GLOSSAIRE

Blockchain

Matthieu **QUINIOU**

Christophe **DEBONNEUIL**



Organisation des Nations Unies pour l'éducation, la science et la culture

Chaire UNESCO ITEN Innovation, Transmission, Edition Numériques

uniTwin

FMSH fondation maison des sciences de l'homme

UNIVERSITÉ PARIS 8 VINCENNES - SAINT-DENIS

Agence Nationale de la Recherche
ANR

UNIVERSITÉ PARIS 8
VINCENNES - SAINT-DENIS

fmsh fondation maison des sciences de l'homme

CréaTIC
INITIATIVE D'EXCELLENCE EN FORMATIONS INNOVANTES

INVESTISSEMENTS D'AVENIR



LES ÉDITIONS DE L'IMMATÉRIEL

G L O S S A I R E

Blockchain

Matthieu **QUINIOU**

Christophe **DEBONNEUIL**

Chaire UNESCO ITEN Innovation, Transmission, Edition Numériques

Organisation des Nations Unies pour l'éducation, la science et la culture

Auteurs :
Matthieu QUINIOU
Christophe DEBONNEUIL

Concept graphique couverture :
Aurélia MAZOYER, UNESCO

Couverture et Mise en page intérieure :
John MOTTA

ISBN : 979-10-91636-18-6

Publié avril 2019
© Chaire UNESCO ITEN, 2019

Publié par :

LES ÉDITIONS DE L'IMMATÉRIEL
17, rue de Lancry 75010 Paris (France)

CréaTIC INITIATIVE D'EXCELLENCE EN FORMATIONS INNOVANTES

Le projet CréaTIC / ANR-11-IDFI-0011 au titre du programme Investissements d'avenir.

Sommaire

Présentation 6

Algorithme de consensus 8

Attaque à 51% 9

Auto-gestion de l'identité *(Self-Sovereign Identity)* 10

Bitcoin 11

Blockchain 12

Blockchain privée *(Private Blockchain)* 13

Blockchain publique *(Public Blockchain)* 14

Chaîne latérale *(Side chain)* 15

Clé 16

Contrat intelligent *(Smart Contract)* 17

Crypto-actif 18

Cryptographie 19

Cryptographie asymétrique 20

Cypherpunk 21

Decentralized Autonomous Organisation *(DAO)* 22

Decentralized Application *(dApp)* 23

Décentralisation 24

Désintermédiation 25

Embranchement *(Fork)* 26

Empreinte d'un fichier *(Hash)* 27
Ethereum 28
Gouvernance 29
Horodatage *(Time-stamping)* 30
Hyperledger 31
Immutabilité 32
Chronologie 33
Initial Coin Offering *(ICO)* 34
Internet de la valeur 35
Interopérabilité 36
Jeton *(Token)* 37
Jeton non-fongible 38
Minage 39
Mise à l'échelle *(Scalability)* 40
Noeud 41
Open Source 42
Oracle 43
Portefeuille *(Wallet)* 44
Preuve à divulgation nulle de connaissance 45
Preuve d'autorité *(Proof of Authority)* 46
Preuve d'enjeu *(Proof of Stake)* 47
Preuve de travail *(Proof of Work)* 48
Problème de la double dépense 49
Pseudonymat 50
Registre distribué 51
Réseau pair-à-pair 52
Signature numérique 53
Tokenisation 54
Tolérance aux fautes byzantines 55
Traçabilité 56
Transaction 57
Transparence 58



Matthieu QUINIOU

Avocat en droit du numérique, docteur en droit privé, titulaire de la certification de l'AMF, chercheur à la Chaire UNESCO ITEN (UP8/FMSH) et membre de la Commission de Normalisation Blockchain à l'AFNOR.



Christophe DEBONNEUIL

Diplômé HEC, ingénieur de l'Ecole Centrale de Lyon, Diplômé Said Business school sur la blockchain, université d'Oxford. Intervenant à l'OCDE sur des programmes de formation aux technologies blockchain.



John MOTTA

Directeur Artistique, chercheur à la Chaire UNESCO ITEN (UP8/FMSH), travaille sur les questions de représentation graphique des notions. Enseignant dans le master CEN/UP8.

Présentation

Innovation technologique formalisée dans les années 2000, la blockchain est devenue au fil des ans un outil incontournable. Simple feuille de calcul magnifiée pour certains, forme ultime de démocratie pour d'autres, la réalité se situe probablement entre les deux.

Les technologies blockchain sont encore jeunes mais d'ores et déjà, les usages imaginés fourmillent dans tous les domaines en particulier dans l'éducation et la science. De plus, le moment est parfait : après une longue période d'essais, l'année 2019 s'annonce comme étant l'année de mise en production pour beaucoup de projets.

La journée Blockchain organisée par l'UNESCO et la chaire UNESCO ITEN fait un point d'étape sur les technologies blockchain, à la fois sur leurs définitions et leurs cas d'usage. Le glossaire que vous tenez entre les mains vise à servir d'outil pour appréhender cette journée.

L'équipe a sélectionné cinquante mots qui façonnent l'écosystème, et qui, nous l'espérons, permettront d'engager la discussion entre les acteurs si divers concernés par la révolution blockchain. Nous espérons aussi qu'il pourra être une source d'inspiration pour ceux qui s'attellent au quotidien à construire un monde meilleur.

Matthieu QUINIOU
Christophe DEBONNEUIL

Algorithme de consensus

Un algorithme de consensus définit les règles qui permettent de mettre à jour la blockchain. Grâce à l'algorithme de consensus, il existe à tout moment un état « officiel » du registre dont chaque noeud a une copie.

L'algorithme de consensus est un élément fondamental de la gouvernance de la blockchain. L'algorithme de consensus le plus connu actuellement est la preuve de travail. C'est en particulier l'algorithme de consensus de la blockchain Bitcoin.

Voir : Gouvernance, Preuve de travail

Attaque à 51%

L’attaque à 51% désigne une attaque d’une blockchain (fonctionnant avec des mineurs) conduite par un ensemble de noeuds du réseau qui contrôle plus de la moitié de la puissance de calcul du réseau. Elle résulte dans la possibilité pour cet ensemble de noeuds de choisir les transactions inscrites dans la blockchain et de rendre possible une double dépense. C’est une attaque classiquement redoutée car susceptible de rendre inutilisable la blockchain. Ce terme est souvent utilisé en référence à la blockchain Bitcoin.

Voir : Bitcoin, Minage

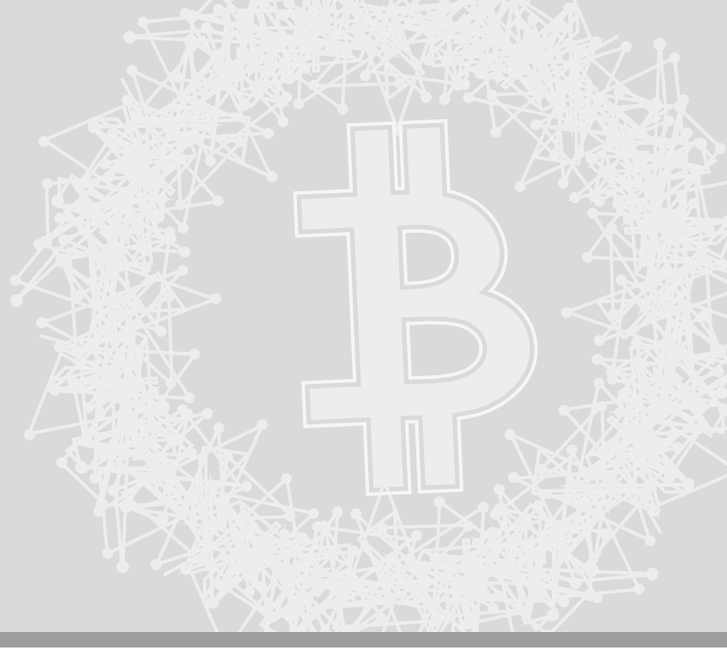
Auto-gestion de l’identité

(Self-Sovereign Identity)



La notion d’auto-gestion de l’identité fait référence aux méthodes de gestion de l’identité par l’individu lui-même, s’appuyant sur le cryptage, la décentralisation et la modularité du partage des données. Les systèmes d’auto-gestion de l’identité numérique sont particulièrement utiles pour la gestion de l’accès aux données sensibles.

