L'ÉCO EN BREF

La blockchain

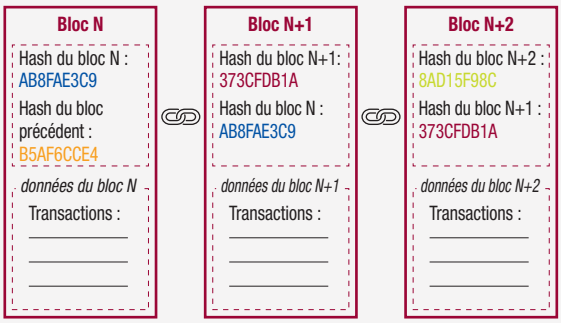
L'ESSENTIEL

La *blockchain* ou « chaîne de blocs » est une technologie de stockage et de transmission d'information qui fonctionne sans organe central de contrôle. La blockchain est née en 2008 avec le Bitcoin. À l'origine, elle a été pensée pour créer ce nouvel actif financier – appelé crypto-actif – géré par un algorithme sans intervention d'autorité centrale.

On parle d'une technologie décentralisée car l'architecture de la blockchain est construite sans serveur central et parce que la gouvernance de la blockchain repose sur la répartition du pouvoir entre tous les utilisateurs de la blockchain.

La blockchain se matérialise par une base de données distribuée au sein d'une communauté d'utilisateurs. Cette base, appelée registre, contient l'historique de toutes les transactions effectuées entre les utilisateurs depuis la création de la blockchain. Les transactions sont regroupées au sein d'une succession de blocs reliés les uns aux autres par un procédé cryptographique. La cryptographie (du grec « crypto » signifiant caché et « graphie » signifiant écrire) prend appui sur une fonction mathématique de « hachage » qui transforme une donnée entrante en un identifiant numérique unique, le « hash », garantissant l'intégrité de la donnée.

Schéma d'une chaîne de blocs

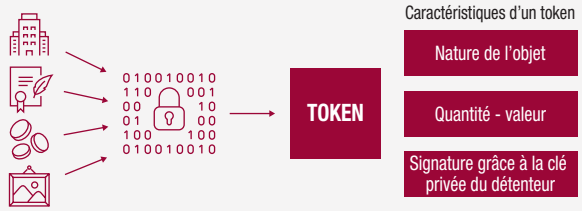


La blockchain est utilisée pour deux fonctions :

Première fonction « enregistrement et stockage » : la blockchain permet d'enregistrer et de stocker des valeurs et des transactions tout comme un notaire. Toute valeur ou information qui entre dans la blockchain par le biais d'une transaction est incluse dans un bloc relié cryptographiquement aux blocs précédents. Les blocs ne pouvant être modifiés, la blockchain constitue une base de données immuable contenant l'historique de tous les échanges effectués sur la blockchain depuis sa création.

Seconde fonction « émission et transmission » : en s'appuyant sur cette capacité d'enregistrement et de stockage de données, la blockchain permet d'émettre et de transmettre des actifs numériques natifs, tels que des Bitcoins, mais aussi des actifs existants enrichis par un procédé appelé « tokenisation ». La tokenisation d'un actif réel consiste à convertir les droits qui lui sont attachés en un enregistrement numérique. C'est une manière de représenter dans le monde digital un bien immobilier par exemple, ou une obligation, une propriété intellectuelle, demain une monnaie, et de pouvoir échanger cet actif en bénéficiant des mécanismes de la blockchain. Une fois enregistré sur la blockchain, le token peut donc être échangé au sein de la communauté et tout l'historique lié à la détention de cet actif est tracé dans les blocs.

Schéma de tokenisation



Grâce à ces deux fonctions « enregistrement/stockage » d'une part et « émission/transmission » d'autre part, la technologie de la blockchain permet à des personnes connectées en réseau, qui ne se connaissent pas ou qui ne se feraient pas nécessairement confiance de :

- s'affranchir des intermédiaires tels que les banques, chambres de compensation, dépositaires, notaires, cadastres...
- s'assurer de la fiabilité et de la sécurité de leurs opérations.

