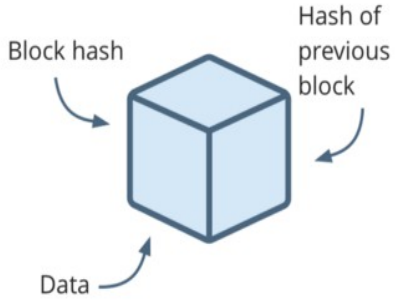
Vulgarisation de la « Blockchain »
A. Bourgeois – 4MP – 08/2019

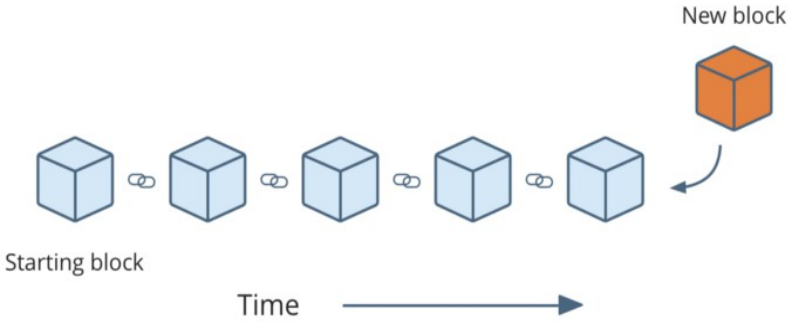
0- Introduction

La technologie blockchain est apparue dans le courant de l'année 2008, à priori en Asie de par le libellé de publication initial. Son code informatique étant « *libre* », c'est à dire exploitable par qui veut bien faire l'effort de le comprendre, elle s'est propagée à travers le monde très rapidement.
=> Son intérêt réside dans le fait qu'elle permette de réaliser des transactions horodatées, souvent anonymes et sans droits à l'entrée (blockchain appelée « *publique* »), sans « *tiers de confiance* » soit sans entité extérieure en contrôlant la validité. La blockchain étant décentralisée et 100% digitale, les contrôles sont en fait nativement intégrés à l'infrastructure technique et à son code informatique.

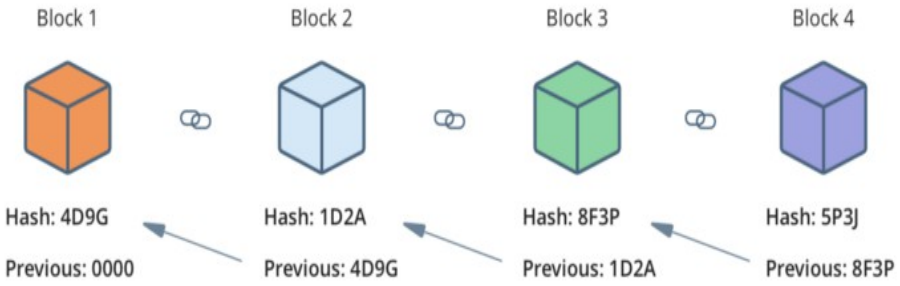
1- Le « block » et le « hash »



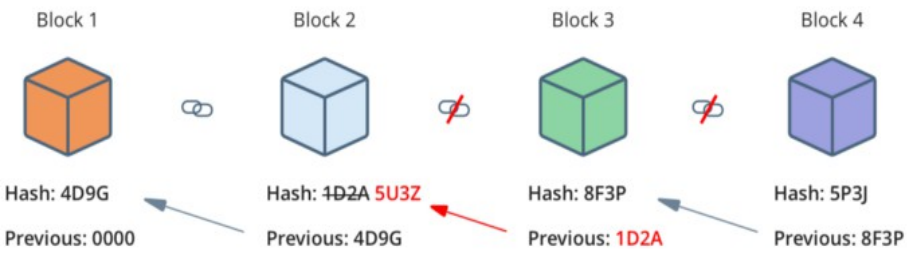
Les « datas » s'empilent dans le block au fur et à mesure que les transactions s'opèrent : les « *datas* » sont en fait les transactions. Chaque block génère en continu son propre « *hash* » mais possède aussi le « *hash* » du block créé précédemment. Le « *hash* » est l'élément sécuritaire de chacun des blocs : il s'agit d'une suite de chiffres et lettres calculée à partir des « *datas* » contenues dans le block. Le « *hash* » constitue une véritable « *empreinte numérique* » sécurisée et unique du block.



Quand le bloc atteint une certaine taille, les « *datas* » sont figées ainsi que le « *hash* », et un nouveau block se crée. C'est ce nouveau block qui empilent alors les nouvelles « datas », autrement dit les nouvelles transactions.



