Smart | APMC

12 2022

Introduction au Blockchain
du concept aux applications

Blockchain, crypto-monnaie, NFT, Web 3.0… Plein de mots qui, au premier abord, peuvent effrayer les personnes non-initiées. Pourtant, les concepts derrière ces termes sont parfois étonnement simples. Cette analyse a l'humble ambition d'introduire le·la lecteur·rice à l'élégance de ces concepts (et plus encore), de leur origine jusqu'à leurs applications concrètes, en y décrivant leurs mécanismes.

L'ORIGINE

La création du concept de la **blockchain** remonte à 1991 quand deux chercheurs – Stuart Haber et W. Scott Stornetta – font breveter une solution informatique permettant l'**horodatage**, à savoir l'indication de la date et de l'heure de documents numériques empêchant qu'ils puissent être antidatés ou altérés.

Leur brevet expire en 2004, quatre ans avant que le **bitcoin** ne soit créé.

Celui-ci a en effet vu le jour en 2008 lorsqu'un inconnu agissant sous le pseudonyme de Satoshi Nakamoto , publie un « livre blanc » (*white paper*) au sujet d'un système de paiement électronique fondé sur le concept de la blockchain.

Mais qu'est-ce que la blockchain et à quoi sert-elle ?

Le concept

Selon le Ministère de l'économie, des finances et de la souveraineté industrielle et numérique français, « *la blockchain est une technologie qui permet de garder la trace (dans un registre) d'un ensemble de transactions, de manière décentralisée, sécurisée et transparente* ». Cette définition est vague car elle se réfère à des concepts abstraits. Développons donc ces concepts de *transaction*, de *décentralisation*, de *sécurité* et de *transparence*.

En économie, une transaction est la plus petite unité qui ne peut être divisée mais qui peut être combinée. C'est l'unité de base du commerce. Acheter une pomme au vendeur du coin est une transaction. L'économie mondiale repose donc sur l'agrégation d'une multitude de transactions de différents acteurs, offrant ou demandant des biens et des services. La monnaie de transaction est, quant à elle, l'outil d'échange utilisé dans une transaction.

La gestion des transactions a pris des formes diverses au cours des âges. Revenons sur son évolution historique avec quelques exemples.

Prenons les tablettes d'argile comme premier moyen historique de compatibilité. C'était une amélioration nette dans les procédés de commerce mais sa lourdeur administrative rendait son utilisation compliquée. Qui plus est, les transactions étaient facilement falsifiables. Dès le VII^{ème} siècle avant J-C, le système évolue avec la monnaie métallique de la Grèce antique. Ainsi, un citoyen ne pouvait pas être plus riche qu'il n'existait de pièces d'or ou d'argent en circulation. Il y a donc une corrélation directe entre la matière constituant la monnaie et sa valeur symbolique.

Le XII^{ème} siècle après J-C connait la naissance de la monnaie fiduciaire avec l'émergence des banques modernes et des lettres de crédits. Considérés comme étant des **tiers de confiance** et dotés de coffres-forts, les orfèvres stockaient de l'or et autres métaux précieux en échange d'un reçu transférable indiquant le montant de ce qui avait été déposé. C'est le début de la convertibilité de la monnaie fiduciaire en un étalon monétaire à poids fixe, le plus souvent l'or. Au XVI^{ème} siècle, on voit apparaître la monnaie de crédit : elle est alors adossée à une dette qui se fait par jeux d'écriture ; et au XVII^{ème} siècle, c'est l'avènement des banques centrales. La fin de la convertibilité en or de la monnaie se fait dès 1970, les monnaies cessent de s'aligner sur la valeur de l'or existant.

On peut dégager de cette évolution jusqu'à aujourd'hui, une tendance à l'utilisation de moyens de plus en plus abstraits et centralisés pour effectuer une transaction.

« Abstraits » puisqu'il y a de moins en moins de rapport entre la valeur réelle de la monnaie de transaction et sa valeur immatérielle (fabriquer un billet de 500€ en 2022 n'en coute pas la valeur dudit billet). Les montants indiqués sur nos comptes en banque ne correspondent également plus à la monnaie en circulation physiquement. Et ces moyens sont aussi « centralisés » puisqu'ils sont contrôlés par des tiers de confiance de

moins en moins nombreux, à savoir les banques centrales.

