire. Il reste qu'une telle blockchain, n'ayant plus de *token* pour rémunérer ses validateurs décentralisés (c'est bien une « blockchain maison ») n'offre guère plus de sécurité qu'une base de donnée maison. La Bourse australienne a fini par l'avouer[163].

Alors on va plus loin. Comme les transactions sur une blockchain peuvent contenir des métadonnées (comme la rubrique « objet » ou « libellé » d'un transfert bancaire) on peut s'en servir comme d'une base de dépôt de données. C'est tout de même confondre la chose avec une Dropbox. Partout il se dit que la blockchain va « bien au-delà de la finance ». Elle permettrait de tenir un cadastre dans le Honduras qui n'en a pas. Cette baliverne est répétée jusqu'à l'ennui, avec quelques autres. En septembre 2016, le vent semble tourner de nouveau. On finit par avouer, dans l'un des hauts lieux de la finance parisienne, que 80 % de ce qui s'est écrit au sujet de la blockchain est « du *bullshit* ». L'obstination à aller « au-delà de la finance » ressemble par trop à l'effort de tous les prestidigitateurs pour attirer le regard sur la main qui ne tient pas le gimmick.

Quant à ceux qui, suivant Mme Masters, ont oublié le bitcoin en septembre 2015 ils sont passés à côté d'une bonne affaire : son cours a doublé dans les 12 mois suivants et même quadruplé depuis lors [164].

L'investissement remarqué de 7 millions d'euros réalisé en avril 2017 dans la société française Ledger par un groupe d'investisseurs institutionnels conduits par MAIF Avenir (avec Xange, Wicklow Capital, GDTRE, Libertus Capital, Digital Currency Group, The Whittemore Collection, Kima Ventures et BHB Network) semble suggérer qu'au delà des diversions sur la "technologie blockchain", ces investisseurs ont bien compris et la valeur des tokens de blockchains publiques comme celle de Bitcoin, et l'impérieuse nécessité de construire les solutions de sécurisation à la pointe du progrès.

Bitcoin : un futur de possibles

Est maintenant venu le temps pour nous de faire un chouïa de prospective. Nous avons tant bien que mal essayé d'en faire le moins possible dans ce livre pour nous limiter avant tout aux solutions existantes et aux aspects concrets. Ce passage est aussi l'occasion de relativiser l'aspect parfois un peu partisan du livre. On s'accorde à dire, depuis Sartre, que de toute manière n'importe quelle œuvre implique un engagement de ou des auteurs. Mais le lecteur constatera que ce n'est pas une vision subjective et extensive à l'infini dans le temps. Elle est simplement corrélée à un continuum de faits nous amenant à penser que Bitcoin est pour l'instant le projet le plus abouti, le plus innovant et le plus à même de survivre.

Ceci dit, en ce qui concerne un futur dont ne sommes pas garants, le lecteur constatera notre ouverture et notre opinion moins tranchée que sur certaines controverses actuelles. De toute façon nous n'avons accès ni au grand rouleau de *Jacques le fataliste* ni aux clefs du *mektoub*.

Commençons par des cas d'usages que l'on pourrait voir apparaître à court terme et que nous avons abordés au fur et à mesure du livre. Tout d'abord Bitcoin peut demeurer une monnaie étalon d'Internet comme il le devient progressivement ; il peut aussi continuer à être un protocole servant à d'autres choses, tout en étant dans un écosystème où les méta-monnaies se combattent et sont en concurrence. Mais rapidement le modèle pourrait aussi bien être inversé et Bitcoin à la manière de Linux pourrait devenir un noyau stable et standard sur lequel se grefferaient nombre d'autres crypto-jetons, circulant sur différentes sidechains.

Dans tous les cas, les différentes applications possibles sont la certification de documents divers dans les blockchains, avec une libéralisation des tiers de confiance, mais aussi l'utilisation de *colored coins* lors d'événements particuliers, pour des devises complémentaires, pour l'émission d'actions, et pour d'autres cas à développer.

Le crypto-jetons peuvent aussi être utilisés par les machines dans le cadre de l'Internet des objets, à l'aide de contrats auto-exécutants. Ils pourront avoir une place prépondérante dans les domaines de l'énergie, mais aussi de la propriété intellectuelle globale, instantanée et accessible à tous.

Les villes connectées pourraient bénéficier des méta-monnaies pour créer des services urbains innovants et plus pratiques, mais également pour horizontaliser la démocratie municipale avec des votes électroniques décentralisés courants. L'utilisation de *tokens* de vote décentralisés est vraiment un cas d'usage qu'il est fort probable de voir se développer.

L'usage peut aussi être celui de la création d'organisations autonomes décentralisées à l'aide de *smart contracts*. Ces organisations peuvent aussi bien être des associations que des entreprises commerciales. Il est également possible d'envisager des applications avec des intermédiaires libres dans de nombreux domaines de l'économie collaborative comme les chauffeurs particuliers, les services entre particuliers, la vente en ligne.

Enfin, des cas un peu plus extrêmes vont voir le jour comme le projet *Augur* qui veut devenir un marché prédictif universel autonome et décentralisé. Comme la décentralisation des protocoles d'échanges décentralisés ouvert ne permet pas de censure, cela peut donner lieu à des situations inédites, déjantées et parfois effrayantes.

Pour expliquer la chose avec un atticisme certain : un marché prédictif revient à être une immense plateforme de paris libres sur n'importe quel sujet. Cela permet de superbes avancées comme de l'assurance

décentralisée matérialisée sous forme de paris sur les conditions de l'assurance. Mais cela pourrait en théorie donner lieu à des choses aussi terrifiantes qu'un *assassination market*, d'autant que l'on peut penser qu'à un moment il devient plus rentable pour le parieur de tuer la personne en payant des spécialistes que de perdre son pari. L'idée d'un seuil de rentabilité sur la mort peut être un peu déroutante. Bien sûr, rien de tout cela ne peut raisonnablement avoir lieu, mais ça deviendra plus facile. Rendre ces marchés sombres et macabres accessibles au public n'est pas forcément une idée riante.

Clôturons par des visions qui semblent utopiques à court terme mais envisageables à long terme pour ce qui est de l'écosystème de Bitcoin et des méta-monnaies. Le tableau de l'utopie bitcoinienne pourrait être dressé de la sorte :

En 2050, tous les États ou la majorité des États ont émis des cadres législatifs non restrictifs et encourageants. L'adoption du Bitcoin a continué son chemin avec une adoption massive au tournant de la troisième décennie du siècle. Son prix a poursuivi son avancée jusqu'à une stabilisation vers 2040 autour de 1 000 000 (digital) USD. Tout le monde est habitué à compter en décaSat, c'est à dire à 10 satoshis près (0,00 000 010 btc) que l'on aura rebaptisé Satoshi pour plus de convenance et toujours en souvenir du créateur. La masse monétaire cumulée de bitcoin est alors 21 mille milliards de dUSD, très proche de ce qu'est aujourd'hui au niveau mondial MB (Base Monétaire = billets et pièces circulant et stockés + réserves obligatoires des banques) soit 22 mille milliards de dollars [165]. Bien sûr les zéros après la virgule ont été étendus avec 8 nouvelles décimales pour donner plus de commodité aux micro-transactions dans le *hard fork* de 2042. En 2050 les micro-transactions sont pléthores, tant du fait de l'adoption massive du bitcoin, de la multitude de services qui l'utilisent et de la diversité existante de sidechains, couplé au fait que des milliards d'objet effectuent des transactions chaque jour.

Nous parlons de dUSD (*digital dollar*) car le dollar est désormais un crypto-jeton circulant sur une *sidechain* de Bitcoin dont les nœuds sont gérés par les banques participantes du système fédéral. Tous les dollars circulants encore sont *backés* sur un *2-way peg* d'une *sidechain* permettant de s'assurer qu'ils ont une vraie valeur comme avant la fin des accords de Bretton Wood sur l'or. Il suffit alors d'ajuster le *peg* pour ajuster si besoin la masse monétaire. Enfin une grande partie des dollars sont numérisés. Mais vu qu'il demeure tout de même encore des endroits sur terre où Internet n'est pas parfaitement accessible, ou bien des réfractaires à l'innovation technologique, les États ont préféré continuer d'émettre quelques dollars physique *backés* de tout manière sur la valeur de Bitcoin : le fantasme de société sans cash était une prédiction d'arrière-garde de banquiers incapables d'imaginer une vraie modernité, mais également aveugles aux dimensions sociétales de l'économie.

Nous parlions ici de valeurs cumulées de Bitcoin car ces sommes incluent la valeur de ses *sidechains*. Lui-même est la monnaie primaire étalon tandis que circulent sur les innombrables sidechains divers jetons numériques servant à tout un tas d'usages. Ainsi on trouve tout d'abord les sidechains étatiques et régionales permettant de faire levier dans l'économie quand c'est nécessaire. Puis on trouve des sidechains de services, comme celle du nouveau réseau social Ex Nihilink, gérant l'identité et la confidentialité de la majeure partie d'Internet. Mais aussi de nombreux autres services, notamment de gestion de fichiers avec des algorithmes très différents mais ayant tous une somme *backée* par des milliers de satoshis.

L'éducation a dû s'adapter, même en France, de telle sorte que les adultes de 2050 sont correctement formés à utiliser les protocoles décentralisés et surtout à gérer leurs clefs. Depuis leur plus jeune âge ils prennent l'habitude de bien stocker leurs mots de passe et de tout chiffrer, non seulement dans leur intérêt mais parce que la pression sociale (le numériquement correct) exclut de laisser un maladroit mettre en risque par ses imprudences les autres utilisateurs du système. Les *hardware wallets* peuvent désormais être des petites puces implantées sous la peau qui servent de seconde identification aux téléphones portables qui sont maintenant des parties de vêtements comme des bracelets à écran pliable, holographiques ou des lunettes de réalité augmentée.