Voir : Cryptographie, Décentralisation



Bitcoin

Le Bitcoin (avec une majuscule) désigne la première blockchain dont la description a été publiée en 2008 sous le nom « Bitcoin : un système de monnaie électronique en pair-à-pair » par un auteur inconnu.

Le bitcoin (avec une minuscule) désigne l'actif numérique transféré sur la blockchain Bitcoin. Le nombre total de bitcoins a été fixé arbitrairement par son créateur à 21 millions. Ceux-ci sont émis actuellement à un rythme de 12,5 bitcoins toutes les 10 minutes environ et servent à récompenser le mineur ayant constitué le bloc le plus récent. L'algorithme de consensus du réseau Bitcoin est la preuve de travail.

Voir : Algorithme de consensus



Blockchain

Une blockchain est un registre distribué basé sur une structure de données appelée chaîne de blocs. Les transactions sont stockées dans des blocs qui sont chaînés les uns aux autres d'où le nom de blockchain. Un bloc contient, en plus de transactions, l'empreinte digitale du bloc précédent. La modification d'une transaction modifie donc non seulement le bloc auquel il appartient mais l'ensemble des blocs qui le suivent.

La structure en chaîne de blocs confère au registre distribué son immutabilité. Souvent, par abus de langage, on désigne par blockchain tout type de registre distribué et non seulement ceux qui sont basés sur une chaîne de blocs.

Voir : Empreinte numérique, Immutabilité, Registre distribué



Blockchain privée

(Private Blockchain)

Une blockchain privée est une blockchain qui nécessite une cooptation pour un nouvel acteur souhaitant participer à la création d'un nœud, à la validation des blocs et au système de consensus. Le potentiel de décentralisation des blockchains privées est par nature inférieur à celui des blockchains publiques.

Hyperledger Fabric est un exemple d'environnement de travail qui permet la mise en place de blockchain privés. Plusieurs groupes de la grande distribution ou du secteur bancaire ont déjà créé leur blockchain privée.

Voir : Blockchain, Blockchain publique



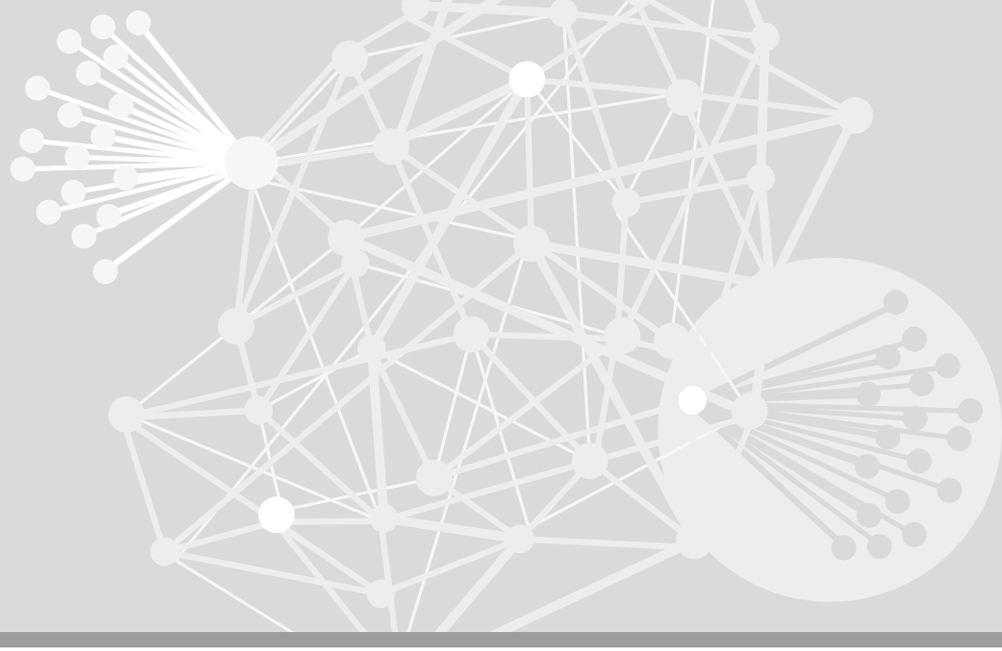
Blockchain publique

(Public Blockchain)

Une blockchain publique est une blockchain que tout utilisateur peut rejoindre sans condition. En particulier, sur une blockchain comprenant des mineurs, n'importe quel utilisateur peut devenir mineur. Bitcoin et Ethereum sont des blockchains publiques.

Les blockchains publiques disposent généralement d'un niveau de décentralisation plus élevé que les blockchains privées.

Voir : Blockchain, Blockchain privée



Chaîne latérale

(Side chain)

Une chaîne latérale est un système d'extension et de désengorgement d'une blockchain principale qui permet ainsi potentiellement d'augmenter le nombre de transactions et de faciliter la mise à l'échelle.

Par exemple, le Lightning Network est une solution développée par le réseau Bitcoin pour accélérer le débit de ses transactions.

Voir : Mise à l'échelle

Clé

Une clé est un terme issu de la cryptographie. C'est une chaîne de caractères qui permet de signer, chiffrer ou déchiffrer un message. On distingue en cryptographie les clés privées qui doivent être gardées secrètes, des clés publiques qui peuvent être divulguées à tous. Techniquement, la clé publique dérive par un calcul irréversible de la clé privée.

Par exemple, la clé privée d'un utilisateur lui permet de transmettre un actif qui lui appartient à un autre noeud de la blockchain. Jusqu'à présent, quand des bitcoins ont été volés à leur détenteur, cela a été dû à un vol de clé privée et non à une défaillance de la blockchain Bitcoin.

Voir : Bitcoin, Cryptographie, Cryptographie asymétrique

Contrat intelligent

(Smart contract)



Un contrat intelligent est un ensemble de fonctions définies par une séquence d'instructions inscrite sur une blockchain. Cette notion attribuée à Nick Szabo trouve ses origines dans le mouvement des cypherpunks et vise à faire la synthèse entre l'informatique et le droit des contrats notamment grâce à des dispositifs cryptographiques.

Les contrats intelligents fonctionnels ont été popularisés par l'écosystème Ethereum avec l'émergence de l'Ethereum Virtual Machine (EVM) et l'utilisation du langage informatique Solidity. Les contrats intelligents permettent notamment de créer des tokens, de réaliser des ICO, des DAO ou encore de créer des dApp.