La blockchain est une rupture forte de cette dernière tendance. En effet, elle permet une gestion décentralisée qui retire la responsabilité de gestion des transactions à un groupe de personnes désignées (comme les notaires pour les transactions immobilières ou les banquiers pour les transactions financières), et place cette responsabilité au cœur de la technologie.

Si nous revenons à notre définition, il nous reste encore deux concepts à définir : la sécurité et la transparence de la blockchain, qui sont les piliers fondateurs de cette technologie. Ainsi, pour se passer des organes de contrôle traditionnels tout en se prémunissant de la fraude, il faut que la technologie établisse des règles strictes et un mécanisme de sécurité qui force tou·tes les participant·es à les respecter. C'est là que la **cryptographie** – une discipline s'attachant à protéger des données considérées comme confidentielles – vient en aide à la blockchain et marque le début de notre immersion dans des concepts un tant soit peu plus techniques.

C'est encore grâce à la cryptographie qu'une blockchain hérite de ses propriétés de transparence. Mais avant de s'attarder sur les tenants et aboutissants de ces fonctions cryptographiques, il convient de mettre en place la fondations sur laquelle une blockchain est construite.

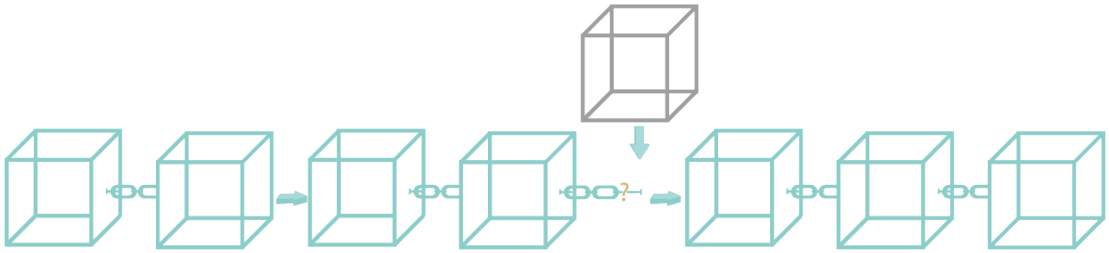
LES DESSOUS DE LA BLOCKCHAIN

Sa structure

Il est difficile de parler de blockchain sans parler de ce qui l'a fait connaitre : le Bitcoin. Des parallèles seront donc souvent fait avec le Bitcoin pour illustrer les propos présentés ici, bien qu'il ne s'agisse pas de l'unique application connue de la blockchain.

La **blockchain** porte bien son nom puisque, conceptuellement, c'est une chaine de blocs. Chacun des blocs d'une blockchain contient toutes les informations d'une transaction validée. On peut déjà remarquer que le concept de « chaîne » est important puisqu'il signifie qu'un bloc est lié à deux autres blocs : le bloc qui le précède et celui qui le succède.

Chaque nouvelle transaction doit être validée « par la communauté » avant de devenir un bloc à part entière de la blockchain. Cette validation est périodique et la période peut varier. Actuellement, elle a par exemple lieu toutes les 10 minutes environ pour le Bitcoin.



Les informations que contiennent un bloc sont les suivantes :

— Un index : la position d'un bloc dans la blockchain.
— L'horodatage : la date à laquelle un bloc a été ajouté à la blockchain.
— Les données : dans une transaction financière, par exemple, il pourrait s'agir du montant de la transaction, de l'expéditeur et du destinataire.
— Un hache : toutes les données du bloc sont passées dans une « fonction de hachage » pour produire un identifiant unique nommé un hache (procédé expliqué ci-dessous).
— Le hache du bloc précédent.
— Le nonce : un nombre utilisé pour générer le hache d'un bloc.

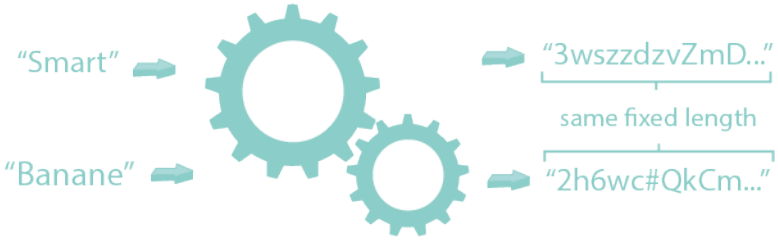
Le hache est au cœur du **principe d'inviolabilité** d'une blockchain et mérite une explication détaillée.