Tous les échanges sont bien plus fluides. La transparence des blockchains des monnaies étatiques permet de surveiller les dépenses publiques, de lutter contre la corruption et d'effectuer une taxe Tobin au niveau du protocole même qui finance la sécurité sociale, les transports en commun urbains, la police, les aides publiques et enfin une partie du revenu de base qui lui aussi est intégré au niveau du protocole. Cela est possible car les sidechains étatiques sont semi-décentralisées ou « permissives ». Ainsi l'État peut répertorier les comptes des citoyens au sein du réseau pour qu'ils soient à même de recevoir un revenu de base. Ce revenu de base est partiellement assuré par une création monétaire qui n'est plus réservée aux seules banques mais distribuée à l'ensemble des citoyens d'une société donnée. Les modèles de répartition monétaire sont désormais inspirés de la TRM [166] (théorie relative de la monnaie) pour permettre une répartition équilibrée et égalitaire de la monnaie tout

en n'empêchant pas le capital, bien qu'en réduisant la durée de thésaurisation passive maximum à une trentaine d'années en moyenne selon les systèmes nationaux ou locaux.

La biodiversité monétaire permet d'avoir un équilibre plus grand et évite ainsi les crises systémiques qui étaient la caractéristique des modèles monétaires précédents. Le crédit a totalement changé de nature, il est soit un système de réserves fractionnaires sur une *sidechain*, ce qui limite la contagion systémique en cas de crise, soit – et c'est la forme de crédit la plus généralisée – des crédits P2P. L'usure classique ayant presque disparu, le placement de base d'actifs dormants est le crédit en pair-à-pair. C'est le seul moyen de lutter contre l'effet de la TRM qui fait que si un individu ne fait absolument rien de son argent sur une très longue durée son épargne stagne. Le monde est désormais pleinement *phygital* (où le numérique est totalement intégré dans le réel) avec des points de contact constants entre le cyberespace et le monde tangible. Le capitalisme n'a donc pas disparu mais il a évolué : c'est un capitalisme actif et inclusif, en total opposition avec le capitalisme de connivence, monopolistique et exclusif qui régnait encore au début du siècle et avait si bien résisté à la crise des *subprimes* et à la dépression qui la suivit.

Cette petite histoire, bien sûr naïve et fantaisiste, permet de comprendre plusieurs choses sur le futur de Bitcoin. Déjà, il est *de facto* corrélé à une multitude de facteurs que sont l'environnement politique, technologique, éducatif et bien d'autres. Le futur de Bitcoin ne peut donc pas être construit de manière isolée, du moins pour ceux qui souhaitent que les efforts de développement suscitent un écho important. D'autres bitcoineurs, au contraire, sont totalement indifférents à l'enjeu d'une diffusion à grande échelle : demeurer dans un espace monétaire confiné ne les dérange pas. Et cela pourrait aussi être un futur pour Bitcoin.

Mais l'important est de comprendre une idée qui nous tient à cœur. La révolution monétaire qu'est Bitcoin peut mener à une (r)évolution systémique globale de l'ordre de la (r)évolution verte ou de la (r)évolution numérique qui ont changé et changent encore notre monde à bien des égards. La monnaie, point central des échanges humains comme nous avons essayé de le montrer dans cet ouvrage, est un vecteur formidable de changement et d'évolution. Bien sûr, nous pourrons encore une fois être taxés de progressisme naïf ou d'idéalisme débridé, mais tel n'est pas notre sentiment. Nous ne disons pas que (tout) cela va se passer. Nous disons qu'il est possible que cela se passe, nous ne disons même pas que cela est bien, moral ou non, mais que cela aura des impacts sur les sociétés au niveau global, tout comme il est probable qu'une partie seulement de ce que nous avons décrit pourrait se passer. Voire rien.

Pourtant voici quelques pistes supplémentaires. On peut aussi raisonnablement penser à un Bitcoin étalon mais pas maître d'une diversité de méta-monnaies. Le bitcoin restant une réserve de valeur comme l'or, avec finalement assez peu de transactions journalières et des frais de transaction très élevés permettant de financer les validateurs (quand il n'y aura plus rien à miner). Bitcoin serait alors une monnaie extrêmement aristocratique permettant de mesurer la valeur plus qu'autre chose. Il serait un placement privilégié pour sa sécurité, et sa valeur approcherait celle de l'or ou d'autres grosses réserves de valeurs. Bitcoin, dans ce monde-là, ne paie pas le café et n'exécute pas de *smart contracts*. Ce sont d'autres cryptomonnaies qui le font, sans pour autant avoir une relation contraignante (ou de cours fixe) avec Bitcoin si ce n'est au niveau des plateformes d'échange. Ethereum serait peut-être la méta-monnaie la plus utilisée car les États auront choisi d'émettre leur monnaie dessus. Tous ses problèmes de jeunesse auront été résolus et de nombreuses sociétés et organisations décentralisées verront quotidiennement le jour. L'écosystème sera donc varié et l'interopérabilité un peu plus difficile.

Une autre vision peut être celle de la marginalité. Bitcoin et les méta-monnaies restent marginales. Les amateurs de « la technologie blockchain » qui va « bien au-delà de la monnaie » ont gagné. La législation est très restrictive pour les systèmes décentralisés en termes monétaires car les pouvoirs en place sont des pouvoirs quasi-totalitaires. Les seuls à les utiliser sont donc des malfrats et des abrutis. L'équilibre monétaire est inchangé et les crises systémiques peuvent rester une réalité avec le monopole des monnaies-dettes. Nous ne disons absolument pas que le changement monétaire ou économique est dépendant de Bitcoin. Mais que Bitcoin peut être un facteur déterminant dans l'évolution et le changement des systèmes monétaires.

Nous n'excluons pas non plus que tout ceci soit supplanté par l'inimaginable, ce qui est souvent le cas en prospective. Il suffit pour ça de jeter un coup d'œil aux très amusantes projections de ce que serait l'an 2000 tout au long des deux derniers siècles, c'est absolument succulent. De plus, l'équilibre géopolitique et écologique actuel fait que le monde, bien qu'il soit de plus en plus pacifique, riche, et éduqué, peut basculer assez rapidement vers des futurs très variés et fortement déterminants pour l'usage du Bitcoin et des méta-monnaies. Ajoutant à cela la

possible transition vers une époque « post-singularité » suite à l'avènement des ordinateurs quantiques, chose inenvisageable du fait de sa nature même qui dépasse toute la pensée humaine actuelle.

Ou bien pour aller encore plus loin dans le rêve et la poésie, une nouvelle conquête spatiale approchant, Bitcoin peut aussi jouer le rôle de monnaie inter-planètes… Les enjeux de synchronisation serait gigantesques (il faut 3 à 20 minutes pour relayer par exemple une transaction « terre-mars »[167]) mais l'absence de tiers de confiance aurait sans doute de grandes vertus dans une configuration aussi prodigieuse.

Le futur de Bitcoin est donc largement ouvert. Le lecteur ne devra pas examiner naïvement les prédictions de tous les devins, qu'ils soient pro ou anti-bitcoin. Pour « classer » les prédictions, nous lui conseillons de se poser la mère de toutes les questions : promet-on de nouveaux avantages (de toute nature) à l'individu ou à un système de prédation financière et de contrôle social ?

L'un des avantages du numérique et d'Internet est l'archivage des prédictions. On peut déjà voir que, sur Bitcoin, une incroyable quantité de prédictions a été effectuée. Un site s'amuse notamment à recenser les nombreuses nécrologies de Bitcoin[168]. Mais on pourrait aussi parler du très divertissant site qui avait recensé les prédictions sur le prix de Bitcoin[169]. Le futur ne nous appartient pas par avance et c'est ce qui fait sa beauté.

Nous souhaitons que le lecteur se montre à la fois tolérant et indulgent devant nos propositions. Nous sommes forcément lacunaires, et nous ne sommes pas plus éclairés que les autres, peut-être un peu plus informés sur le sujet, mais tout est relatif. Et puis le lecteur est aussi, désormais, en mesure d'imaginer des (r)évolutions possibles !

CONCLUSION

Nous l'avons dit dès l'introduction, et c'est une formule désormais consacrée, « Bitcoin est une expérience ». Or cette expérience, qui dérange et dont on a annoncé plus de cent fois l'échec, continue son développement. De nouveaux problèmes surgissent (mise à l'échelle, gouvernance…) mais surtout de nouvelles perspectives s'ouvrent pour ainsi dire chaque jour. En bref, il est trop tôt pour faire un bilan qui soit autre chose qu'un simple point d'étape. De même qu'il est trop tôt pour nommer telle ou telle personne « experte », la connaissance se mesurant encore pour l'instant par le temps consacré à l'expérimentation, à la participation aux différents aspects de la vie communautaire et à l'acquisition des savoirs les plus divers permettant à la fois le recul et la contextualisation. Bitcoin ne connaît pas d'experts (si ce n'est une dizaine de personnes dont nous ne faisons pas partie) mais des expérimentateurs.

Notre pari a été d'expliquer au lecteur les raisons pour lesquelles cette expérience devrait l'intéresser ainsi que de lui fournir des explications techniques, forcément simplifiées mais nécessaires. Sa curiosité une fois éveillée, il pourra continuer ailleurs sa recherche et sa propre expérimentation. Dans ces conditions, il nous a paru que notre conclusion devait continuer d'ouvrir des portes.

Bitcoin s'inscrit dans un mouvement de fonds, celui des « communs »

On entend souvent la critique selon laquelle le bitcoin serait une monnaie privée, pour la distinguer des monnaies souveraines, supposées être publiques [170]. C'est se tromper deux fois.