Il existe plusieurs types de blockchain :

- des blockchains publiques : l'accès et l'utilisation sont ouverts à tous depuis internet. Des exemples de ce type de blockchain sont Bitcoin ou Ethereum ;
- des blockchains privées, également appelées « permissionnées » : l'accès et l'utilisation sont réservés à un nombre restreint d'utilisateurs. Une unité centrale en contrôle les accès. Une blockchain privée est de fait moins décentralisée qu'une blockchain publique.

Comprendre la technologie de la blockchain

L'identification de chaque partie (acheteur, vendeur) s'effectue par un procédé cryptographique. Chaque utilisateur dispose (1) d'une clé privée lui permettant de signer ses transactions, (2) d'une clé publique qui ne peut s'associer qu'à la clé privée, permettant de vérifier l'authenticité et l'intégrité des transactions, et enfin (3) d'une adresse, combinaison de lettres et de chiffres, dérivée de la clé publique et comparable à l'identifiant d'un compte bancaire. L'utilisation de la paire de clés permet de garantir l'intégrité et la sécurité des transactions entre utilisateurs identifiés chacun par leur adresse publique.

La transaction entre deux parties se fait en renseignant les adresses (pour identifier les contreparties). Puis, l'émetteur signe la transaction grâce à sa clé privée. L'information relative à la transaction est ensuite envoyée à un réseau décentralisé composé de « nœuds » hébergés sur des ordinateurs situés dans le monde entier pour les blockchains publiques.

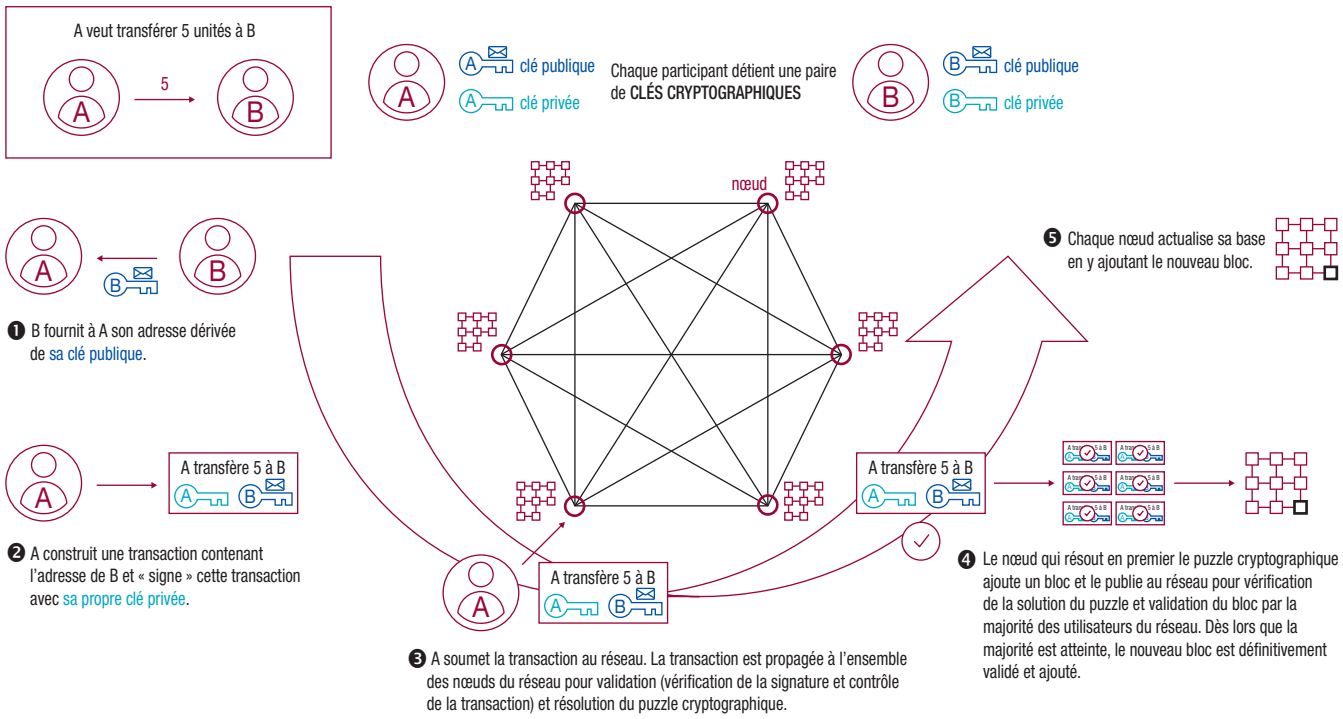
Dans les blockchains fonctionnant sur le principe de la preuve de travail (« *proof of work* », voir schéma), certains nœuds dotés de puissance de calcul et appelés mineurs, vérifient les transactions reçues puis se lancent dans la résolution d'une équation mathématique (appelée puzzle cryptographique). Le premier mineur qui réussit à résoudre l'équation mathématique crée un bloc et le transmet à la communauté pour vérification de la solution de l'équation mathématique et validation du bloc par la majorité des utilisateurs du réseau (on parle d'un consensus à 50,1 % du réseau). C'est lui seul qui percevra une rémunération pour le travail accompli.