Le hache

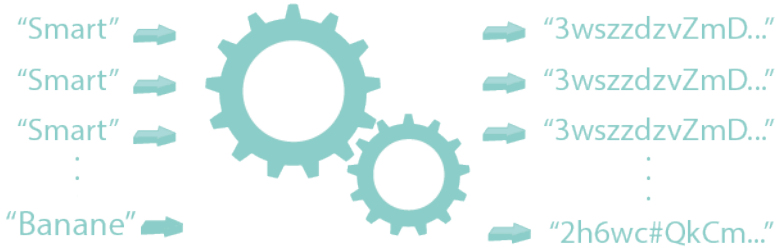
Les fonctions de hachage – qu'on peut considérer simplement comme de petits logiciels informatiques – sont une famille d'**algorithmes cryptographiques** bien pratiques. Elles génèrent un « hache », c'est-à-dire une suite de caractères qui semblent à première vue tout à fait aléatoires, depuis n'importe quel ensemble de données, afin de les identifier de manière unique. Par exemple le mot « Smart » une fois « haché », c'est-à-dire passé dans une fonction de hachage, pourrait générer le hache suivant : « *3wszzdzvZmDExT26R1v* ».

Pour comprendre l'utilité des haches dans une blockchain, il est surtout important d'en connaître les propriétés :

Un hache a une taille fixe. Hacher une image, un film ou un tweet produira toujours un hache de la même taille.

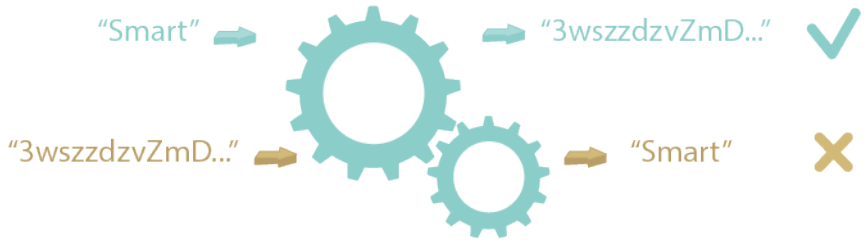


Des données différentes produisent toujours un hache différent, et les mêmes données produisent toujours le même hache. *« Smart » et « Banane » produisent des haches différents l'un de l'autre. En revanche, hacher « Smart » produira toujours « 3wszzdzvZmDExT26R1v» et hacher « Banane » produira toujours « 2h6wc#QkCm8047eRt1l ».*

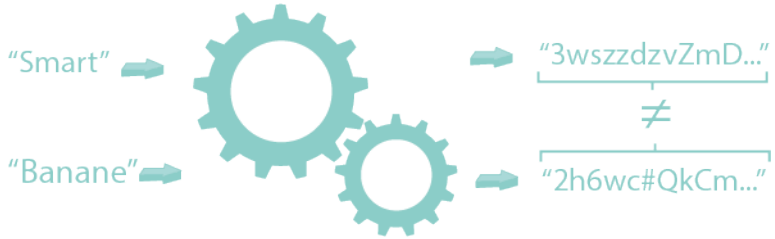


Remarquons aussi que si on hache ensemble les mots Smart et banane (« SmartBanane »), le hache résultant n'aura aucune corrélation avec l'enchaînement du hache du mot « Smart » et du hache du mot « banane ». Il produira, lui-aussi, un hache tout à fait unique.

Il est très facile de calculer un hache depuis des données spécifiques, mais très difficile de calculer des données depuis un hache spécifique. *On peut facilement trouver le hache « 3wszzdzvZmDExT26R1v » depuis le mot « Smart » mais il serait impossible de trouver le mot « Smart » depuis le hache « 3wszzdzvZmDExT26R1v ».*



Le moindre changement de données produit un immense changement dans le hache résultant. *Le hache de « Smart » et « SMart » produisent des haches radicalement différents*.



Dans une blockchain, le hache de chaque bloc est calculé à partir de ses données mais également à partir du hache du bloc précédent. En conséquence, si je souhaite modifier un bloc d'une blockchain, je devrais recalculer le hache de tous les blocs précédents pour obtenir des haches qui correspondent aux données de la nouvelle transaction.