Voir : DAO, Ethereum, dApp, Initial Coin Offering, Jeton, Cypherpunk

Crypto-actif



Le terme crypto-actif désigne de manière neutre et générique à la fois les crypto-monnaies et les tokens. Les crypto-actifs sont des actifs numériques ou monnaies virtuelles dont la particularité est de fonctionner avec une blockchain. Le bitcoin ou l'ether sont par exemple des crypto-actifs.

Les transactions réalisées avec des crypto-actifs peuvent l'être avec plus ou moins d'opacité selon les caractéristiques de la blockchain dont ils dépendent.

Voir : Jeton, Bitcoin, Ethereum



Cryptographie

La cryptographie permet à deux personnes d'échanger des messages sans que ceux-ci puissent être interceptés par des tiers. Elle consiste à déterminer un algorithme pour crypter les messages et un autre pour les décrypter.

La cryptographie est une discipline clé pour comprendre le développement des blockchains.

Voir : Cryptographie asymétrique

Cryptographie asymétrique

La cryptographie asymétrique est la branche de la cryptographie la plus utilisée dans le monde des blockchains. Elle s'appuie sur deux clés que possède chaque participant : une clé privée gardée secrète par son propriétaire et une clé publique qui peut être distribuée à tous.

Par exemple, si A veut envoyer un message lisible uniquement par B, alors A chiffre son message avec la clé publique de B. Ce message ne pourra être déchiffré que via la clé privée de B dont B est le seul possesseur. A noter qu'une clé privée permet aussi de signer un message.

Voir : Clé, Cryptographie

Cypherpunk

Cypherpunk désigne un courant de pensée crypto-anarchiste et les personnes qui y sont affiliées. Ce courant de pensée s'est développé depuis les années 90 avec l'informatisation.

L'idéologie cypherpunk repose sur des valeurs comme l'anonymat, l'interaction directe désintermédiée ou encore l'open source.

L'approche décentralisée et pair-à-pair de la blockchain en font un outil technologique structurellement adapté aux valeurs et objectifs sociétaux cypherpunks.

Voir : Décentralisation, Open Source, Réseau pair-à-pair



Decentralized Autonomous Organisation *(DAO)*

Le terme DAO désigne un système d'organisation autonome et décentralisé dont les règles de fonctionnement et de participation sont prévues par un smart contract inscrit dans une blockchain.

Il convient de noter que le projet Ethereum, au coeur du développement, désigne actuellement par DAO non plus des Decentralized Autonomous Organizations mais des Democratic Autonomous Organizations.

Le terme DAO a également été utilisé par le projet « The DAO » qui avait pour ambition de voter pour le financement de projets blockchain mais ce projet a été piraté.

Voir : Contrat intelligent, Ethereum



Decentralized Application

(dApp)

Une Decentralized Application (dApp) est un programme avec plusieurs smart contracts fonctionnant sur une blockchain et généralement une interface utilisateur.

Parmi les dApps qui ont le plus fait parler d'elles, on peut citer La'Zooz - un Uber décentralisé, OpenBazaar - une place de marché, Lighthouse - une plateforme de financement participatif.

Voir : Décentralisation, Contrat intelligent



Décentralisation

Le terme décentralisation appliqué à l'architecture de la blockchain s'inscrit en opposition avec les architectures fonctionnant avec un seul serveur ou un seul administrateur. La décentralisation est une caractéristique importante de la blockchain pour limiter l'altération unilatérale de la base de données et justifiant le recours à des algorithmes de consensus.

La décentralisation réelle des blockchains est discutée, notamment pour les blockchains privées fonctionnant avec un nombre limité d'acteurs ou en raison de l'utilisation généralisée de services de clouds administrés.

Voir : Blockchain privée, Gouvernance

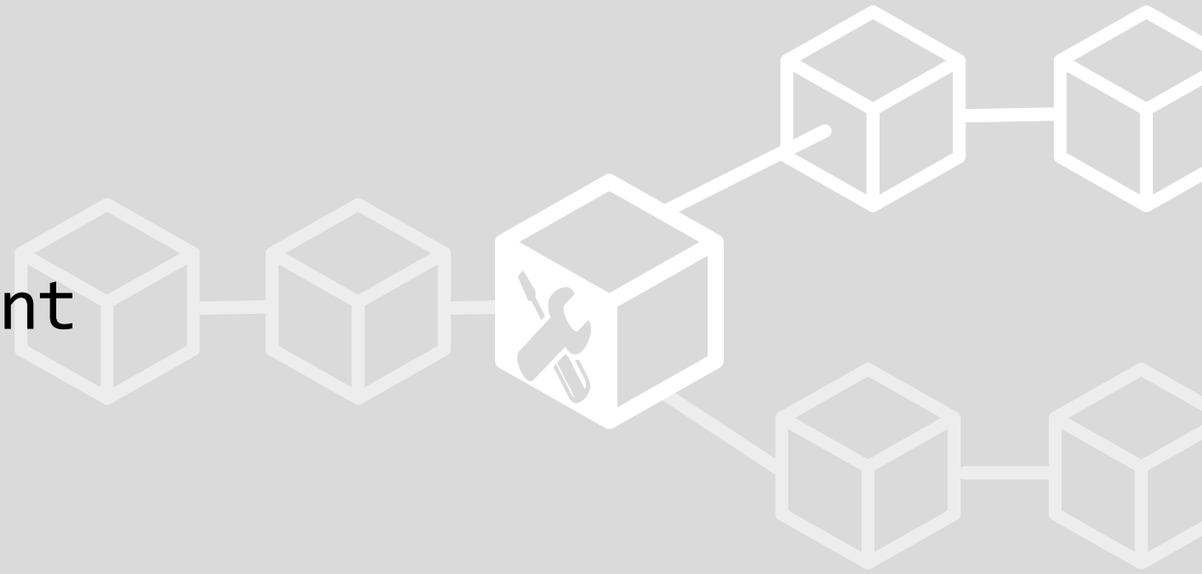


Désintermédiation

La désintermédiation désigne le fait de proposer des dispositifs permettant d'éviter le recours aux intermédiaires existants et donc de réduire les coûts de mise en relation et d'opérations. Pour autant la désintermédiation ne signifie pas nécessairement absence de médiation, celle-ci pouvant être automatisée.

La blockchain permet d'enclencher des processus de désintermédiation grâce à la création d'écosystèmes pair-à-pair fonctionnant sur des plateformes autonomes, décentralisées et open source.

Voir : Open source, Réseau pair-à-pair



Embranchement

(Fork)

Un fork ou selon une transcription française un embranchement désigne la modification réalisée par consensus des règles régissant la blockchain pouvant lorsque les modifications sont importantes et non rétro-compatibles donner lieu à un hard fork, c'est-à-dire, à la séparation de la blockchain en deux, ainsi qu'à la création d'un nouveau crypto-actif.

Les embranchements ont pour objectif principal de corriger des bugs, de limiter les effets d'un piratage rétroactivement, d'améliorer la blockchain ou encore de modifier les règles de fonctionnement.

Voir : Algorithme de consensus, Crypto-actif

Empreinte d’un fichier

(Hash)



Le hash d’un fichier est une empreinte numérique de ce fichier. Techniquement, il s’agit d’une chaîne de caractères de longueur fixe calculée à partir du fichier par l’action d’une fonction appelée « fonction de hashage ». Cette empreinte a la propriété d’être caractéristique du fichier, tout en ne permettant pas (en tout cas pratiquement) d’inférer le fichier à partir de son empreinte.

La plupart du temps, pour des raisons à la fois d’espace mémoire et de confidentialité, seules les empreintes des données sont stockées dans la blockchain et non les données elle-mêmes.