Commençons par le dire tout de go : les monnaies légales ne sont plus depuis longtemps des monnaies publiques. Indépendance des banques centrales, « capture des régulateurs » qui voit les mêmes hommes passer des établissements régulés aux organismes de régulation, non sans détour par les banques d'affaires et les cabinets ministériels, où le premier souci est parfois trop visiblement celui du carnet d'adresses à constituer plutôt que du bien public à défendre, absence de toute référence de valeur qui laisse la fixation de celle-ci aux seules forces du marché, masse monétaire constituée à 90 % de monnaies scripturales, dettes privées transformées en dettes publiques… la liste est longue des détails fâcheux qui font que les monnaies légales sont bien loin d'exprimer un lien social démocratiquement fondé.

Bitcoin est indépendant de la force publique ; cela n'en fait pas une monnaie privée, comme on l'entend parfois désigner (par ceux-là même qui vont ensuite s'inquiéter de ce qu'elle n'appartient à personne). Certes, pour celui qui le possède, le jeton de bitcoin est un bien privé, bien plus que ne l'est une créance sur la banque du coin de la rue. Mais le protocole Bitcoin est à tous, le registre de Bitcoin est ouvert et transparent. Chacun peut se servir de Bitcoin sans demander l'autorisation de quiconque, alors même que l'on doit solliciter l'accord d'une banque pour détenir un compte (quand bien même la détention d'un compte est en pratique obligatoire) et que nul n'est autorisé à ouvrir une nouvelle banque. Il faut bien garder à l'esprit qu'un contrat bancaire est à résiliation unilatérale : il est possible de quitter une banque à tout moment, mais la banque peut également chasser un client à n'importe quel moment et sans justification.

Certes la validation, par minage aujourd'hui, contre commission à terme, est devenue une fonction réservée, *de facto*, à une mince partie de la communauté. Il y a un aspect évidemment non démocratique à cela, même si ce n'est pas aux membres du club ultra-sélectif des établissements de crédit (6 groupes bancaires seulement en France) de s'en offusquer. On a parlé de ploutocratie (mais le minage est-il aujourd'hui aussi rentable que la

banque ?) ou d'aristocratie : on pourrait forger le terme de « hashocratie ». Il faut quand même souligner un alignement des intérêts entre mineurs et bitcoineurs de base qui, loin d'être parfait (cf. les débats comme celui de la taille du bloc) n'est pas à moquer quand on songe à ce qu'il en est dans le paysage bancaire, qui a vu tant de fois des banques jouer contre leurs clients, que ce soit en conseil ou sur les marchés.

Tout ceci posé, ce dont Bitcoin est le plus proche, c'est ce que l'on désigne de plus en plus sous le vieux nom historique de biens « communs ». Sont privés, explique l'économiste Gaël Giraud (dans son *Illusion financière*) les biens dont la possession est exclusive et entre en rivalité avec celle des tiers. Sont publics ceux qui ne sont ni-exclusifs ni-rivaux (l'éclairage public). Mais il existe bien des hybrides. Ainsi l'air que l'on respire est un bien non-exclusif, mais non rival et il n'est pas public pour autant. La « Nobel » d'économie en 2009, Elinor Ostrom (1933-2012) a appelé « communs » les biens qui sont non-exclusifs (difficile d'interdire vraiment l'accès à une rivière) mais rivaux (le poisson pêché par Jacques ne le sera plus par Adli). Selon Ostrom et Hess, les « communs » ne sont pas à proprement parler des « biens » matériels, mais, dit Gaël Giraud, « des systèmes de règles régissant des actions collectives, des modes d'existence et d'activité de communautés ». Ne pourrait-on pas reprendre cette définition pour un protocole comme Bitcoin ?

Giraud lui-même considère que la liquidité et le crédit « devraient être organisés à la manière de communs » (ce qui n'implique pas forcément pour lui comme pour nous que la monnaie soit intrinsèquement un commun, ou qu'elle soit répartie avec une égale distribution, même si une distribution égalitaire au moment de la création monétaire peut être envisagée) : « aucun citoyen ne devrait être exclu de l'accès à la monnaie, en d'autres termes la liquidité monétaire devrait être un bien non exclusif… à la manière d'une zone de pêche ».

Du fait que, dans la pratique, tous les biens naturels (menacés) sont des « communs », cette théorie a suscité un intérêt particulier chez les écologistes. Cependant, ceux-ci manifestent une hostilité non dissimulée à Bitcoin pour deux mauvaises raisons. Premièrement sa consommation énergétique provoque une hostilité qui n'est compréhensible que pour celui qui considèrerait l'empreinte énergétique de la monnaie-dette comme inférieure, et l'on a vu combien c'était loin d'être le cas, ou qui négligerait par ignorance ou malice le fait qu'il est assez facile de faire des mines autonomes en énergie, avec le solaire par exemple. Deuxièmement, leur attachement (partagé par les auteurs !) aux circuits courts leur donne une foi naïve dans les monnaies locales, dont malheureusement la capacité de régénérer le commerce local est une mythologie dont les supporters eux-mêmes peinent à vérifier l'efficacité en pratique. Que ces équivoques soient levées et Bitcoin apparaîtra au contraire comme un protocole riche en potentialités techniques et sociétales au service des fins qu'ils poursuivent.

Les changements réels qu'apportera Bitcoin sont multiples, du paiement au travail

On a déjà passablement risqué des hypothèses, notamment en fin de dernier chapitre, quant au chemin que peut prendre Bitcoin. Focalisons-nous ici sur ce qu'il pourrait changer. Si l'on pense, comme le disait Oresme au XIV^e^ siècle, que le paiement est au cœur du commerce (ce pourquoi la monnaie appartient à ceux qui la gagnent et l'échangent, non à ceux qui la fabriquent, surtout *ex nihilo*, ou qui la régulent), on ne peut qu'imaginer de profondes mutations sociétales. Aujourd'hui le bitcoineur apparaît comme un jeune (souvent, pas toujours) original, technophile maniaque, qui fait de façon bien bizarre ce que l'on peut faire plus simplement, bref un peu *snob* si l'on reprend la définition que donnait en artiste Salvador Dalí : « Le snobisme consiste à pouvoir se placer toujours dans les endroits où les autres n'ont pas accès »[171]. Exactement comme les premiers automobilistes roulant tant bien que mal sur des routes prévues pour les diligences, qui ont vécu ce qu'Andeas Antonopoulos décrit comme la phase d'inversion des infrastructures[172], cherchant de l'essence et trouvant du foin, crevant toutes les 20 bornes et menant un train d'enfer. Ces pionniers ont changé non pas le monde de la technique ou les routes du monde, mais l'homme lui-même, ses symboles, son travail, ses loisirs, sa famille et sa connaissance des autres hommes.



Si Bitcoin progresse comme instrument (de paiement, de transaction, d'échange de preuves, de contournement des tiers de confiance), il sera – dans 50 ans – aussi profondément inscrit que ne l'est le système actuel dans les représentations spontanées. Celles-ci sont un mixte passionnant de choses fausses parce que périmées et de choses vraies mais démentes. Certains croient encore qu'il y a une valeur en gage dans les banques centrales (de l'or, du dollar, on entend de tout quand la question est soulevée) ou des dépôts dans les banques pour consentir des crédits ; le plus surprenant est pourtant de voir comment l'absence de toute référence à quelque valeur que ce soit est aujourd'hui largement intériorisée. On a ici envie d'évoquer le magnifique faux coffre-fort supposé contenir la recette secrète, dans le musée Coca-Cola d'Atlanta. Ce qui était scandale pour Gide écrivant ses *Faux-Monnayeurs* [173], étudiés par Jean-Joseph Goux, ce qui était inacceptable pour le Général De Gaulle, est devenu aujourd'hui la norme présentée non comme un accident historique mais comme un progrès conceptuel.

Quand on lit en tête de l'article *Monnaie* de Wikipedia, juste après la mention canonique des trois fonctions citées par Aristote que « ces définitions anciennes persistent mais doivent être amendées entre autres, par la suppression de toute référence à des matières précieuses (à partir du IV^{e} siècle en Chine) » on tombe des nues : c'est nous qui sommes contraints, non d'amender (améliorer, rendre meilleur) mais bien de polluer la pensée du Stagyrite par ce qui s'assimile bien mieux à un cache-misère qu'à un progrès. Qui a considéré le « doigt d'or » du 15 août 1971 [174] comme une contribution théorique indépassable à la définition de la monnaie ? Ce qui fut « une décision sémiotique, une révolution de la notion même de signe ou d'écriture, ou dans le rapport de subordination habituelle de la réalité à la symbolicité [175] » devient une chose tellement banale qu'on peut l'oublier pour ne pas déranger le confort intellectuel de nos contemporains : il suffit de corriger le passé. Quant à l'histoire des billets chinois, c'est négliger les faillites et les émeutes qui émaillèrent leur histoire et confondre (quel aveu !) le support matériel d'un reçu avec la référence à un étalon.

Autant dire que Bitcoin, en se développant, continuera d'apporter son propre mélange de concepts et de mythes.

Le bitcoin et les autres « disrupteurs » sont à l'origine d'un nouvel écosystème sociétal et politique

Il ne progressera pas seul. Quelle que soit l'incertitude évoquée à la fin de cet ouvrage sur son usage propre et premier (monnaie fluide, monnaie réserve, monnaie marginale), quelle que soit la part respective des autres crypto-jetons construits à sa ressemblance, pour le concurrencer ou le compléter, quelle que soit l'attitude des États face aux crypto-jetons monétaires, des tribunaux face aux contrats auto-exécutables, des polices face aux échanges anonymisés et décentralisés, des fiscs envers une traçabilité affichée en cas de besoin mais pratiquement limitée dans une nébuleuse incroyable d'instruments et de réseaux, il y a un fait majeur : la capacité de rendre un objet numérique unique fait que Satoshi Nakamoto a ouvert une porte, comme Gutenberg, comme Colomb, comme Turing. Son Bitcoin est moins la monnaie de l'Internet que, comme le dit Andreas Antonopoulos, l'*Internet de la Monnaie* un nouveau monde de transactions.