Chaque nouveau bloc validé est ajouté à la blockchain et une copie est transmise à tous les nœuds du réseau. Chaque nœud héberge donc une copie de la base de données dans laquelle est inscrit l'historique complet des transactions effectuées depuis la création de la blockchain. Toutes les parties prenantes peuvent y accéder car chaque partie a sa propre copie de l'entièreté de la base.

Grâce à cette technologie, l'intégration des blocs est chronologique, indélébile et infalsifiable. Le système de validation repose sur un mécanisme de consensus de tous les « nœuds » à chaque ajout d'information. Cette décentralisation de la gestion de la sécurité rend très difficile voire impossible la falsification des transactions, sauf à posséder l'équivalent de 50,1 % des ordinateurs. C'est la pluralité des nœuds qui permet une répartition du pouvoir sur le réseau.

La blockchain, via son mécanisme de consensus, permet ainsi de réduire les coûts des intermédiaires et des organes centraux de contrôle qui sécurisent une transaction. Ceci ne signifie pas que l'usage de la blockchain est gratuit pour ses utilisateurs. Sur les blockchains publiques, chaque transaction est effectivement payante afin de rémunérer les nœuds mobilisant de la puissance de calcul nécessaire à la création des blocs et de prévenir les attaques informatiques. Ainsi, en moyenne, une transaction sur Bitcoin a coûté environ 1,80 $ en 2021, une transaction sur Ethereum environ 23 $ et seulement quelques fractions de centimes pour les blockchains de dernières générations (Tezos, Solana, Avalanche…).

Schéma de validation d'une transaction dans une blockchain à preuve de travail



Comprendre

Les domaines d'usage

La technologie blockchain est une innovation majeure à l'origine du Bitcoin, mais son champ d'application est bien plus large.

Elle assure, via une diffusion très efficace de l'information à tous les utilisateurs de la communauté, une transparence des échanges et offre des possibilités d'automatisation et de tokenisation via les « *smart contracts* ». Ces « contrats intelligents » sont des protocoles informatiques qui permettent la réalisation automatique, donc sans tiers de confiance, de transactions sur la blockchain lorsque certaines conditions prédéfinies et inscrites dans le code sont respectées.