On obtient alors une « *chaîne de blocks* », d'où le nom « *blockchain* », les blocks étant reliés entre eux par le « *hash* » du block précédent et leur propre « *hash* » qu'ils vont léguer au block suivant.



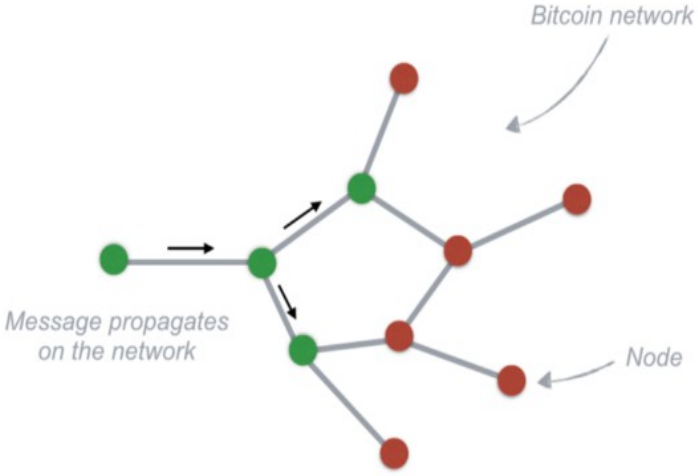
L'image ci-contre présente une blockchain qui aurait été corrompue : le « *hash* » partagé par 2 blocks qui se suivent n'est pas le même !

La manière dont les blocks sont validés, avec des notions de preuve de travail (proof of work) ou de preuve de participation (proof of stake) n'est pas abordée dans ce document, considérant que cela va au delà de la simple vulgarisation.

2- Le « réseau »

La blockchain, c'est aussi un réseau d'ordinateurs qui gèrent les transactions, et assurent nativement la sécurité de cet ensemble en exécutant le même code informatique. Chacun des ordinateurs, ou assimilés, sur le réseau est appelé un « *noeud* » (« *node* » en anglais).

=> C'est ainsi q'on parle souvent de « *registre mondial distribué* » dans la mesure où les datas sont réellement dispatchées en une multitude d'endroits sur le réseau, soit en une multitude de noeuds.



Chacun des nœuds du réseau reçoit progressivement les nouvelles transactions. L'empilement des transactions dans les blocks se fait donc sur chacun des nœuds comme vu précédemment. Ce n'est que lorsque l'ensemble des nœuds du réseau ont intégré une même transaction que celle-ci est parfaitement validée et sécurisée. Dans l'attente d'une validation par l'ensemble du réseau, la transaction n'est que partiellement sécurisée.

Sur le réseau « *bitcoin* » qui est la plus connue des utilisations de la blockchain (création et gestion d'une cryptomonnaie du même nom), on considère généralement qu'il faut 1 heure pour totalement sécuriser une transaction.

3- Utilisations potentielles

=> Outre la création de crypto-monnaies, désormais dénombrées à plus de 200 à travers le monde, on peut rencontrer les utilisations possibles suivantes portées par des acteurs très différents :

- dans les « *supply chain* » (chaînes d'approvisionnement) ce qui permettrait de suivre à la trace les marchandises de la production à la consommation,
- pour les « actifs d'entreprises » où les actions seraient représentées numériquement par des « *tokens* » (jetons), ceux-ci s'échangeant ensuite facilement et en toute sécurité,
- dans la banque où il deviendrait possible d'inscrire les actifs des clients (et autres éléments) dans une blockchain afin de réduire les coûts d'infrastructure bancaire,
- chez les notaires et d'autres professions réglementées où les actes traditionnels et les titres de propriété seraient remplacés par des « *smart contracts* » (contrats intelligents),
- au cadastre où les parcelles cadastrales et leurs évolutions seraient consignées au fur et à mesure du temps, dans les greffes des tribunaux de commerce pour les Kbis, etc …

=> On constate par ailleurs que de grosses sociétés (IBM, Microsoft, Amazon) propose désormais un service « *BaaS* » (Blockchain as a Service), en fait un service Cloud permettant aux utilisateurs de créer, d'héberger et d'utiliser leurs propres services ou applications blockchain. Proposition allant évidemment dans le sens d'une adoption de la blockchain par le plus grand nombre.

Remarque : ***Il n'y a pas « une blockchain » mais « des blockchains » !***

C'est ainsi que la « blockchain des services de paiement » développée par la société 4MP est une « blockchain privée », en partie centralisée du fait des procédures de KYC (Know Your Costumer) indispensables au plan réglementaire, ne provoquant aucune création du moindre « crypto-objet » tel que le bitcoin ou autre, ne reprenant pas -techniquement parlant- la structure des « blocks » en se contentant d'empiler les transactions signées grâce à des jeux de clefs privées et publiques.