Ici une remarque fondée sur le vocabulaire français. Dans le premier Dictionnaire de l'Académie (1694), le mot *commerce* signifie d'abord « trafic, négoce de marchandises, d'argent, soit en gros, soit en destail mais aussi, communication & correspondance ordinaire avec quelqu'un, soit pour la société seulement, soit aussi pour quelques affaires ». Il reste bien peu probable que Bitcoin modifie l'un des aspects du commerce sans modifier l'autre. On peut même penser (comme les auteurs du présent livre) que c'est parce que le commerce entre les gens change, se fait en réseau, horizontal, souvent pseudonyme, que les relations commerciales changent aussi.

De même peut-on penser que l'origine du mot « économie », du grec *οἰκονομία*, « la gestion du foyer », peut nous éclairer sur la force de Bitcoin. Il est bon que chacun puisse participer activement à la vie du foyer. Avec Bitcoin, cette possibilité est de nouveau donnée à chacun, grâce à son code libre et ouvert appartenant à tous. Ce ne sont plus des institutions privées, des privilégiés qui sont garants du foyer, mais une multitude de personnes, agissant avec diligence de leur plein gré. À la manière de ce que l'on observe dans cette *do-ocratie* reconnue qu'est Wikipédia, où le « pouvoir du faire » est une forme d'auto-organisation dans laquelle les individus s'assignent à eux-mêmes des tâches et les exécutent.

Les sens étendus du mot *οἰκονομία* sont donc eux aussi opportuns : ainsi Bitcoin permet-il une meilleure « organisation » et peut-être une meilleure « distribution » par ses caractéristiques intrinsèques.

Il est peu probable, alors même que les systèmes démocratiques donnent tant de signes de fatigue, qu'un instrument offrant une nouvelle façon de voter reste sans conséquences. Ce ne sont pas tant les idéaux démocratiques, en effet, qui sont épuisés ou remis en cause, le plus souvent, que leur travestissement par un mixte d'oligarchie (caste) et de ploutocratie (pouvoir total de l'argent dans les marchés mais aussi dans les médias) et l'obsolescence des procédures : est-il normal que les finalistes d'une élection soient tous deux aussi décriés ? Que l'élu soit illégitime presque le lendemain de son élection ? Les échanges décentralisés permettront d'entrevoir d'autres mécanismes, le jour où les hommes, émancipés des sujétions infantiles, décideront enfin de voter leurs lois et non plus d'élire leurs rois.

Décidément, c'est bien, du début à la fin du livre, d'enlever l'effigie des puissances tutélaires et les majestueux profils des autorités sur toutes sortes de médailles qu'il a été question, en commençant par la monnaie acéphale !

NOTES

Le lecteur trouvera ci-dessous les références complètes étayant certaines assertions dans le corps du texte. Ne sont citées, dans les sources imprimées, anciennes ou modernes, que des œuvres dont les auteurs estiment la lecture profitable.



Un QR Code vers notre site

En ce qui concerne les documents numériques, ce sont soit des sources brutes, soit des textes ou discussions reprenant ou synthétisant une question et permettant au lecteur de se laisser porter par la sérendipité du web. À cet égard, et pour permettre au lecteur une recherche commode, les pages de notes de cet ouvrage avec des liens actifs ont été mis en ligne par les auteurs à l'adresse suivante : http://bitcoinlamonnaieacephale.fr. Le lecteur y trouvera également des ressources documentaires et un espace de commentaires permettant l'échange.

Introduction

1. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, octobre 2008, en ligne en traduction française sur le site Gitbook.com et dans la page « salle de lecture » sur le blog *La Voie du Bitcoin* (http://blog.lavoiedubitcoin.info/public/Bibliotheque/Nakamoto.pdf). Version originale : https://bitcoin.org/bitcoin.pdf.

2. John Maynard Keynes, *Théorie Générale* (1936), Introduction.

I. Sidérant bitcoin

3. « L'empirisme primaire peut être pire que toute autre forme de sottise quand il met les gens en confiance », selon Nassim Taleb, *Le Hasard sauvage*, Paris, Les Belles-Lettres, 2008, page 100.

4. Cité par Andreas Antonopoulos en exergue de son livre *Internet of Money,* 2016.

5. Philip Zimmermann, *Pourquoi j'ai écrit PGP ?* (première version 1991, réédition 1998), en ligne.

6. Tim May, *Manifeste crypto-anarchiste*, 1992, traduction en ligne notamment sur le site *La revue des Ressources* ici : http://www.larevuedesressources.org/manifeste-crypto-anarchiste,2316.html

7. Eric Hughes, *Manifeste d'un Cypherpunk*, 1993, traduction en ligne notamment sur le site *Terminator Studies* ici : http://terminatorstudies.org/html/589422319753363456.html.

8. Christian As. Kirtchev, *Cyberpunk Manifesto*, 1997, traduction en ligne notamment sur le site *La Revue des Ressources*, ici : http://www.larevuedesressources.org/un-manifeste-cyberpunk-le-cyberpunk-manifesto,2317.html.

9. *Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux*, rapport de la Commission présidée par M. Pierre-Antoine Gally, 2015, en ligne ici : http://www.lecese.fr/sites/default/files/pdf/Avis/2015/2015_10__nouvelles_monnaies.pdf.

10. Michel Foucault, *Surveiller et Punir,* 1975.

11. « Un million de dollars en deux heures pour SuperNET » : https://le-coin-coin.fr/1205-million-dollars-en-heures-supernet/

12. Nassim Nicholas Taleb, *Antifragile, Things That Gain from Disorder*, 2012, disponible en ligne sur un site dédié à un cours de l'université de Pennsylvania : http://cpor.org/af/Taleb_Antifragile.pdf.

13. Au commencement, des bugs et des failles ont pu être constatés et réparés avant que Bitcoin n'ait une telle importance financière. On verra, par exemple, celui-ci où Jeff Garzik avait détecté un problème assez sérieux : https://bitcointalk.org/index.php?topic=822.0.

14. La note blanche de Lamport, Shostak et Pease, publiée en 1982, est en ligne ici : http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf. Il en existe une présentation en langue française par Aymeric Lesert (http://aymeric.lesert.pagesperso-orange.fr/expose/dea/byzantin/algorithmes.pdf). En 1983, Michel Ben-Or avait publié son étude *Another Advantage of Free Choice: Completely Asynchronous Agreement Protocols* qui fait date dans l'histoire du consensus. Enfin on peut aussi lire l'article *Asynchronous Byzantine Agreement Protocols* publié en 1987 par Gabriel Bracha et qui est en ligne ici : http://www.sciencedirect.com/science/article/pii/089054018790054X.

15. Réunissant, après la dernière guerre, des malfrats mâtinés de collaboration, le « gang des tractions Avant » entre dans la chronique avec l'attaque d'un fourgon du Crédit Lyonnais, le 7 février 1946, avenue Parmentier à Paris. À bord de deux Citroën du modèle éponyme, « Pierrot le Fou » et ses complices s'emparent de trois millions de francs. Le gang commettra cette année-là une dizaine de hold-up. Il a suscité des romans et des films de Jacques Deray (*Le Gang* avec Alain Delon) et Claude Lelouch (*Le Bon et les Méchants* avec Jacques Dutronc) et il est cité par Mc Solaar dans la chanson *Quand le soleil devient froid*. Loin d'être interdite, la Traction-Avant restera produite jusqu'en 1957. Sa notice Wikipedia explique sobrement que « son histoire est liée dans la mémoire collective à l'Occupation, tour à tour voiture de la Gestapo et icône de la Résistance. Elle est également le véhicule préféré des gangsters en raison de qualités routières exceptionnelles pour son époque. »

16. L'historique de l'idée consistant à contraindre les machines à résoudre des puzzles, énigmes ou problèmes mathématiques pour réduire le spam en rendant le courrier électronique « coûteux » à envoyer comme le courrier physique est reprise ici : http://www.hashcash.org/papers/ ; lire en particulier A. Back, *Hashcash, a denial of service counter-measure* : http://www.hashcash.org/papers/hashcash.pdf, 2002.

17. Voir note 1.

18. Nombre de nœuds, ici comptabilisés par la société 21 : https://bitnodes.21.co/.

19. http://jasondrowley.com/2015/12/04/the-bitcoin-network-is-11000x-faster-than-the-top-500-supercomputers-combined/#easy-footnote-1. Calcul réactualisé en décembre 2015 par rapport à un calcul de Forbes de 2013 : http://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/.

20. Ricardo Perez-Marco (CNRS), conférence à la Société Informatique de France le 15 novembre 2016.

21. Jean-Paul Delahaye (Université Lille I) le même jour à la conférence de la SIF, reprenant par ailleurs une assertion déjà formulée. On trouvera sur le blog de Jean-Paul Delahaye d'intéressants éléments dans les billets : http://www.scilogs.fr/complexites/lattaque-goldfinder-dune-blockchain/ http://www.scilogs.fr/complexites/contenu-en-calcul/ http://www.scilogs.fr/complexites/epee-de-damocles-bitcoin/.

22. On verra un peu plus loin, au point II, 1, que l'intervalle entre deux blocs suit une loi exponentielle, et que ce n'est pas sans conséquences (positives) sur la sécurité du protocole.

23. « Ἀπόδοτε οὖν τὰ Καίσαρος Καίσαρι καὶ τὰ τοῦ Θεοῦ τῷ Θεῷ. » (Rendez donc à César ce qui est à César et à Dieu ce qui est à Dieu) dans les évangiles de Matthieu, XXII,21, Marc, XII, 17 et Luc, XX, 25.

24. D. Bayer, S. Haber, W.S. Stornetta, « Improving the efficiency and reliability of digital time- stamping », dans *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

25. Pierre Noizat, *Bitcoin, mode d'emploi*, 2015, page 54.

26. Données recueillies sur blockchain.info : https://blockchain.info/charts/n-transactions-per-block?timespan=all.

27. R.C. Merkle, *Protocols for public key cryptosystems*, dans *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, avril 1980.