Les fonctions de hachage nous permettent même de faire mieux : en hachant les données d'un bloc A avec le hache du bloc B (après tout, un hache est juste un bout de texte), nous avons cryptographiquement lié ces deux blocs. *Comme les deux blocs sont liés, si les données du bloc B sont altérées, son hache sera différent, et donc le hache du bloc A le sera aussi, même si les données de ce dernier n'ont jamais été modifiées.*

Le nonce

Pour les plus avertis, il reste néanmoins une question en suspens : comment générer des haches différents pour un bloc qui contiendrait les mêmes données ?

Selon la deuxième propriété énumérée d'un hache, le même jeu de données produit toujours exactement le même hache. Il serait effectivement impossible de créer des haches différents pour les mêmes données. Pour altérer un hache sans en changer les données pertinentes, on utilise un nombre arbitraire aléatoire appelé « nonce ».

Le nonce ou « nombre de consensus » fait lui aussi partie des données d'un bloc. Son intérêt réside donc dans le fait que, une fois ajouté aux données d'un bloc, le modifier change à son tour le hache d'un bloc. Outre son intérêt pour le calcul d'un hache qui respecterait une structure imposée, le nonce n'a aucune autre signification ou utilité : c'est un nombre « poubelle » utilisé comme paramètre de diversification pour la création de haches uniques.

> **Dans une blockchain, le hache de chaque bloc est calculé à partir de ses données mais également à partir du hache du bloc précédent.**

Ainsi, hacher les données d'un bloc qui contient (comme dans l'exemple de la transaction financière) l'expéditeur, le destinataire et le montant de la transaction financière permet d'identifier de manière unique ces données. Si je décide d'altérer le montant d'un bloc existant d'une blockchain, le changement serait visible immédiatement, en constatant simplement que le hache de ce bloc a changé. Nous avons alors un tout nouveau hache, qui peut être parfois très différent du hache de départ.

Le protocole Bitcoin impose que le hache de chaque bloc commence par certains caractères arbitraires. Or, pour générer un hache qui contient un préfixe spécifique, il faudra calculer de nombreux haches différents pour un même bloc avant de tomber sur la bonne combinaison.

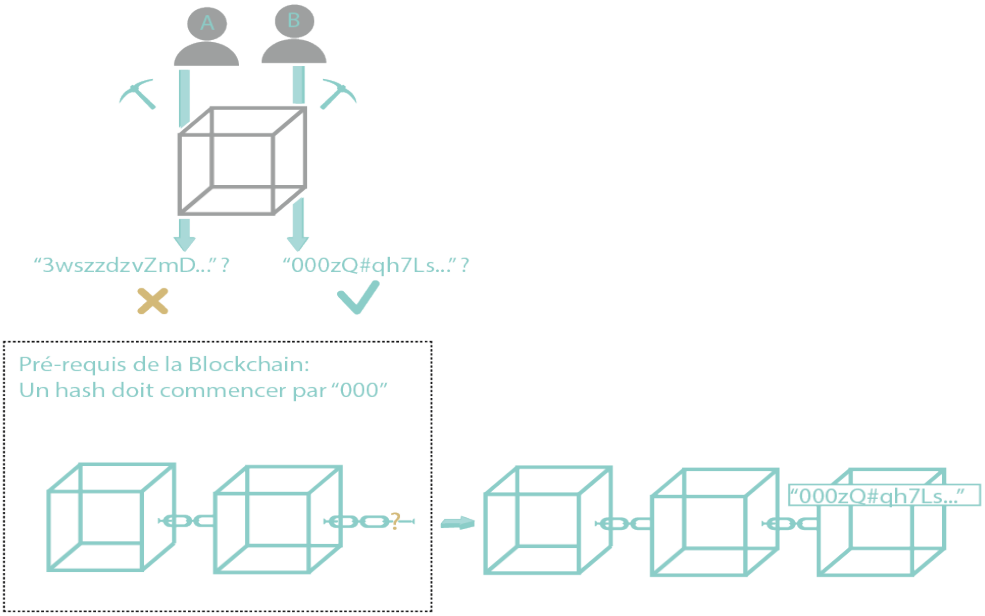
Ses mécanismes

La preuve de travail

Dans le protocole Bitcoin, le calcul d'un hache s'appelle « la preuve de travail » (*Proof of Work*). Concrètement, quand un ordinateur calcule un nouveau hache pour une blockchain, il peut le soumettre à validation. La validité du hache par rapport aux données du bloc constitue la preuve de travail, parce qu'il démontre qu'il a dû effectuer un travail computationnel[1] pour arriver au hache.