Voir : Blockchain, Bitcoin



Ethereum

Ethereum est une blockchain programmable décrite dès décembre 2013 par son créateur Vitalik Buterin. C'est la première blockchain pleinement programmable (au sens de Turing). Elle a permis l'émergence d'applications décentralisées nommées dApps. Les noeuds du réseau forment alors un «ordinateur global» appelé Ethereum Virtual Machine (EVM).

L'algorithme de consensus actuellement utilisé est la preuve de travail, même si le projet de passer en preuve d'enjeu, malgré ses nombreux reports, est toujours d'actualité.

Voir : Algorithme de consensus, Contrat intelligent, dApp, Minage



Gouvernance

La gouvernance correspond aux méthodes de décision et de mise en œuvre des choix organisationnels. Par principe dans les blockchains, la prise de décision est, comme l'architecture du réseau, décentralisée. L'administration de la blockchain est répartie entre les nœuds du réseau et les règles de prise de décisions bien que différentes d'une blockchain à l'autre reposent sur des mesures d'incitation au maintien de l'intégrité des données et à l'amélioration des composantes techniques et des méthodes de cryptage. L'algorithme de consensus est une composante essentielle de la gouvernance d'une blockchain.

Voir : Algorithme de consensus, Décentralisation, Noeud

Horodatage

(Time-stamping)



La blockchain permet d'horodater les données qui y sont inscrites. La présence d'un horodatage pour une transaction permet de certifier l'antériorité d'une information sur une autre et donc d'ordonner des transactions dans un environnement décentralisé.

Voir : Transaction



Hyperledger

Hyperledger est une plateforme open source de développement de blockchains. Ce projet a été initié en décembre 2015 par la fondation Linux. Elle propose plusieurs environnements de développement. Le plus connu, dont IBM est contributeur, est Hyperledger Fabric qui permet la mise en place de blockchains privées à destination des entreprises.

Voir : Blockchain privée



Immutabilité

L'immutabilité de l'information stockée sur une blockchain est un des principaux atouts de la blockchain : l'information une fois stockée ne peut plus être modifiée. L'immutabilité est garantie d'abord par le caractère distribuée de la blockchain : modifier le registre demanderait de modifier le registre de l'ensemble des noeuds. Ensuite, pour les blockchains, la structure de blocs renforce encore l'immutabilité en invalidant la blockchain dans son ensemble dès qu'une simple transaction est modifiée.

En revanche, si l'immutabilité de l'information est garantie pour la blockchain, sa véracité doit elle être vérifiée avec soin grâce à la présence d'oracles.

Voir : Blockchain, Oracle

Chronologie blockchain



1979 — Invention des arbres de hachage par Ralph Merkle



1988 — Rédaction d'un Manifeste crypto-anarchiste par Timothy C. May



1993 — Elaboration du concept de contrats intelligents par Nick Szabo



1998 — Projet de système de monnaie anonyme B-money par Wei Dai



2003 — Projet scientifique Timesec pour l'horodatage numérique



2008 — Article fondateur de Bitcoin par Satoshi Nakamoto



2009 — Création du premier bloc Bitcoin (genesis bloc)



2011 — Création du site illégal Silk Road



2013 — Première Initial Coin Offering réalisée par le projet Mastercoin



2014 — Piratage de la plateforme d'échange MtGox



2015 — Création de la blockchain Ethereum



2016 — Piratage du projet « The Dao »



2017 — Implémentation par le Venezuela de la crypto-devise Petro



2018 — Levée de fonds de 1,7 milliard $ lors de l'ICO de Telegram



2019 — Création de visas pour labelliser les ICO par l'AMF

Initial Coin Offering *(ICO)*



Une Initial Coin Offering (ICO) désigne l'émission de crypto-actifs pour une acquisition par le grand public ou des investisseurs agréés en contrepartie de devises, ou plus généralement d'autres crypto-monnaies. Les contrats intelligents permettent d'automatiser la réalisation des ICO en procédant à cette opération sur une blockchain préexistante.

Le niveau d'encadrement réglementaire des Initial Coin Offering dépend en grande partie des caractéristiques des tokens émis et de leur qualification ou non en produits financiers (securities). Les ICO portant sur des securities sont souvent qualifiées de Security Token Offering (STO).

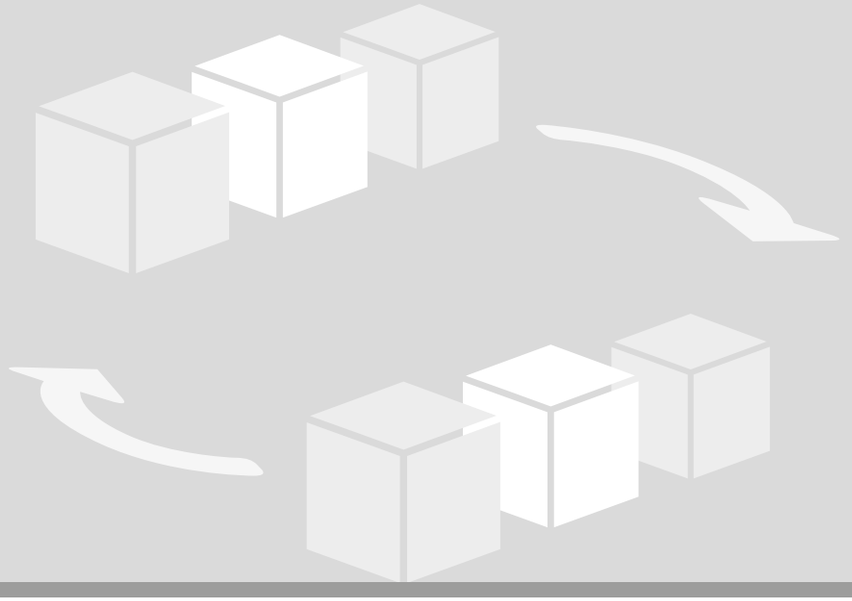
Voir : Contrat intelligent, Crypto-actif



Internet de la valeur

Expression souvent employée pour désigner l'apport de la blockchain par rapport à un Internet de l'information (l'Internet). L'internet de l'information permet de transmettre de l'information, en la copiant : celui qui envoie l'information en garde une copie. En revanche la blockchain permet l'émergence d'un internet de la valeur, au sens où un actif numérique transmis à un destinataire n'est plus en possession de l'expéditeur grâce à la résolution du problème de la double dépense. L'internet de la valeur, permis par la blockchain, innove en donnant la possibilité de tracer la possession d'un actif numérique ou même sous certaines conditions physique.