28. Voir note 1.

29. Au sujet du problème de la « base monétaire », on se reportera avec intérêt à la page 95 de l'ouvrage de Nicolas Bouleau, *Martingales et marchés financiers,* Paris, Odile Jacob, 1998. Faire ses comptes en bitcoin serait un pari probabiliste a priori sur l'avenir. « Dès lors que les devises ont des transactions bruitées les unes par rapport aux autres, faire ses comptes dans une monnaie ou une autre n'est pas indifférent. »

30. La chose est peut-être ignorée du grand public, mais elle n'est pas secrète. Voir le document « Qui crée la monnaie ? », mis en ligne en septembre 2015 par la Banque de France https://www.banque-france.fr/uploads/tx_bdfpatchirfaq/NI_Monnaie_09_2015.pdf.

31. Compte-rendu de la Commission des affaires économiques, mardi 14 juin 2011, séance de 17 heures (Compte rendu n° 77) sur le site de l'Assemblée Nationale.

32. Zoltan Jakab et Michael Kumhof, *Banks are not intermediaries of loanable funds – and why this matters*, Working paper n°529 de la BoE, mai 2015, en ligne sur son site. Une autre lecture intéressante : Michael McLeay, Amar Radia and Ryland Thomas, *Money in the modern economy : an introduction*, Bulletin de la BoE pour le premier trimestre 2014, en ligne sur le site de la BoE et en traduction française sur le blog d'Alain Grandjean: https://alaingrandjean.fr.

33. C'est clairement ce que sous-entend André Gide dans *les Faux-Monnayeurs* publiés en 1925. Voir Guillaume Bardet et Dominique Caron, *Les Faux-Monnayeurs*, Paris, Ellipses, 2016.

34. La position d'Europol a plusieurs fois changé. En janvier 2016 l'organisme relativisait très fortement la réalité d'un usage de Bitcoin par les terroristes :

https://www.europol.europa.eu/sites/default/files/publications/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf. En septembre 2016, un partenariat Interpol-Europol-Basel Institute for Governance était annoncé pour lutter contre le blanchiment de bitcoin en relation avec le terrorisme. « There is a clear consensus that digital currencies pose a money laundering and terrorism financing threat » lisait-on dans le communiqué, qui avouait ensuite n'en avoir trouvé que fort peu d'exemples.

35. Étienne de la Boétie, *Discours de la servitude volontaire*, rédigé en 1549, première édition en 1576. Texte majeur de la philosophie politique, écrit par un humaniste de 18 ans et souvent invoqué dans les écrits anarchistes ou libertaires. À noter que La Boétie établit une relation entre une économie de la rivalité de chacun contre tous et la tyrannie.

36. Publication du *leak* listant le domaine des adresses piratés ainsi que les mots de passe les plus utilisés : https://www.leakedsource.com/blog/friendfinder.

37. Pour être plus précis la clef privée est une suite en hexadécimal (0-9 A-F / base 16) de 64 caractères, mais en caractères lisibles elle fait 51 caractères quand elle est associée à une clef publique non-compressée et 52 caractères quand elle est associée à une clef publique compressée. C'est cet encodage que nous voyons le plus fréquemment, cf. https://en.bitcoin.it/wiki/Private_key.

38. Pour se rendre compte du nombre de solutions : http://directory.io/ qui est la liste de toutes les clefs privées du monde, et pourtant il n'y a aucun risque de tomber sur la clef de quelqu'un en se baladant sur le site. Voir aussi cette discussion pour imaginer ce vertige : https://www.reddit.com/r/Bitcoin/comments/3faio9/counting_sand_and_bitcoin_addresses/.

39. Taille relevée sur blockchain.info : https://blockchain.info/fr/charts/blocks-size.

40. Article de *Science* montrant précisément l'aspect non secret de Bitcoin : http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

41. Voir note 19.

42. Il s'agit d'une estimation livrée en septembre 2016 par l'un des auteurs du site Bitcoin.fr (article « Bitcoin au Tibet », en ligne ici https://bitcoin.fr/bitcoin-au-tibet/) et qui nous a paru vraisemblable ; il faut toutefois souligner qu'elle repose sur un empilement d'hypothèses (puissance de calcul, âge et efficience des matériels de minage employés). Pierre Noizat (note 82) tablait en novembre 2015 sur 250 MW.

43. Le nombre de liens potentiels dans un réseau comptant n nœuds est n(n-1)/2 et cette fonction est équivalente à ½ n^2 lorsque n tend vers l'infini. L'utilité d'un réseau est donc, selon la remarque de Robert Metcalfe, proportionnelle au carré du nombre de ses utilisateurs. C'est une loi empirique qui a par ailleurs été critiquée.

44. Gilles Châtelet, *Vivre et penser comme des porcs*, Paris, Exils, 1998, chapitre 11. Merci à Antoine Favier pour la référence.

45. Maurizio Lazzarato est un sociologue et philosophe italien indépendant, résidant à Paris et auteur notamment de deux ouvrages importants, *La fabrique de l'homme endetté : Essai sur la condition néolibérale* (Editions Amsterdam, 2011) et *Gouverner par la dette* (Les Prairies ordinaires, 2014). Ce dernier livre est évoqué dans le billet n° 18 du blog *La Voie du Bitcoin*.

46. Les exemples sont innombrables. Les fouilles entreprises par Louis Malleret, dans les années 1940, ont permis de retrouver des pièces romaines dans des tombes du Mékong. Encore en septembre 2016 des fouilles sur l'île d'Okinawa au Japon, ont exhumé des pièces romaines, une première sur le territoire japonais où les anciens Romains n'ont jamais été.

II. Le bitcoin, sans mystère ni fantasme

47. *The limits to growth,* Donella H. Meadows, Dennis L. Meadows, Jorgen Randers William W. Behrens III, Universe Books, 1972, disponible en ligne ici : http://www.donellameadows.org/wp-content/userfiles/Limits-to-Growth-digital-scan-version.pdf.

48. Dictionnaire numérisé sur ce site : http://www.furetière.eu

49. Papier décrivant l'algorithme publié par le NIST : http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

50. Bitcoin utilise une courbe elliptique précise, à savoir la courbe secp256k où $y^2 = x^3+7$ dans un corps fini (on dit aussi un champ de Galois) de cardinal p, avec p égal à $2^{256}-2^{32}-2^9-2^8-2^7-2^6-2^4-2^0$ soit un nombre à 78 chiffres, lire : https://en.bitcoin.it/wiki/Secp256k1.

51. Toutes les règles du protocole sont bien résumées ici : https://en.bitcoin.it/wiki/Protocol_rules.

52. Pierre Noizat sur son blog http://e-ducat.fr/2013-12-21-lattaque-des-selfish-miners/. Silvio Micali, dans sa publication *Algorand* http://arxiv.org/pdf/1607.01341.pdf

53. Toutes les données peuvent être vérifiées en ligne au chapitre 7 de Mastering Bitcoin : http://chimera.labs.oreilly.com/books/1234000001802/ch07.html ou à l'aide de cet excellent article : https://codesuppository.blogspot.fr/2014/01/how-to-parse-bitcoin-blockchain.html ou enfin grâce au wiki Bitcoin : https://en.bitcoin.it/wiki/Block#Block_structure, données réunies dans une infographie très claire traduite en français par BitConseil : http://bitconseil.fr/wp-content/uploads/2016/03/bitcoin-blockchain-infographic-fr.pdf.

54. Cet « identifiant magique » permet d'identifier le début d'un bloc et correspond à 0xD9B4BEF9. Voir https://bitcoin.stackexchange.com/questions/2337/how-was-the-magic-network-id-value-chosen.

55. Cette notion d'extranonce est assez peu connue. Elle est cependant très fine. En effet le nonce de base est beaucoup trop limité (en terme de bits : 2^{32} soit près de 4 milliards) pour permettre la résolution de la difficulté dans la plupart des cas. Les autres facteurs d'ajustement du hasard sont donc des éléments capitaux de la belle mécanique qu'est Bitcoin, qu'il s'agisse du *timestamp*, de la possibilité de permutations des transactions au sein du bloc (dans l'hypothèse d'un bloc de 1000 transactions il y a factorielle 1000 possibilités, soit un nombre à 2568 chiffres) et enfin de l'extranonce (mais changer la *coinbase* requiert de recalculer tout l'arbre de Merkle, ce qui en fait la solution la plus coûteuse en énergie). On peut voir différents échanges à ce sujet sur des forums, pour approfondir la notion : https://bitcointalk.org/index.php?topic=1040859.msg11222991#msg11222991 https://bitcointalk.org/index.php?topic=9438.0 et https://bitcoin.stackexchange.com/questions/5048/what-is-the-extranonce. Ces explications non académiques mais exprimées par des

membres « légendaires » du forum Bitcointalk ou par des personnalités reconnues comme Pieter Wuille peuvent être considérées comme fiables dans le monde réputationnel qu'est Bitcoin.

56. La clef privée a été générée à partir de ce site : https://coinb.in/#newAddress non pas aléatoirement mais avec pour *custom seed* « Bitcoin, la monnaie acéphale » et avec l'option de compression des adresses. Vous pouvez essayer et vous devriez tomber sur les mêmes valeurs. N'envoyer cependant aucun bitcoin à cette adresse qui est désormais « grillée » !

57. Voir ces pages pour plus de détails sur la raison de la variété possible du nombre précis de caractères dans les adresses : https://bitcoin.stackexchange.com/questions/36944/what-are-the-minimum-and-maximum-lengths-of-a-mainnet-bitcoin-address ou https://en.bitcoin.it/wiki/Address ou https://bitcointalk.org/index.php?topic=613068.0. La taille minimale est de 26 caractères pour les adresses connues : http://pastebin.com/KJmYYmtC. Tout cela dépend en réalité du préfixe d'adresse choisi par Satoshi : https://en.bitcoin.it/wiki/List_of_address_prefixes.

