ANCRE
ASSOCIATION NATIONALE pour la COUVERTURE des risques, la RETRAITE et l'EPARGNE

Mieux comprendre l'économie et la finance

La blockchain

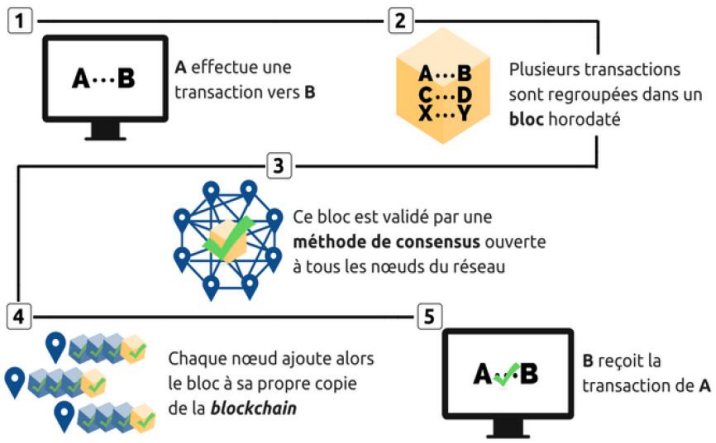
La blockchain en quelques mots

La blockchain est un mécanisme informatique de stockage des données, qui se distingue d'une base de données traditionnelle par plusieurs aspects :

- La blockchain est littéralement une « chaîne de blocs » reliés chronologiquement, chaque bloc faisant référence au bloc précédent. Un bloc ne peut être ajouté qu'en dernière position de la chaîne.
- La blockchain est sécurisée par cryptographie : l'ajout d'un nouveau bloc doit être validé par la résolution d'un problème mathématique complexe.
- La blockchain est généralement décentralisée : elle n'est pas hébergée sur un serveur unique mais répartie sur de multiples ordinateurs.

La blockchain est avant tout un principe d'organisation de base de données. Il n'existe donc pas « la » blockchain : n'importe qui peut créer une chaîne, tout comme n'importe qui peut créer un fichier informatique.

Aujourd'hui, la technologie blockchain est principalement utilisée comme support à des cryptomonnaies (le Bitcoin par exemple). Des usages dans d'autres secteurs sont possibles, et les expérimentations sont nombreuses.
Illustration de la blockchain en une image :



« Source : Office parlementaire d'évaluation des choix scientifiques et technologiques,
Note scientifique n°4
"Comprendre les blockchains (chaînes de blocs)", avril 2018 ».

La cryptographie : la garantie de sécurité de la blockchain

Les blocs forment la base de la blockchain. Ils regroupent des informations homogènes et horodatées.

Dans le domaine financier, un bloc peut par exemple regrouper un ensemble de transactions ; dans le domaine logistique, un bloc peut archiver les points de passage d'une cargaison ou refléter l'historique d'un stock de produits…

Les blocs sont reliés entre eux chronologiquement, formant une chaîne. Des algorithmes de cryptographie (la « science des mots de passe ») assurent la sécurité de la chaîne. Ces algorithmes sont tellement complexes qu'ils sont impossibles à résoudre seul, même en disposant d'outils puissants de calculs.

Sur certaines blockchains, un système de récompenses indemnise les personnes qui participent à la recherche de solution. Ce n'est pas forcément nécessaire : les participants peuvent aussi avoir des motivations intrinsèques à réaliser ce travail de recherche (besoin de valider une transaction, intérêt à développer la confiance dans le système…).

Dès que la solution est trouvée et vérifiée, à l'image d'une signature, le bloc est ajouté à la chaîne. Les informations contenues dans le bloc acquièrent alors un caractère de vérité, permettant par exemple d'attester qu'un paiement a eu lieu.

Ce fonctionnement rend impossible toute modification de bloc : altérer une information passée invaliderait la signature du bloc modifié et celles de tous les blocs suivants. Le faussaire devrait alors calculer la bonne signature de tous ces blocs, ce qui est impossible à faire seul.

La blockchain n'a pas besoin d'une autorité de validation externe : elle porte en elle-même l'intégralité des données permettant d'attester qu'elle n'a pas été falsifiée, puisqu'il suffit de vérifier la signature du dernier bloc pour vérifier que l'intégralité de la chaîne est valide.

Les usages et applications de la blockchain

L'usage le plus emblématique de la technologie blockchain est le Bitcoin... si bien que l'on confond parfois les deux !

Le Bitcoin est une monnaie numérique (« crypto-monnaie ») qui utilise la technologie blockchain comme registre d'archivage des transactions et facteur de confiance : nul ne peut créer de faux Bitcoins.

Sur la blockchain du Bitcoin, les personnes qui tentent de valider les blocs sont appelées « mineurs ». L'expression provient de la récompense (un certain nombre de Bitcoins) offerte à chaque personne qui parvient à valider un bloc, en référence à un chercheur d'or dans une mine.

Le Bitcoin est loin d'être la seule crypto-monnaie en circulation : on en compte une centaine d'autres conçues sur le même principe. Cependant, rares sont celles réellement utilisées, l'enjeu n'étant pas la faisabilité technique mais l'adoption.

Petit à petit, les monnaies numériques gagnent en légitimité : l'Autorité des Marchés Financiers commence ainsi à réguler les prestataires du secteur établis en France, tandis que le réseau social Facebook a lancé l'initiative « Libra », destinée à créer une monnaie virtuelle concurrente au Bitcoin dont la valeur serait adossée sur des devises réelles (dollar, euro...).

Néanmoins, l'utilité et l'avenir de ces monnaies sont encore incertains, notamment compte tenu de la consommation d'énergie élevée nécessaire pour assurer la sécurité des blockchains publiques.

La technologie blockchain a d'autres usages que les monnaies virtuelles. L'inaltérabilité et l'absence de dépendance à un organisme centralisateur sont appréciées dans des domaines tels que la traçabilité alimentaire, la logistique, l'amélioration des services publics ou la tenue de cadastre.

Un exemple concret : en Suède, dans une démarche visant à éliminer le papier, l'organisme gérant la propriété foncière stocke désormais les informations dans une blockchain privée que peuvent interroger propriétaires, agences immobilières, notaires et banques. Ainsi, les personnes autorisées à accéder à la blockchain, souhaitant vendre ou acheter un logement, peuvent vérifier la transaction avec une garantie de sécurité, et personne ne peut la contester.