Voir : Blockchain, Problème de la double dépense



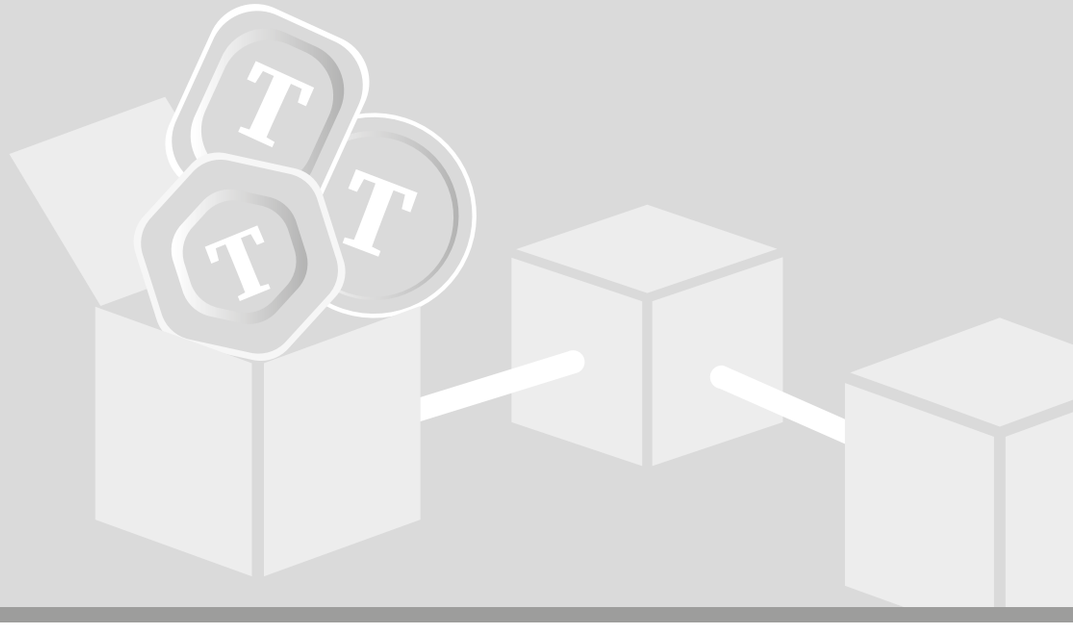
Interopérabilité

L'interopérabilité inter-blockchain désigne la possibilité de faire fonctionner ensemble deux ou plusieurs blockchains. L'interopérabilité est un enjeu important de la normalisation et certains projets blockchain sont axés sur la possibilité de créer de l'interopérabilité, les termes cross-chain et atomic swap sont également employés pour désigner cette interopérabilité.

Voir : Blockchain

Jeton

(Token)



Un jeton ou token désigne un crypto-actif qui s'échange de pair-à-pair au sein d'une blockchain préexistante à laquelle le contrat du token est adossé. Un jeton n'est pas la monnaie virtuelle native de la blockchain de laquelle il est issu. Par exemple, ether est l'unité de valeur native d'Ethereum et de nombreux projets ont créé des jetons sur Ethereum grâce à des contrats intelligents.

Il existe plusieurs catégories de jetons, la principale distinction étant généralement faite entre les jetons d'usage (utility tokens) et les jetons à droit de vote (security tokens).

Voir : Crypto-actif, Ethereum

Jeton non-fongible





Un jeton non-fongible se définit par son caractère non-interchangeable, son caractère unique. A la différence des crypto-monnaies qui par nature sont fongibles, des tokens non-fongibles sont uniques et spécifiquement identifiables.

Les tokens non-fongibles ont été popularisés par la dApp Crypto Kitties avec des tokens correspondant à des figurines virtuelles uniques de chats.

Voir : Crypto-actif, Decentralized Application, Jeton



Minage

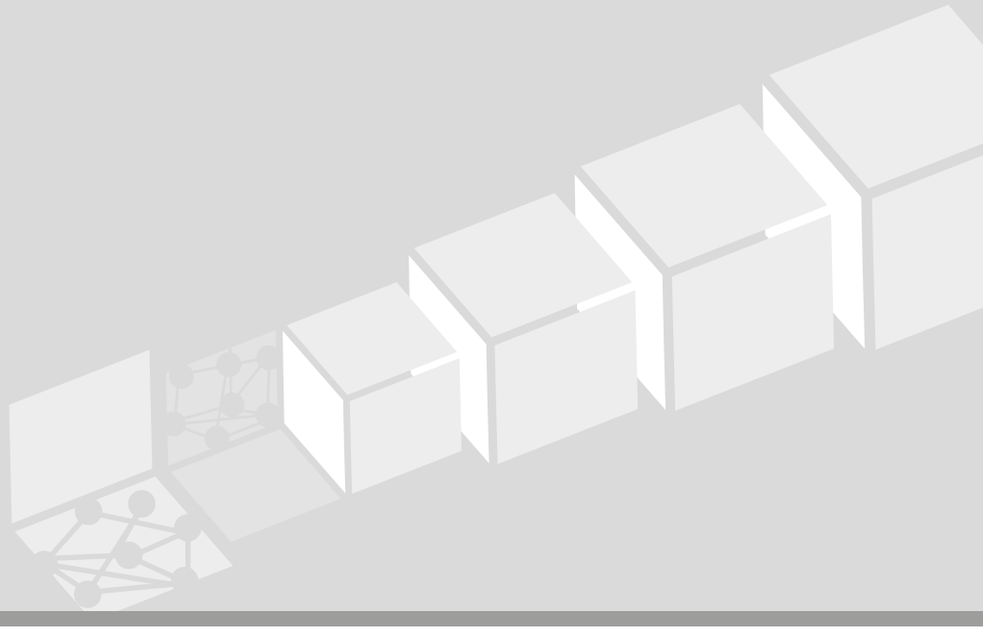
Utilisation de la puissance de calcul informatique afin de résoudre un problème cryptographique simple dans son principe mais demandant une puissance de calcul importante. Un mineur est un particulier ou une société qui connecte sur le réseau une ou plusieurs machines équipées pour effectuer du minage. Un mineur est rémunéré en jetons lorsqu'il est le premier à trouver la solution du problème cryptographique posé par le minage.

On parle de minage pour une blockchain fonctionnant en preuve de travail. Bitcoin en est l'exemple le plus connu.

Voir : Bitcoin, Preuve de travail

Mise à l'échelle

(Scalability)



La scalability ou mise à l'échelle, dans le domaine de la blockchain, désigne la possibilité de faire fonctionner un réseau avec une masse critique d'utilisateurs. La difficulté de la mise à l'échelle dans la blockchain tient en grande partie à l'énergie et la puissance de calcul nécessaires pour valider de manière sécurisée un grand nombre de transactions et de faire fonctionner rapidement un système de consensus fiable, comme celui de preuve de travail.

Voir : Algorithme de consensus, Preuve de travail

Noeud



Une blockchain est déployée sur un ensemble d'ordinateurs. Chaque ordinateur constitue un noeud du réseau.

On distingue habituellement les « noeuds complets » qui contiennent une copie complète de la blockchain et les « noeuds légers » qui hébergent une version minimale de la blockchain leur permettant de participer aux échanges sur le réseau.

Voir : Algorithme de consensus, Registre distribué

Open source

Le terme open source désigne à l'origine un code source partagé avec le public du fait de la volonté de son ou ses auteurs. L'open source correspond à une renonciation définitive aux droits de propriété intellectuelle susceptibles d'être revendiqués sur une œuvre de l'esprit. De nombreux codes sources mêlent open source et code propriétaire.

Si des pans entiers de code source sont open source dans la technologie blockchain, notamment les fondamentaux de la technologie de la blockchain Bitcoin, certains codes source, particulièrement dans les blockchains privées sont propriétaires et de nombreux brevets ont été déposés.

Voir : Décentralisation

Oracle

Un oracle est une source d'information à laquelle il est possible de faire confiance. Un oracle est crucial car, même si ce qui est écrit dans la blockchain l'est à jamais, la qualité de l'information qui y est inscrite n'est pas garantie. Seul un oracle assure que l'information inscrite dans la blockchain est exacte permettant à un « registre incorruptible » de devenir « une source d'informations fiable ».

Le terme oracle désigne les dispositifs permettant d'intégrer dans la blockchain des données extérieures certifiées. Les oracles fonctionnent souvent avec des objets connectés dotés de capteurs.