58. Taille relevée sur blockchain.info : https://blockchain.info/fr/charts/blocks-size.

59. Benoît Mandelbrot, *Une approche fractale des marchés*, Paris, Odile Jacob, 2004, page 249. La lecture de ce livre antérieur tant à la crise des *subprimes* qu'à l'apparition de Bitcoin reste un antidote indispensable à la vanité et à la suffisance de bien des exposés sur l'efficience des marchés et sur la pertinence des modèles mathématiques qui y sont mis en œuvre.

60. Ajout réalisé pour compléter des faiblesses de nLocktime à la suite de la *Bitcoin Improvement Proposal* (BIP65) de Peter Todd : https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki et intégré fin 2015 dans Bitcoin 0.11.12 https://bitcoin.org/en/release/v0.11.2.

61. Nick Szabo, Smart Contracts : http://virtualschool.edu/mon/Economics/SmartContracts.html.

62. Vidéo consultable ici : https://www.youtube.com/watch?v=N7j8LnBvlp0.

63. Numérama, *Sandy Bridge : Intel ajoute un DRM dans ses processeurs*, 2011, http://www.numerama.com/magazine/17759-sandy-bridge-intel-ajoute-un-drm-dans-ses-processeurs.html.

64. S. Haber, W.S. Stornetta, *_How to time-stamp a digital document*, dans le *Journal of Cryptology*, Vol. 3, n°2, pages 99-111, 1991 et *op. cit.* note 22.

65. La probabilité de réussite d'une double-dépense peut être estimée en remplaçant grossièrement une loi binomiale négative par une loi de Poisson. Cela a été expliqué par Meni Rosenfel dans un article de 2012, « Analysis of hashrate-based double-spending » (en ligne : https://bitcoil.co.il/Doublespend.pdf). Cyril Grunspan et Ricardo Perez-Marco, en reprenant ces calculs, ont montré que ladite probabilité peut s'exprimer simplement à l'aide d'une formule fermée mettant en jeu une seule fonction béta régularisée incomplète, et ensuite que cette probabilité tend exponentiellement vers 0 en fonction du nombre de confirmations reçues. Ce résultat était souvent cité mais semble-t-il de manière purement intuitive. Ils ont aussi donné d'autres formules plus fines en prenant en compte les temps de minage. Voir la fin de la conférence du 2 janvier 2017 à Paris 7 en ligne sur https://bitcoin.fr/video-paiements-securises-et-non-securises-sur-une-blockchain-2eme-partie. Voir aussi le résumé en langue française publié par Grunspan : http://cyrilgrunspan.fr/index.php/2017/02/10/supplement-a-letude-du-bitcoin/

66. En théorie, du moins, et en l'absence de « famine monétaire » comme celles que connaissaient les hommes de certaines époques au Moyen Âge. On lira avec intérêt le petit ouvrage de jeunesse de Laurent Feller *Faux-Monnayeurs et fausses monnaies en France à la fin du Moyen Âge,* Paris, Le Léopard d'or, 1986.

67. Article de Marie Lafitte, Florent Brousse, Laurent Noël, Yvan Gaillard et Gilbert Pépin : « Traces de stupéfiants sur les billets, in Revue de la Société française de toxicologie analytique », http://cat.inist.fr/?aModele=afficheN&cpsidt=13774974.

68. Nicolas Oresme, *Traité des Monnaies*, au chapitre VI : « La monnaie est l'étalon de la permutation des richesses naturelles ; elle est donc la possession de ceux auxquels appartiennent ces richesses. En effet, si quelqu'un donne son pain ou le labeur de son propre corps pour de l'argent, une fois qu'il l'a reçu, il est à lui comme l'était le pain ou le labeur de son corps. »

69. Souvent cité de manière générale, la distinction par Aristote des trois fonctions se déduit du livre I du *Politique* et ne doit pas être confondue avec le cinquième livre de *l'Ethique à Nicomaque* dans lequel il déclare que la monnaie est un fait légal qui n'existe pas dans la nature.

70. Note en consultation libre : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62014CJ0264&from=FR.

71. Friedrich Hayek, *The denationalization of money*, 1976, traduit en français sous le titre *Pour une vraie concurrence des monnaies*, Paris, PUF, 2015.

72. Simulation des différents temps de confirmation et leur impact : https://arthurgervais.github.io/Bitcoin-Simulator/results.html Résumé des arguments pour et contre : http://bitcoin.stackexchange.com/questions/1863/why-was-the-target-block-time-chosen-to-be-10-minutes/1864 Avis de Mike Hearn et raison de Satoshi en discours rapporté : https://www.reddit.com/r/Bitcoin/comments/30lxo4/replace_by_fee_a_counter_argument_by_mike_hearn/cptwk21/

73. Site s'amusant à recueillir les avis de décès de Bitcoin : https://99bitcoins.com/bitcoinobituaries. Le site recensait 118 avis à fin 2016. Un chiffre fort proche du nombre de BIP (propositions d'amélioration du protocole), et deux raisons de penser que Bitcoin aura raison des oiseaux de mauvais augure.

74. On trouve des condamnations à mort ou de simples faire-part signés de Paul Krugman, Robert Shiller ou Joseph Stiglitz. Un cryptologue franco-polonais de University College à Londres, Nicolas Tadeusz Courtois, s'est également fait une spécialité de prononcer sans trop de démonstration que Bitcoin est *extrêmement déficient* (lire ici : https://bitcoin.fr/bitcoin-est-un-systeme-extremement-deficient/). Il avait pris en avril 2016 le pari que l'algorithme *ECDSA (Elliptic Curve Digital Signature Algorithm)*, utilisé dans Bitcoin pour la signature des messages de transaction, serait cassé avant la fin de l'année (https://bitcoin.fr/le-pari-manque-de-nicolas-t-courtois/). Ses thèses, que l'on trouvera présentées dans une conférence mise en ligne (https://bitcoin.fr/video-etat-de-lart-de-la-securite-des-blockchains) suscitent des réserves même chez les universitaires.

75. Voire le documentaire d'Arte sur Ponzi : http://www.arte.tv/guide/fr/048693-000-A/le-systeme-de-ponzi.

76. Citation de *Monnayé*, 32ème tome des *Annales du Disque Monde* du défunt Sir Terry Pratchett (titre original : *Making Money,* 2007).

77. Les transactions en coquillages (en cauris, pour les appeler par leur nom) formant un marronnier de la littérature monétaire, autant se référer aux meilleures sources, les publications de Pierre P. Edoumba, *Aperçu sur les systèmes monétaires africains,* 2001, en ligne sur Persée et de Francis Dupuy, *Les monnaies primitives*, 2009, en ligne sur Cairn-info.

78. La fameuse citation sur la « relique barbare » mériterait d'être faite avec scrupule. Dans son ouvrage *A Tract on Monetary Reform* (1923) où il plaide contre le retour de l'étalon-or, il souligne le risque de privilégier la stabilité des changes au détriment de celle des prix nationaux. La formule « l'étalon-or est déjà une relique barbare » ne vise pas le métal mais le système monétaire construit dessus.

79. Un article résumant bien la question : http://www.bitcoinnotbombs.com/bitcoin-vs-the-nsas-quantum-computer/.

80. Voir cette article du *Financial Times* qui fait le point sur les avancées des diverses banques centrales : https://www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a.

81. Voir note 42.

82. Pierre Noizat, sur son blog : http://e-ducat.fr/2015-11-28-cop21-et-blockchain/, a une estimation (250 MW) un peu basse de la puissance pour bitcoin, nous avons suivi l'estimation de l'ordre de 423 MW (voir note 42).

83. Fiodor Dostoïevski, dans *Souvenirs de la maison des morts,* 1862.

84. Voire note 100 pour plus de détails.

85. Voir le Graphique 1 dans cette étude de Natixis : https://www.research.natixis.com/GlobalResearchWeb/Main/GlobalResearch/DownloadDocument/OX2UPzH-2VJ_z_O_tuopoQ%3D%3D

86. Au sujet des bitcoins perdus, voir note 111.

87. On trouve trois fonctions légèrement différentes déduites et énoncées par Jean-Joseph Goux dans *Les monnayeurs du langage*, Paris, Galilée, 1984, pages 50 sqq et 172 : l'archétype, le jeton et le trésor.

88. Le « Cercle du Coin » a été à l'initiative, en novembre 2016, de la conversion de ce lieu parisien historique et élégant qui est ainsi devenu le premier « Bitcoin Boulevard » français. Toujours dans l'idée de populariser la monnaie cryptographique auprès des publics les plus divers, le Cercle a également encouragé le projet d'un Youtubeur français, Raj, « Autodisciple » qui s'est assigné le défi de « vivre 30 jours en bitcoins ». Cette expérience a été menée en janvier-février 2017, on peut la suivre sur le site https://www.youtube.com/autodisciple

89. Voltaire, *Candide*, 1759.

90. Voir note 68.

91. Voir notamment ce qu'en dit David Graeber au chapitre 2 de son livre *Dette, 5 000 ans d'histoire*, Paris, Les liens qui libèrent, 2011, notamment page 34 et note 6.

92. Maurice Joly, *Dialogue aux enfers entre Machiavel & Montesquieu*, Bruxelles, 1864.

93. Elle ne fut pas la seule. Un homme d'affaires plein d'humour assurait en privé s'être à l'époque plusieurs fois « réveillé la nuit en sueur en se demandant s'il était assez endetté. »

94. Bien des discours contre Bitcoin pourraient enrichir l'étude de Laure Belot, *La déconnexion des élites. Comment Internet dérange l'ordre établi,* Paris, Les Arènes, 2015.