Revenons à l'exemple d'une personne qui souhaite changer la valeur d'un bloc existant. Elle devra non seulement recalculer le hache de tous les blocs qui le suivent, mais également y ajouter le nonce adéquat. En présence d'une blockchain contenant beaucoup de blocs comme le Bitcoin (actuellement, il y en a plus de 760.000[2]), cela commence à faire beaucoup de travail, même pour un ordinateur.

La **preuve de travail** est au centre du processus de validation d'une transaction dans la blockchain.



1 Utilisation des concepts fondamentaux de l'informatique pour résoudre une problématique.

2 Cf. https://www.blockchain.com/explorer/blocks/btc

Le minage

Nous avons vu que pour ajouter un bloc à une blockchain, il fallait d'abord lui calculer un hache valide pour qu'il puisse être validé par la communauté. Dans le protocole Bitcoin, l'acte de validation d'une transaction s'appelle le « minage » (dans notre exemple, on parle même plus précisément de minage via preuve de travail).

Les autres participant·es de la blockchain vérifient que le hache corresponde bien aux données du bloc et, si c'est le cas, il est ajouté à la blockchain. L'ordinateur responsable du calcul du hache valide est défini comme le mineur du bloc et sa contribution au réseau est récompensée par des frais de transaction qui correspondent à un certain montant en Bitcoin.

Cela encourage tout le monde à participer activement à la validation des transactions. Malheureusement, cela crée aussi une compétition entre les différent·es participant·es d'une blockchain pour être le/la premier·ère mineur·e d'un bloc. Les ordinateurs tournent tous simultanément dans l'espoir de trouver la combinaison gagnante d'un bloc avant les autres. Le/la vainqueur·euse remporte les frais de transactions et le calcul de tous les autres – qui ont eu moins de chance[3] – a été vain. Toute cette puissance de calcul perdue a évidemment un coût énergétique non-négligeable[4].

L'or numérique

Il convient encore de préciser que le Bitcoin est une ressource finie, comme l'or par exemple. Le nombre limité de Bitcoin a été mathématiquement fixé à 21 millions et il ne pourra pas y en avoir plus[5].

Afin de poursuivre la comparaison avec l'or, les Bitcoins n'ont également pas encore été entièrement minés. En effet, on constate que la meilleure motivation pour qu'un·e participant·e mette son ordinateur à disposition de la communauté pour valider des blocs, est la perspective d'une récompense en Bitcoin. Et ces Bitcoins de récompense viennent de la réserve de Bitcoin qui n'ont pas encore été minés. Pour s'assurer qu'on n'arrive pas à bout trop rapidement de cette réserve de Bitcoin (et donc d'assurer qu'on puisse récompenser les mineurs pendant un certain temps encore), le protocole Bitcoin augmente progressivement sa complexité, et donc le temps nécessaire pour miner un bloc. Dans les faits, la

3 En réalité il s'agit plus de pouvoir computationnelle que de chance. Celui qui a la/les machine(s) les plus performantes ont le plus de « chance » de miner un bloc.

4 Il existe d'autres moyens quelque-peu plus écologiques pour déterminer un·e mineur·e comme le *Proof of Stake* utilisé par une autre crypto-monnaie appelée *Ethereum*.

5 https://www.numerama.com/tech/quest-ce-que-le-halving-du-bitcoin-et-pourquoi-est-ce-si-important·html

complexité pour miner un bloc est définie par la structure imposée pour qu'un hache soit considéré comme étant valide.