Voir : Contrat intelligent



Portefeuille

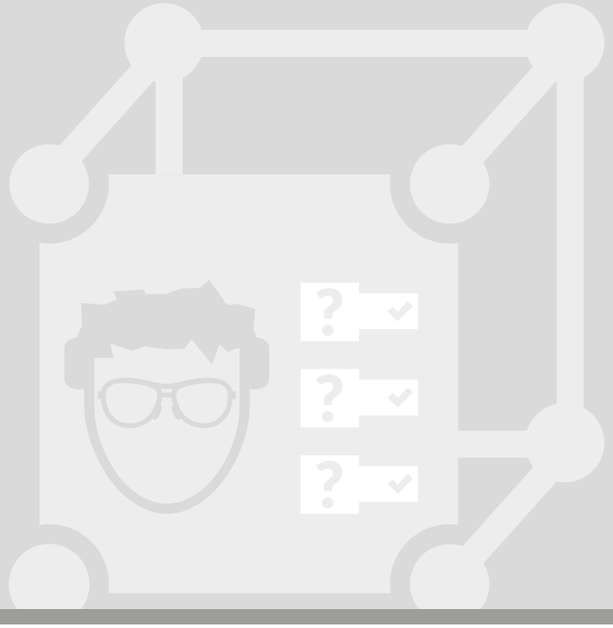
(Wallet)

Un portefeuille blockchain est un système permettant de gérer des clés liées à une blockchain, d'y envoyer et d'y recevoir des crypto-actifs. Certains portefeuilles blockchain fonctionnent également comme un moyen d'accès à un écosystème blockchain et représentent une interface compatible avec une blockchain.

Les portefeuilles blockchains prennent des formes variées : papier avec un QR code, extension de navigateur ou encore matériel hardware.

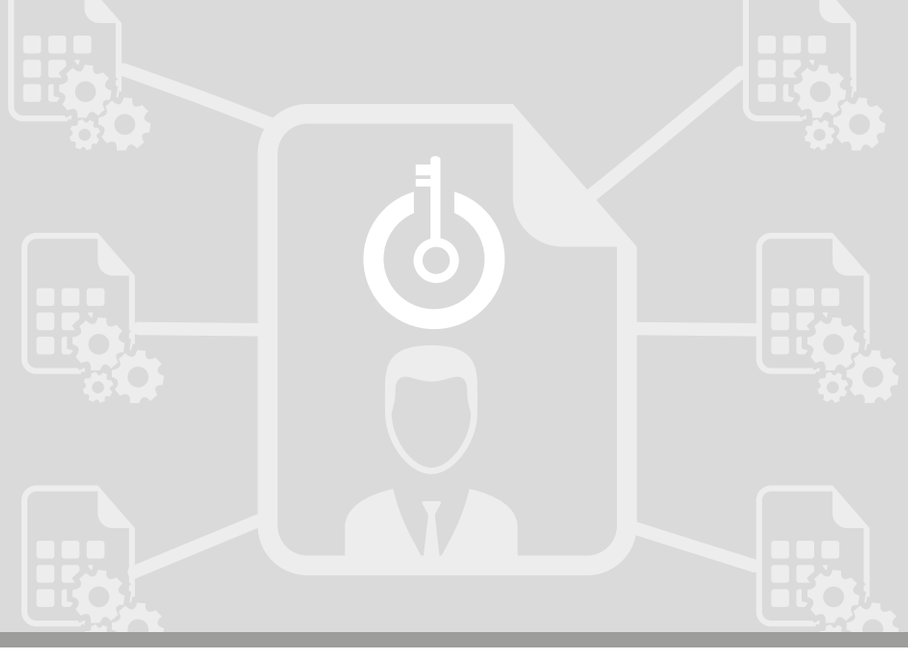
Voir : Crypto-actif

Preuve à divulgation nulle de connaissance



La preuve à divulgation nulle de connaissance consiste pour un noeud du réseau blockchain à prouver qu'il détient une information sans divulguer cette information. Par exemple, donner la preuve qu'une personne est majeure sans donner son âge est une preuve à divulgation nulle. La preuve à divulgation nulle est très utilisée car l'information selon laquelle un noeud possède l'information est souvent suffisante, sans qu'il y ait besoin de connaître cette information.

Voir : Algorithme de consensus, Noeud



Preuve d’autorité

(Proof of authority)

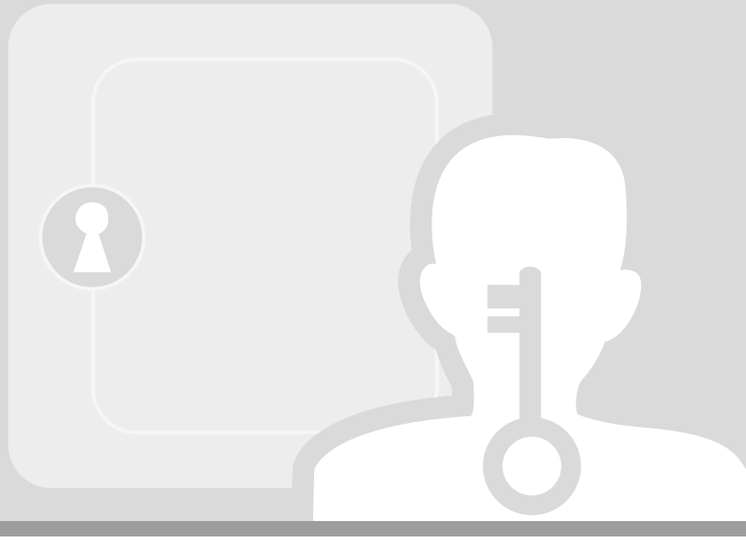
La preuve d’autorité est un algorithme de consensus utilisé le plus souvent pour des blockchains privées. Elle permet de désigner des noeuds du réseau comme validateurs, ces noeuds ayant pour rôle de déterminer l’état du registre pour l’ensemble du réseau.

La preuve d’autorité est principalement utilisée comme une alternative à la preuve de travail ou à la preuve d’enjeu. Elle permet d’augmenter significativement la vitesse de validation des transactions, au détriment cependant de la décentralisation de la blockchain.

Voir : Algorithme de consensus, Blockchain privée, Preuve d’enjeu

Preuve d’enjeu

(Proof of stake)



La preuve d’enjeu est un système de consensus alternatif à la preuve de travail qui prévoit le droit de créer le prochain bloc à un validateur actif sur le réseau ayant mis en dépôt des unités de la crypto-monnaie de cette blockchain. Les consensus à preuve d’enjeu s’inspirent de la théorie des jeux pour fonctionner.

Les consensus à preuve d’enjeu sont moins énergivores que ceux à preuve de travail.

Voir : Algorithme de consensus, Crypto-actif, Preuve de travail



Preuve de travail

(Proof of work)

La preuve de travail, dans une blockchain, est un système de validation de blocs par consensus fonctionnant avec la force brute de calcul, aléatoire et itérative et attribuant les crypto-actifs en fonction de la puissance de calcul mise en disposition.

La preuve de travail est, notamment, le mode de consensus de la blockchain Bitcoin. Ce mode de consensus a été critiqué pour sa consommation d'énergie. D'autres modes de consensus comme la preuve d'enjeu (Proof of Stake) ont fait leur apparition et cherchent à proposer un modèle plus efficace en s'appuyant notamment sur la théorie des jeux.