95. Étude de 2010 du Crédit Agricole : https://www.ca-cotesdarmor.fr/Vitrine/ObjCommun/Fic/CotesdArmor/CondGenBanque/Parlons_clair.pdf, *Alternatives Économiques*, 2011 : http://alternatives-economiques.fr/blogs/gloukoviezoff/2011/11/01/au-moins-5-millions-d%E2%80%99exclus-bancaires-selon-le-gouvernement/, Rapport de l'observatoire de l'inclusion bancaire, Banque de France, 2016 : *http://www.lesclesdelabanque.com/Web/Cdb/ActeursSociaux/Content.nsf/DocumentsByIDWeb/AEFDFJ/$File/Rapport-de-l-observatoire-de-l-inclusion-bancaire-2015.pdf.*

96. Le chiffre de 10 millions de *unbanked* aux USA est donné par la Federal Deposit Insurance Corporation (FDIC) dans une étude de janvier 2011 intitulée « Tapping the Unbanked Market », en ligne ici : https://web.archive.org/web/20110102190942/http://www.fdic.gov/consumers/community/unbanked/index.html

97. https://www.youtube.com/watch?v=BrRXP1tp6Kw.

98. Chiffres calculés par la Banque Mondiale, cités par Wikipedia. Détail en ligne ici : http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1199807908806/4549025-1450455807487/Factbookpart1.pdf.

99. Emmanuel Kant, *Vers la paix perpétuelle*, 1795.

100. Plusieurs études de cabinets spécialisés convergent autour de ces chiffres : voir ces rapports sur : https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, https://www.ericsson.com/au/res/region_RASO/docs/2010/ericsson_50_billion_paper.pdf, https://www-ssl.intel.com/content/www/us/en/Internet-of-things/infographics/guide-to-iot.html ou ce résumé des prédictions contradictoires de *Structure Connect* : http://www.structureconnect.com/prediction-there-wont-be-50b-connected-iot-devices-by-2020/.

101. Éclairage intéressant sur la difficulté de faire adopter des objets connectés : http://tempsreel.nouvelobs.com/economie/20161209.OBS2448/les-objets-connectes-n-interessent-personne.html

102. Les messages de Satoshi dans l'ordre chronologique inversé :

103. https://bitcointalk.org/index.php?action=profile;u=3;sa=showPosts. https://bitcoin.org/en/alert/2016-11-01-alert-retirement La « clef d'alerte » ayant été trop dévoilée au fur et à mesure du développement de Bitcoin, il a été choisi de la supprimer. De plus, le réseau

Bitcoin est désormais épaulé par de nombreux relais médiatiques, il n'a plus semblé nécessaire de maintenir un affichage de message urgent dans le client.

104. Calcul du nombre de bitcoins possédés par Satoshi : https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/.

105. Papier de 2005 de Nick Szabo sur Bitgold : https://unenumerated.blogspot.fr/2005/12/bit-gold.html

106. Réponse de Satoshi : http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:52186.

107. L'équipe d'une quarantaine d'étudiants du *Aston University Centre for Forensic Linguistics* de l'Université de Birmingham était dirigée par le Professeur Jack Grieve. Elle confirmait au demeurant l'étude publiée par le bloggeur Skye Grey en décembre 2013, en ligne ici : https://likeinamirror.wordpress.com/2013/12/01/satoshi-nakamoto-is-probably-nick-szabo/.

108. http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate Estimation du prix du Bitcoin à partir de 2009.

109. Le message en question sur Bitcointalk : https://bitcointalk.org/index.php?topic=137.0.

110. Article de la BBC sur le sujet : http://www.bbc.com/news/uk-wales-south-east-wales-25134289.

111. Étude en langue anglais en ligne ici : https://letstalkbitcoin.com/blog/post/rise-of-the-zombie-bitcoins.

112. À la fin de l'année 2012, la banque britannique HSBC a été condamnée à payer un montant record de 1,9 milliard de dollars) pour mettre fin à des poursuites des autorités américaines dans une affaire de blanchiment. « Nous assumons la responsabilité de nos erreurs passées. Nous avons déjà dit que nous en sommes profondément désolés et nous le disons une nouvelle fois », déclarait alors Stuart Gulliver, directeur général de HSBC.

113. http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main Le *White Paper* intitulé « The Deep Web : Surfacing Hidden Value », publié en 2001, dresse un portrait de ce que pourrait être ce Web « profond ».

114. Cours relevés sur blockchain.info.

115. Volumes relevés sur blockchain.info.

116. Ross Ulbricht a continué d'entretenir la chronique judiciaire. De nouveaux éléments tendant à prouver, atténuer ou contester sa culpabilité sont régulièrement publiés. Il semble notamment que des connexions suspectes usant de l'identité de Dread Pirate Roberts aient eu lieu depuis l'incarcération d'Ulbricht.

117. Un exemple parmi d'autres, avec ce fâcheux raccourci du titreur du Figaro : http://www.lefigaro.fr/flash-actu/2015/08/21/97001-20150821FILWWW00037-l-ex-patron-francais-de-bitcoin-reste-en-prison.php.

118. La BCE donne de nombreux détails (en anglais) ici : http://www.ecb.europa.eu/stats/money/euro/circulation/html/index.en.html. et quant aux chiffres en valeur, là : http://sdw.ecb.europa.eu/reports.do?node=1000004112.

119. https://www.federalreserve.gov/paymentsystems/coin_currcircvalue.htm.

120. Concernant l'or des particuliers, on ne peut que risquer des estimations. Celle-ci provient du site http://www.orargent.com/OrArgentvaleur.asp. Il est probable qu'elle soit assez prudente.

121. Les statistiques touchant à l'or sont toujours assez opaques, même en ce qui concerne celui détenu par les Banques Centrales. Leurs réserves seraient selon l'inventaire du World Gold Council, de 32 702 tonnes au 1er janvier 2016. Un chiffre qui paraît plausible.

122. Il s'agit de l'application *Bitcoin Ticker*, selon le site américain spécialisé dans les technologies mobiles BGR. Ce n'est naturellement pas le seul exemple.

123. https://bitcoin.fr/hausse-du-cours12/.

124. C'est ce qu'avance Patrice Bernard sur son blog *C'est pas mon idée* le 10 décembre 2016 : http://cestpasmonidee.blogspot.fr/2016/12/bitcoin-dans-une-prevision-choc-de-saxo.html.

125. Sur ce qui suit, lire https://le-coin-coin.fr/3071-bitcoin-in-tempore-belli/.

126. En page 7 du rapport du 18 janvier 2016 « Changes in modus operandi of IS in terrorist attacks ». Le rapport en ligne sur le site d'Europol (voir note 34 plus haut) étant régulièrement complété ou réécrit en palimpseste, on trouvera sa version d'origine sur le site Bitcoin.fr à l'adresse https://bitcoin.fr/europol-bitcoin-ne-finance-pas-les-terroristes.

127. Site avec la liste la plus exhaustive conservant les monnaies « mortes » : http://cryptoguru.tk/.

128. Petit historique des premières cryptomonnaies : https://github.com/ppcoin/ppcoin/wiki/History-of-cryptocurrency.

129. Toutes les capitalisations et leurs historiques sont issus de https://coinmarketcap.com/.

130. Adresse de l'ICO d'Ethereum : https://blockchain.info/address/36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2.

131. Adresse de l'ICO de NXT : https://blockchain.info/address/1BCN1ugdKdWd9pQ8Am9hMhtHZfmbXzxE8a.

132. Q3 Blockchain State par Coindesk : http://www.coindesk.com/research/state-of-blockchain-q3-2016/.

133. On les trouvera sur des sites comme https://www.worldcoinindex.com.

134. Sur l'anonymat des cryptomonnaies, lire « Sur la fongibilité, Bitcoin, Monero et pourquoi zCash est une mauvaise idée » en ligne ici : https://steemit.com/bitcoin/@dnaleor/on-fungibility-bitcoin-monero-and-why-zcash-is-a-bad-idea.

135. Au total à la fin 2016, il y a eu 123 BIP (Bitcoin Improvement Proposals) dont une vingtaine a été définitivement acceptée. Et nul ne prétend que Satoshi Nakamoto ait été omniscient et infaillible. On a souligné qu'il avait notamment sous-estimé les chances d'un attaquant (sans grande conséquence d'ailleurs car elles décroissent bien exponentiellement vers zéro comme cela a été montré par Ricardo Perez-Marco et Cyril Grunspan).

136. Historique des forks Bitcoin : https://blog.blockchain.com/2016/02/26/a-brief-history-of-bitcoin-forks/.

137. Fork Ethereum vs Ethereum Classic : frise historique sur le site https://ethereumclassic.github.io/.

138. Voir note 18.

139. On peut lire notamment l'étude prépubliée en octobre 2016 par G. Bissias, B. N. Levine, A. P. Ozisik, et G. Andresen, *An Analysis of Attacks on Blockchain Consensus* : https://arxiv.org/pdf/1610.07985v2.pdf.

140. Lire en particulier l'étude *Eclipse Attacks on Bitcoin's Peer-to-Peer Network* de E. Heilman A. Kendler A. Zohar et S. Goldberg : https://eprint.iacr.org/2015/263.pdf.

141. Pour en savoir un peu plus sur les signatures de Schnorr https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496.

142. Il est possible de constater encore aujourd'hui cette modification sur le lien suivant, à la ligne 17 de main.sh : https://github.com/bitcoin/bitcoin/commit/8c9479c6bbbc38b897dc97de9d04e4d5a5a36730.

143. « "Argument from Authority" is a logical fallacy, so "Because Satoshi Said So" isn't a valid reason. However, staying true to the original vision of Bitcoin is very important. That vision is what inspires people to invest their time, energy, and wealth in this new, risky technology. » in https://bitcoinfoundation.org/a-scalability-roadmap/.

144. Voir ici la répartition des différents nœuds : https://coin.dance/nodes. Voir également les prises de positions ici : https://coin.dance/poli

145. *The Resolution of the Bitcoin experiment*, un véritable article hégelien : https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7.