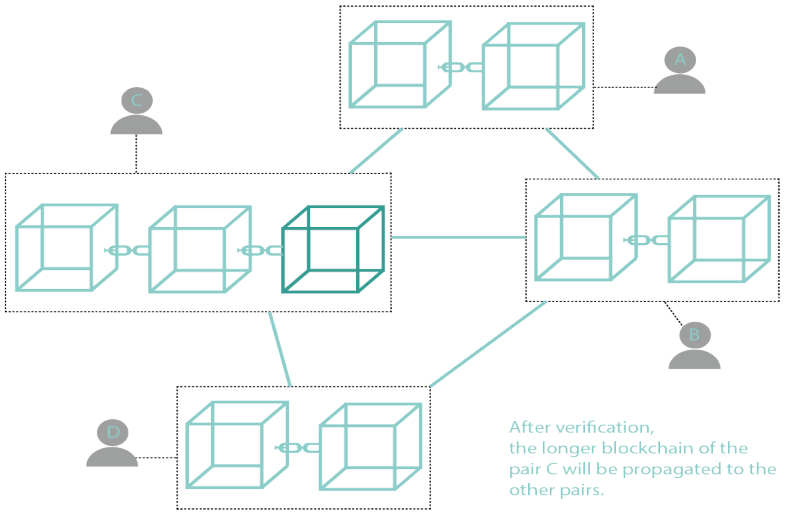
Cette complexité est également proportionnelle aux ressources computationnelles du réseau et s'assure qu'une transaction ne puisse être ajoutée qu'environ toutes les dix minutes. Autrement dit, plus il y a d'ordinateurs sur le réseau, plus le hache d'un bloc pourrait être calculé facilement, et donc plus le protocole Blockchain doit imposer une structure de hache complexe[6].

Dans un système où il n'y pas de tiers de confiance, tout le monde doit pouvoir posséder les informations sur la blockchain pour valider une transaction : la blockchain est un registre distribué, c'est-à-dire que chaque participant·e possède une copie de la blockchain sur son ordinateur. Toutes ces copies de blockchain constituent ce qu'on appelle le réseau pair à pair (*Peer to Peer*).

Le réseau pair à pair

Admettons que je mine un bloc, je l'ajoute alors à la copie locale de la blockchain sur mon ordinateur et communique au pair le plus proche géographiquement pour lui signifier de mettre sa blockchain à jour avec la mienne. Le « pair » en question remarque que sa copie de la blockchain n'est plus à jour et, après avoir vérifié que les haches des blocs sont conformes, ajoute le bloc à sa copie. Il répètera lui-même ce procédé pour avertir de nouveaux pairs du changement, et ainsi de suite jusqu'à ce que tout le réseau ait pris connaissance du nouveau bloc.

Si deux pairs minent simultanément un nouveau bloc, la blockchain qui finira par se propager sera celle sur laquelle le prochain bloc sera miné en premier puisqu'elle sera considérée comme la blockchain la plus à jour.



6 Il existe un deuxième mécanisme pour équilibrer le Bitcoin appelé « *halving* » qui consiste à réduire de moitié la récompense du minage d'un bloc. Elle se produit plus au moins tous les 4 ans. Le prochain *halving* de la blockchain Bitcoin se produira en 2024.

Dans le cas d'un fraudeur qui aurait altéré les informations d'un bloc déjà validé sur la blockchain, compte tenu du temps nécessaire au recalcul de chaque hache qui précèdent le bloc modifié, sa copie de la blockchain serait non seulement complètement différente mais aussi bien moins à jour que la copie des autres pairs. Elle serait dès lors ignorée par les pairs du réseau et ne pourra pas se propager.

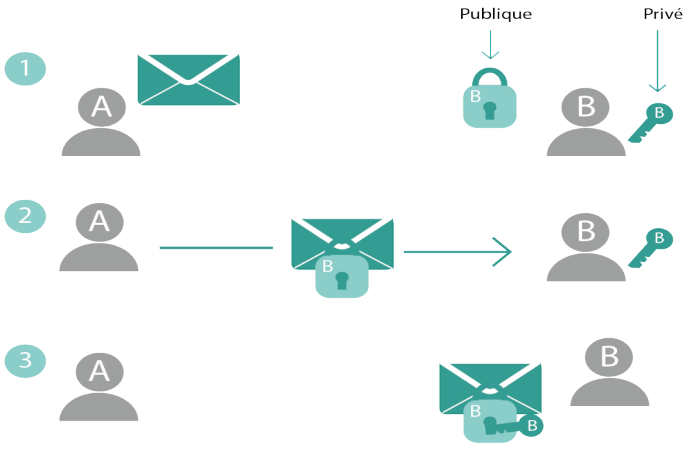
Les termes « participant·es », «pairs » et « acteurs·rices » sont mentionnés tout au long de cette analyse et de manière interchangeable. Dans le contexte qui nous intéresse, ils/elles correspondent tou·tes à l'idée d'une personne qui possède une copie de la blockchain[7].