Voir : Algorithme de consensus, Crypto-actif, Preuve d'enjeu

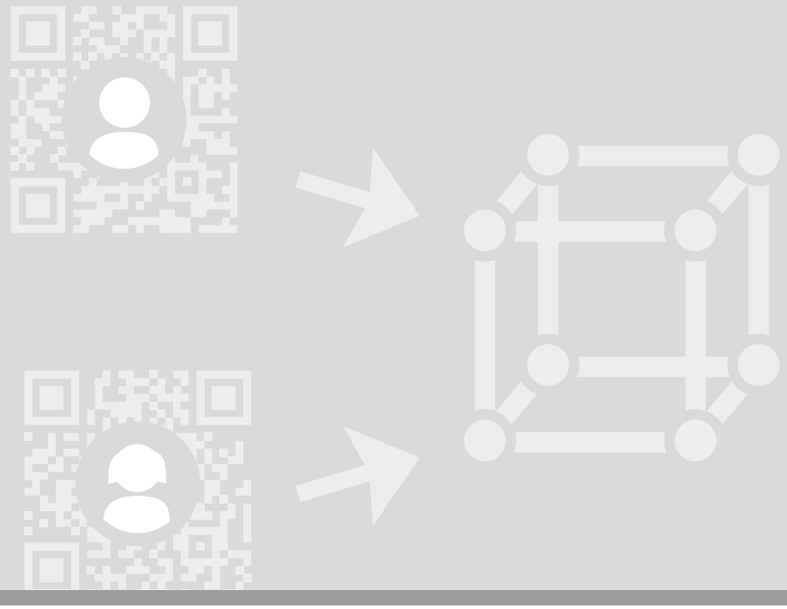


Problème de la double dépense

Un fichier peut être dupliqué lorsqu'il est transmis. En revanche, lorsque la quantité transférée est un actif numérique, il est important de s'assurer que celui qui transmet l'actif n'en garde pas une copie. C'est ce qu'on appelle le problème de la double dépense. Ce problème a été pour la première fois résolu par la blockchain Bitcoin. En tout cas, à condition d'attendre la validation de 3-5 blocs et de s'assurer que la moitié de la puissance de calcul du réseau n'est pas détenue par un seul acteur.

Ce problème doit être absolument résolu pour toute blockchain afin de permettre le transfert de valeur correct d'un noeud à un autre.

Voir : Attaque à 51%, Bitcoin, Internet de la valeur



Pseudonymat

La plupart des blockchains sont pseudonymes au sens où les transactions se font d'une adresse blockchain à l'autre et que les adresses ne disent rien sur l'identité de leur propriétaire. Cependant, dans de nombreux cas, lors de l'achat de tokens sur une blockchain donnée, il est demandé à l'acheteur de décliner son identité.

Certaines blockchains (ZCash, Monero, Dash par exemple) sont anonymes : le registre distribué n'indique pas l'adresse de l'expéditeur ni celle du destinataire.

Voir : Registre distribué, Jeton



Registre distribué

Un registre distribué est un registre contenant un ensemble de transactions. Ce registre au lieu d'être stocké en un endroit unique, le serveur central, est dupliqué sur un ensemble de machines. Le fait que le registre soit copié à l'identique de multiples fois rend l'information coûteuse à modifier : il faudrait la modifier sur tous les noeuds du réseau.

Voir : Noeud, Transaction

Réseau pair-à-pair

Un réseau pair-à-pair est un réseau d'ordinateurs qui communiquent directement d'un ordinateur à l'autre. Le modèle pair-à-pair s'oppose au modèle client serveur où l'un des ordinateurs est le serveur et l'autre le client.

Internet permet aux ordinateurs de communiquer de l'information de pair-à-pair (c'est à dire sans intermédiaire). La blockchain permet à deux ordinateurs d'échanger de la rareté (ou de la valeur) de pair-à-pair (c'est à dire sans avoir à faire appel à un tiers de confiance).

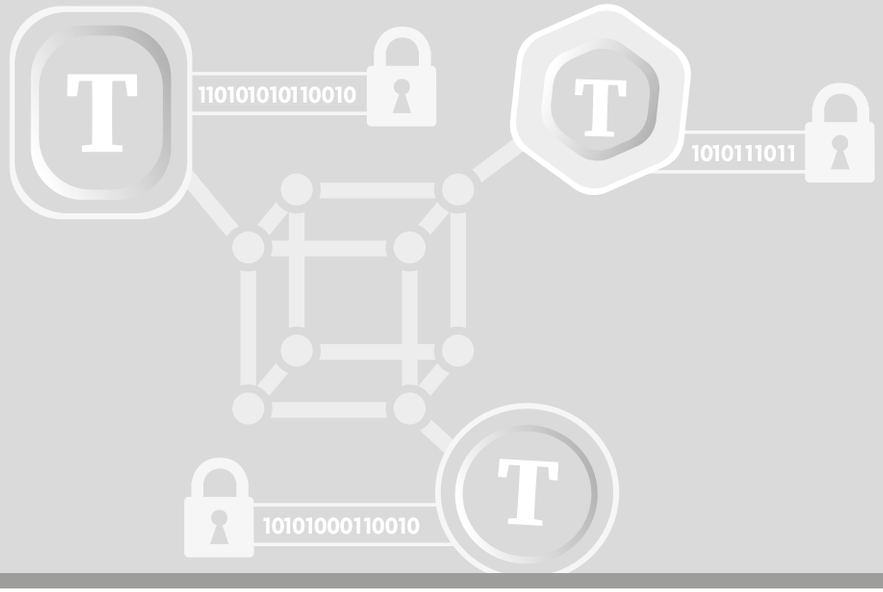
Voir : Blockchain, Internet de la valeur

Signature numérique

La signature numérique d'un document garantit à la fois le contenu de ce document et l'authenticité de la personne qui en est l'auteur. Pour cela, l'auteur prend une empreinte numérique du document (son hash) et le crypte avec sa clé privée. Ainsi, il suffit à réception du document de décrypter avec la clé publique de l'expéditeur l'empreinte numérique (garantie de l'expéditeur) et la comparer à l'empreinte du document dont on veut vérifier l'authenticité (garantie du document).

La signature numérique est utilisée systématiquement sur une blockchain pour passer une transaction par exemple.

Voir : Clé, Cryptographie asymétrique, Empreinte numérique



Tokenisation

La tokenisation désigne la création d'une nouvelle catégorie de jetons dans une blockchain pour déployer une économie propre à un écosystème. La tokenisation est souvent conçue de manière à créer des mesures incitatives pour les contributeurs et usagers de l'écosystème. Le phénomène de tokenisation s'inscrit en partie en réaction au phénomène de perte de confiance dans les devises et monnaies étatiques officielles.