146. Une étude en langue anglaise fait un point complet sur le « fees market » : https://dl.dropboxusercontent.com/u/43331625/feemarket.pdf

147. Le papier d'origine mise à jour en 2016 : https://lightning.network/lightning-network-paper.pdf.

148. Un bon résumé de cela est disponible sur Wikipedia : https://fr.wikipedia.org/wiki/Six_degrés_de_séparation, et pour approfondir ces questions de chemins au sein d'un réseau : https://www.franceculture.fr/emissions/la-conversation-scientifique/les-reseaux-quils-soient-sociaux-ou-non-sont-ils.

149. Papier décrivant le principe des sidechains : https://blockstream.com/sidechains.pdf.

150. Couverture correspondante : http://www.economist.com/printedition/covers/2015-10-29/ap-e-eu-la-me-na-uk. Les plus attentifs noteront en bas à droite que le canonique « *vires in numeris* » a été remplacé par « *in blockchain we trust* » absolument révélateur du glissement. Dans l'article premier du magazine : http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine il est intéressant de noter que blockchain apparaît 26 fois et Bitcoin seulement 13 fois.

151. Voir cet article du *International Business Times* : http://www.ibtimes.com/amazon-nearly-20-years-business-it-still-doesnt-make-money-investors-dont-seem-care-1513368.

152. Voir cet article de *The Atlantic* : https://www.theatlantic.com/business/archive/2009/09/facebook-turns-a-profit-users-hits-300-million/26721/.

153. Voir cet article de *CNNMoney* : http://money.cnn.com/2016/03/21/technology/twitter-10th-anniversary/.

154. Il y aurait une thèse à écrire sur le très efficace marketing mis en œuvre par les initiateurs de la start-up R3CEV autour d'un projet de « blockchain consortiale » qui après avoir été vanté comme l'esprit de la blockchain enfin objectivé dans le monde réel et sérieux, celui des banques, n'avait, en fin 2016, délivré qu'un projet de base de donnée distribuée dont les concepteurs durent avouer à mi-mot qu'il n'était pas stricto sensu une blockchain. À la fin de l'année, trois des premières banques à avoir rejoint le consortium en sortaient assez bruyamment.

155. Tous ces différents graphiques peuvent être consultés ici : https://blockchain.info/charts.

156. Voir notes 73 et 74.

157. Le Rapport de la BCE *Virtual currency schemes –a further analysis* (février 2015) est en ligne ici : https://fr.scribd.com/document/257441572/Virtual-Currency-Schemes-A-Further-Analysis?ad_group=Online+Tracking+Link&campaign=Skimbit%2C+Ltd.&content=10079&irgwc=1&keyword=ft500noi&medium=affiliate&source=impactradius.

158. Déclaration de David Andolfatto, vice-président de la Federal Reserve Bank de St. Louis.

159. Tout cela est disponible dans la note du secrétaire générale de la SEC, Robert W. Errett : https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf.

160. Voir note 70.

161. On trouvera le poids des mots et le choc des photos en ligne sur Bloomberg ici https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything.

162. « Il n'existe en réalité aucun pouvoir au monde capable d'assurer l'honnêteté d'une banque qui ne tient pas à rester honnête », comme le note Sir Terry Pratchett dans l'ouvrage fondamental déjà cité en note 76.

163. Lire ceci http://www.theaustralian.com.au/business/opinion/alan-kohler/asxs-blockchain-plans-may-have-been-hacked/news-story/5427ce8ebc8f44387bc1c966e86817bc et entre les lignes ici : https://www.ft.com/content/45851b58-62d1-11e6-8310-ecf0bddad227.

164. La fin de l'année 2016 a vu, avec de premiers signes de désenchantement devant les résultats concrets des entreprises fondées sur la « technologie blockchain » un sensible retournement d'opinion, chez les plus pragmatiques, envers un bitcoin qui ne cesse de survivre à ses fossoyeurs. En décembre les experts de la Saxo Banque incorporaient dans leurs dix prédictions choc pour 2017 un bitcoin propulsé à

2000 euros par l'aventurisme de la nouvelle administration américaine. Lire le document de Saxo Banque ici : http://fr.saxobank.com/Documents/Prévisions %20choc %202017%20FR.pdf.

165. Source déjà citée en note 85.

166. Stéphane Laborde, *Théorie Relative de la Monnaie 2.718*, 2016 : http://trm.creationmonetaire.info/.

167. Article détaillant les problèmes de transmissions de données terre-mars : http://www.astrosurf.com/luxorion/mars-communication3.htm.

168. Voir notes 73 et 74.

169. Site reprenant les prédictions de personnalité du milieu en 2014 : https://foundersgrid.com/bitcoin-price/, site prenant des prédictions volontaires : https://www.hedgeable.com/research/bitcoin/estimator.

170. Sans compter que la monnaie classique, régalienne si l'on puit dire par sa gravure, a été vue par une tradition longue et bien établie, comme de nature commune autant que publique. Citons ici Oresme, au chapitre V du Traité des Monnaies : « La monnaie, l'impression du coin, doit être faite par une personne publique ou par plusieurs, désignées pour cela par la communauté, parce que, comme on l'a déjà dit, la monnaie est, par nature, instituée et inventée pour le bien de la communauté. Et en son chapitre VI : L'argent appartient donc à la communauté et à chacune des personnes qui la composent. »

171. Salvador Dalí, *Journal d'un génie*, Paris, Gallimard, 1994.

172. Conférence donnée à Zurich en mars 2016. Texte dans *The Internet of Money*, page 55 et vidéo sur www.youtube.com/watch?v=5ca70mCCf2M.

173. Jean-Joseph Goux, *Les monnayeurs du langage*, Paris, Galilée, 1984.

174. On a parfois l'impression que certains orateurs (même nés avant le 15 août 1971) n'ont ou ne veulent avoir aucune idée de ce qui existait auparavant : « Nous nous basons trop sur l'histoire récente (en particulier lorsque nous nous exclamons: «on n'a jamais vu ça!») et pas assez sur l'histoire dans sa globalité. En d'autres termes, l'histoire nous enseigne que ce qui ne s'est jamais produit finit par arriver. Elle nous apprend beaucoup de choses en dehors des séquences temporelles étroites : plus notre vision est élargie, plus ces leçons s'avèrent enrichissantes. Bref, l'histoire nous prévient contre l'empirisme naïf qui consiste à apprendre des faits superficiels », Nassim Taleb, *op. cit.*, p.133.

175. Jean-Joseph Goux, *Le trésor perdu de la finance folle*, Paris, Blusson, 2013, page 127. Goux parle d'un « moment inouï, dont on mesure encore mal les conséquences et la signification historique. » dans *Dette*, (*op. cit.* page 441). Graeber parle aussi d'une « phase nouvelle de l'histoire financière, une phase que personne ne comprend tout à fait. »

176. En particulier pour nous avoir communiqué avant publication le support de sa présentation du 12 janvier 2017 au Séminaire de Cryptofinance de Paris, « The Mathematics Behind Bitcoin Double Spend Race… » et avoir patiemment répondu à nos questions.

Remerciements

Les bitcoineurs sont des êtres humains finalement assez normaux. Leur gratitude va tout naturellement d'abord vers leurs familles respectives même si celles-ci ont parfois du mal avec un sujet jugé pointu ; et vers leurs amis et leurs proches.

Les auteurs tiennent à exprimer leur reconnaissance à CNRS Editions qui a accepté dès 2015 le projet d'un sujet franchement axé sur le bitcoin comme monnaie, alors que le mot bitcoin était pudiquement évacué du débat durant de longs mois, et à Grégoire Kauffmann pour son accompagnement dans le travail de publication.

Ils veulent aussi exprimer leur profonde gratitude à Jean-Joseph Goux, non seulement pour leur avoir fait l'honneur de préfacer ce livre, mais aussi pour la simplicité et la cordialité qui a présidé à la longue rencontre qui a permis de lui présenter le projet et de situer Bitcoin par rapport aux thèmes qu'il avait déjà abordés par ailleurs en matière de monnaie.

Ils remercient également tous ceux qui ont fourni des ressources documentaires, partagé des réflexions ou prodigué des conseils : le site Bitcoin.fr a été d'une aide précieuse, les sites Bitconseil ou e-ducat sont d'une grande richesse ; les amis et membres du « Cercle du Coin » et notamment Adrian Sauzade, Charles Couillard, Jean-Yves Rossi, Michel Foucault et Pierre Noizat se sont montrés toujours disponibles pour donner un renseignement ou développer un point un peu technique, sans même connaître la finalité des questions. Enfin de savants mathématiciens, cryptologues ou informaticiens doivent être ici salués, notamment Jean-Jacques Quisquater, Jean-Paul Delahaye, Ricardo Perez-Marco, avec des remerciements particuliers à Cyril Grunspan [176].

Retrouvez tous les ouvrages de CNRS Éditions
sur notre site
www.cnrseditions.fr

Table des Matières

Présentation de l’éditeur 2
Titre 3
Copyright 4
Sommaire 5
Préface de Jean-Joseph Goux 6
Introduction 9
I. Sidérant bitcoin 14
1- Une solution inédite pour un désir ancien 14
2- Un agencement génial, instrument de véritables exploits 22
3- Une création révolutionnaire cause d’enthousiasme ou de scandale 30
II. Le bitcoin, sans mystère ni fantasme 40
1- Esquisse de son ingénieux assemblage 40
2- Croquis des caractéristiques tant numériques que monétaires du bitcoin 51
3- Ébauche des usages hétéroclites du bitcoin 61
III. Histoire passée et présente d’une monnaie jeune, féconde et universelle 74
1- Une enfance difficile, une adolescence turbulente : le bitcoin dans la zone à risque 74
2- Bitcoin père de toutes les cryptomonnaies 84
3- L’entrée dans la vie active 96
Conclusion 107
Notes 111
Remerciements 119
Retrouvez tous les ouvrages de CNRS Éditions 120