Pourtant, les pairs ne s'identifient pas avec leur vrais noms: ils utilisent des sortes de pseudonymes pour communiquer. Cela leur permet de disposer d'un certain anonymat pour effectuer des transactions. Pour autant, grâce à un nouvel outil de notre arsenal cryptographique, nous allons voir qu'un pair ne pourra pas se faire passer pour un autre en signant simplement ses transactions avec un pseudonyme qui n'est pas le sien.

Le pseudo-anonymat authentifié

Il existe une technique cryptographique fréquente qui – en plus d'être à la base des communications sécurisées sur le web – est très utile sur la blockchain : le **chiffrement asymétrique**.

La problématique est la suivante : comment un pair qui veut communiquer avec un autre peut-il prouver son identité en ne divulguant aucune information secrète/sensible au réseau et, en même temps, s'assurer que son message arrive dans les mains du destinataire désiré ? En réalité, chaque pair possède une clef secrète qui lui permet d'ouvrir un cadenas public.



7 Il existe plus précisément 2 types de participants : les nœuds complets qui possèdent une copie complète de tous les blocs de la blockchain et qui peuvent miner des blocs et nœuds partiels ne possèdent qu'une version résumée des blocs d'une blockchain dans un arbre de Merkel. Un arbre de Merkel est un algorithme cryptographique qui permet de conserver toutes les propriétés de vérification entre pairs de la Blockchain en ne gardant que certaines transactions clés.

Chaque cadenas public ne peut être ouvert qu'avec la clef secrète correspondante. Si le pair A veut être certain de communiquer avec le pair qui possède le cadenas B, il créera un message et le partagera (le vrai terme est « chiffré ») avec le cadenas B. Seul le propriétaire de la clef secrète B qui permet d'ouvrir le cadenas B sera capable de l'ouvrir et le pair A peut donc être certain que son message est arrivé à bon port.

Inversement, si le pair B veut s'assurer que le message vient bien du pair A, il écrit un message qui demande si le pair A veut communiquer avec lui et le protège avec le cadenas A avant de le transférer. S'il reçoit une réponse positive, il sait qu'il communique à la bonne personne.

Le cadenas public est l'équivalent d'un pseudonyme sur une blockchain et sert comme adresse pour le destinataire. La clef privée est identique à un mot de passe : c'est l'unique information qui prouve qu'un pair est propriétaire d'un cadenas spécifique et donc d'une ou de plusieurs transactions.

Transparence

Un des traits fascinants de la cryptographie moderne est la maxime de Shannon[8]: « l'adversaire connait le système »[9]. Elle part du principe qu'un acteur malicieux finira forcément par mettre la main sur toutes les informations concernant les moyens de protection utilisés. L'objectif pour les cryptographes est donc la conception de méthodes de protection qui restent sécurisées, même si elles sont parfaitement connues d'un adversaire. De là découle naturellement la propriété de transparence de la blockchain. L'entièreté des transactions réalisées sur une blockchain peuvent être visualisées publiquement, ainsi que l'ensemble de son code source, sans pour autant constituer une faille de sécurité. Comme nous l'avons vu avec la cryptographie asymétrique, c'est la clef privée qui rend le système sécurisé, et en ce qui concerne les fonctions de hachage, c'est l'impossibilité de pouvoir décrypter un hache.

Maintenant que nous avons couvert toutes les propriétés énoncées dans notre définition initiale, nous sommes capables de passer rapidement en revue certaines utilisations spécifiques de la blockchain.

8 Un ingénieur américain en génie électrique, fondateur de la théorie de l'information. Cf. https://www.itsoc.org/about/shannon.

9 Claude Shannon, « Communication Theory of Secrecy Systems », in *Bell System Technical Journal*, vol. 28,ſ 1949, p. 662

LES DÉRIVÉS

Les crypto monnaies

On a déjà beaucoup parlé du protocole Bitcoin dans le cadre de la blockchain, mais il existe aussi une multitude d'autres crypto-monnaies qui peuvent, en plus des principes de la blockchain déjà énumérés ici, posséder d'autres fonctionnalités.

Ethereum est par exemple une autre crypto-monnaie bien connu, qui permet de contenir des applications au sein de sa blockchain appelées des « Contrats intelligents » (*Smart Contract* en anglais)[10].