Voir : Jeton

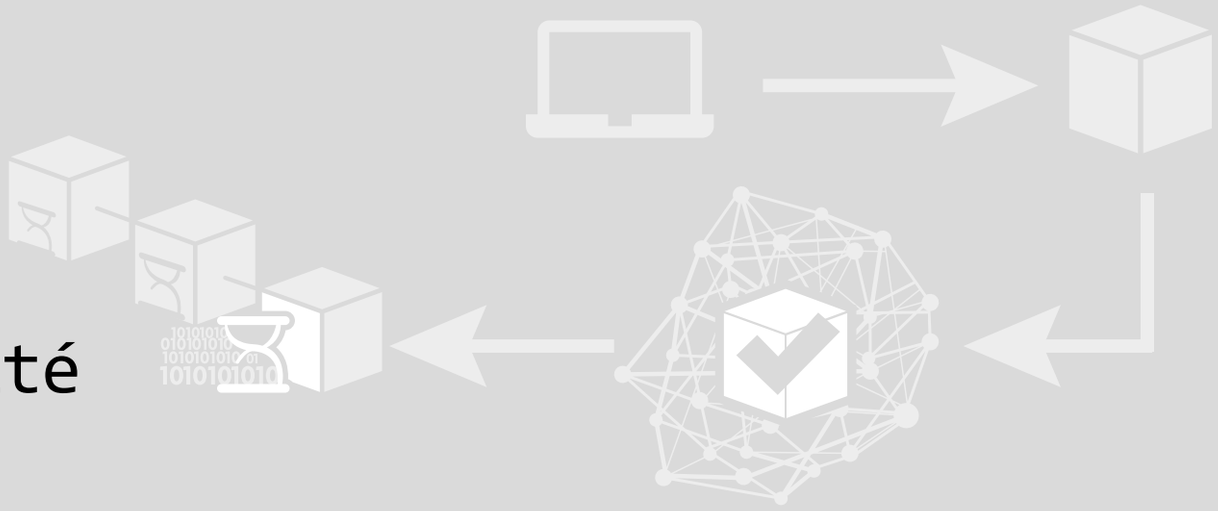
Tolérance aux fautes byzantines



La tolérance aux fautes byzantines est une caractéristique d'algorithmes qui permettent d'éviter les difficultées liées au problème des généraux byzantins, selon lequel, en l'absence de liens de confiance entre les participants, deux tiers de ces derniers doivent agir (ou plus exactement avoir intérêt à agir) de manière honnête pour que le consensus ne soit pas biaisé. Pour éviter les défaillances dans un écosystème décentralisée, les algorithmes de consensus de blockchains doivent être tolérants aux fautes byzantines.

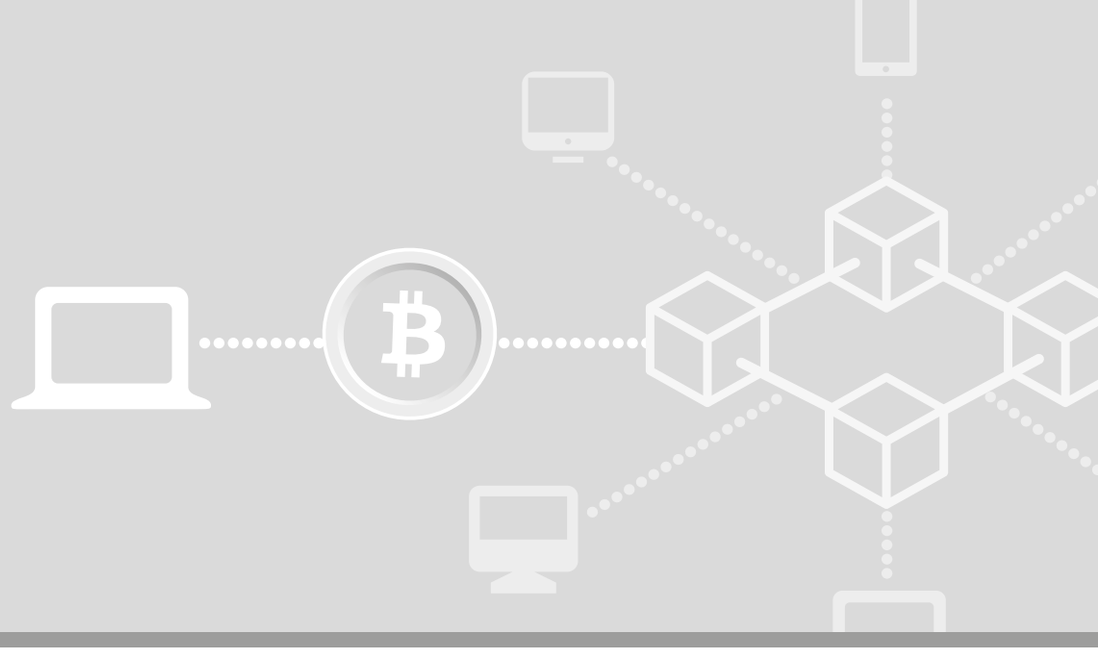
Voir : Algorithme de consensus, Décentralisaiton

Traçabilité



La traçabilité désigne la possibilité de suivre un parcours soit de manière continue à distance grâce à un système de géolocalisation connecté soit *a posteriori* à partir de traces horodatées intégrées lors du parcours. La technologie blockchain permet de limiter les risques d'altération unilatérale des données et d'assurer un degré de transparence élevé.

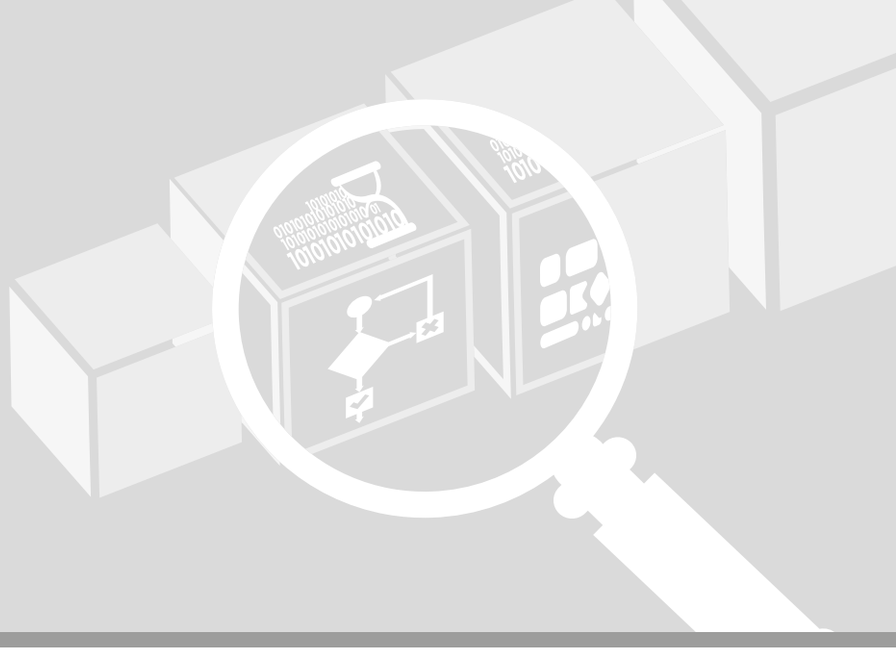
Voir : Horodatage, Transparence



Transaction

Le registre d'une blockchain est constitué de transactions. La transaction la plus simple est l'échange d'actifs numériques d'un noeud à l'autre (A envoie X jetons à B). Une transaction peut aussi se faire d'un noeud vers un contrat intelligent dans le cadre de l'exécution d'un contrat intelligent sur une blockchain programmable comme Ethereum.

Voir : Blockchain, Contrat intelligent, Crypto-actif, Ethereum



Transparence

La transparence est une propriété fondamentale de certaines blockchains (en particulier les blockchains publiques). La transparence d'une blockchain assure que l'ensemble des transactions est visible de l'ensemble du réseau. La transparence permet par exemple d'avoir accès à toutes les transactions de la blockchain Bitcoin depuis sa création.

Dans le cas de blockchains privées, la transparence peut être volontairement limitée afin de préserver la confidentialité.

Voir : Bitcoin, Blockchain privée, Pseudonymat