Ces protocoles associés à la blockchain pourraient modifier le fonctionnement de nos systèmes de régulation centralisée, diminuer les coûts et transformer de nombreux domaines : la banque (par la tokenisation des actifs pour enregistrer et valider des transactions), l'assurance (pour automatiser les procédures de remboursement), l'immobilier (pour enregistrer les transactions), le marché de l'art avec les jetons non fongibles (NFT – *Non Fongible Token*), les plateformes de mise en relation, les élections (pour sécuriser le vote en ligne), l'attribution des diplômes et des certificats…

Les limites de certaines blockchains

La réglementation « *Know your customer* » (obligation de connaître son client), que les banques et entreprises appliquent pour vérifier l'identité de leurs clients, n'existe pas sur une blockchain publique, ce qui entraîne des risques au regard de l'utilisation de blockchain pour financer le terrorisme ou blanchir de l'argent. En effet, la connaissance de la clé publique ne permet pas de connaître l'identité réelle de la contrepartie, connue uniquement par son adresse que l'on peut comparer à un pseudonyme.

Par ailleurs, la vitesse des transactions sur la blockchain est ralentie par le mécanisme de validation des blocs.

Enfin, la mise à disposition permanente d'ordinateurs répartis dans le monde entier est énergivore. La blockchain fonctionnant sur le principe de la preuve de travail (« *proof of work* ») est très consommatrice d'énergie car le réseau d'ordinateurs mobilise une forte puissance de calcul pour les procédés de validation des blocs. De surcroît, les mineurs sont poussés à toujours augmenter leur puissance de calcul du fait du caractère essentiellement concurrentiel de leur activité. En effet, la récompense pour le travail réalisé n'est attribuée qu'au premier mineur ayant réussi à assembler le puzzle cryptographique et à calculer un bloc validé par le réseau. À titre d'illustration, la consommation énergétique d'une seule transaction en Bitcoin équivaut à celle de 834 000 transactions par carte bancaire.

Ainsi, certains protocoles comme Ethereum prévoient d'abandonner la preuve de travail au profit notamment de la preuve d'enjeu (« *proof of stake* ») à 99,95 % moins énergivore. Dans une blockchain fonctionnant à la preuve d'enjeu, les mineurs sont appelés validateurs et sont chargés de créer de nouveaux blocs. Pour réduire la compétition, un validateur est choisi aléatoirement au sein d'une communauté d'utilisateurs ayant décidé de s'engager en misant une partie de leur portefeuille de crypto-actifs. La mise est une somme placée sous séquestre qui peut être confisquée par l'algorithme si le travail attendu n'est pas réalisé ou mal réalisé. Le validateur reçoit une rémunération une fois le travail de validation accompli.

Un peu d'histoire

- 2008 Invention de la technologie de la blockchain par un ou plusieurs individu(s) inconnu(s) dont le pseudonyme est **Satoshi Nakamoto**.
- 2009 Première transaction en **Bitcoin**.
- 2015 Lancement d'**Ethereum** et des premiers **contrats intelligents**, programmes informatiques exécutés sur la blockchain permettant de rendre des transactions programmables.
- 2017 MADRE **première blockchain interbancaire permissionnée** dans le monde mise au point par la Banque de France pour gérer les identifiants SEPA.
- 2019 En France, la loi PACTE crée un régime optionnel pour encadrer l'émission de **jetons numériques** (token).
- 2020 Lancement par la **Banque de France** du programme d'expérimentation sur la monnaie numérique de banque centrale interbancaire.
- 2021-2022 La **Chine** interdit l'activité de minage sur son sol. Le **Salvador** puis le **Centrafrique** octroient au Bitcoin le cours légal dans le pays.

Pour en savoir plus

À voir

- Qu'est-ce que la blockchain ?, YouTube, vidéo Rue 89
- Le bitcoin, qu'est-ce que c'est ?, vidéo Citeco
- Une minute pour comprendre la blockchain, vidéo Les directions de Bercy

Liens utiles

- La blockchain : une révolution ?, La Finance pour Tous
- Les enjeux des blockchains, France Stratégie