NFT – Non-Fongible Token

Il s'agit d'un identifiant unique – aussi appelé « jeton»/token, stocké sur la blockchain. Ce n'est plus de l'argent qui est échangé, comme dans le cas du protocole Bitcoin, mais le « jeton»/token en question. Ce jeton est non fongible, c'est-à-dire qu'il n'est pas interchangeable (au contraire de la monnaie qui est fongible : une pièce de 1€ vaut la même chose qu'une autre pièce de 1€)[11]. Il suffit d'apposer à un jeton cryptographique une photo (même numérique), une œuvre ou n'importe quel autre objet pour qu'il fasse conceptuellement partie de la blockchain.

Le WEB 3.0

Le WEB 3.0 se veut être l'évolution de l'internet qu'on connaît aujourd'hui, le Web 2.0. Dans ce dernier, les données sont relayées aux utilisateur·rices par des serveurs web qui font office « d'autorité » sur les informations qu'elles partagent. Le Web 3.0 vise à décentraliser ces informations en s'appuyant sur le concept de la blockchain. Chaque utilisateur·rice (par le biais de leur ordinateur) possède les informations – auparavant uniquement contenues sur des serveurs web – et se les partagent entre eux/elles sans aucuns intermédiaires (/serveurs).

10 Concept formulé en 1996 par le développeur Nick Szabo, un Smart contract est un programme informatique enregistré sur une Blockchain, la plupart du temps *Ethereum*. Il permet de déclencher des transactions conditionnelles dont l'exécution dépend de facteurs définis à l'avance via un algorithme.

11 Cf. https://www.futura-sciences.com/tech/definitions/tech-non-fungible-token-19205/

LES APPLICATIONS

Il existe de très nombreuses applications possibles de la blockchain, en dehors des crypto-monnaies, qui ont popularisé son concept. En effet, Les mécanismes de transparence, de décentralisation, d'anonymat et d'inviolabilité, qui sont au cœur de la blockchain, permettent d'entrevoir de nombreuses possibilités dont en voici quelques exemples :

Sécurité alimentaire

Le mouvement des produits alimentaires, de leur origine de production jusqu'au supermarché peuvent être persistés dans la blockchain. Ainsi, non seulement le consommateur dispose d'une transparence inégalée qui leur permettrait de prendre des décisions éclairées basées sur des choix écologiques et éthiques (ou autres) mais aussi par exemple de tracer très rapidement la source d'un contaminant d'origine alimentaire.

Immobilier

Outre la réduction des coûts des contrats d'achat et de vente de propriétés immobilières qui se passent alors d'un tiers de confiance spécialisé (comme un notaire), les propriétés cryptographiques inhérentes à la blockchain permettent de minimiser les risques liés à ces transactions.

Vote numérique

La blockchain a la capacité d'éliminer la fraude électorale en rendant les votes complètement transparents et de visibiliser tout changement qu'on pourrait lui apporter. L'identité des votants est évidemment anonymisée.

Gestion de l'identité

L'identité d'une personne pourrait également être vérifiée directement dans une blockchain. Cela aurait différents bénéfices comme l'interopérabilité de cette identité sur plusieurs services, l'assurance qu'elle sera persistée (plus de vols d'identité), sa résilience à la censure,...

Système de santé

La blockchain permet de conserver la trace des médicaments prescrits à un patient et ses antécédents médicaux. Les informations restent – bien entendu – confidentielles et les patients peuvent accéder à ses informations avec une clé numérique.

Testaments, héritages, suivi des armes,... La blockchain peut trouver une application pour toutes les données dont la transparence, l'intégrité et la disponibilité doivent être garanties[12].

Victor Van Duijnen
Décembre 2022

12 Cf. https://morethandigital.info/fr/blockchain-possibilites-applications-et-cas-dutilisation-de-la-technologie/;
https://actualiteinformatique.fr/blockchain/quelles-sont-les-applications-de-la-blockchain

SOURCES ET RESSOURCES

https://www.forbes.com/advisor/investing/cryptocurrency/who-is-satoshi-nakamoto/

https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application

https://www.oracle.com/fr/security/qu-est-ce-que-la-cryptographie·html

https://www.blockchain.com/explorer/blocks/btc

https://www.numerama.com/tech/quest-ce-que-le-halving-du-bitcoin-et-pourquoi-est-ce-si-important·html

https://www.itsoc.org/about/shannon.

https://www.futura-sciences.com/tech/definitions/tech-non-fungible-token-19205/

https://morethandigital.info/fr/blockchain-possibilites-applications-et-cas-dutilisation-de-la-technologie/

https://actualiteinformatique.fr/blockchain/quelles-sont-les-applications-de-la-blockchain