Blockchain

Le nouveau marché de la confiance

Depuis la une « the economist » qui traite du sujet, le nombre d'articles sur la blockchain a littéralement explosé. Cette technologie est supposée transformer radicalement notre organisation économique et sociale. Aussi radicalement que l'a fait Internet…

Une blockchain permet de créer un **registre distribué** dont l'historique ne peut **pas être effacé**, sur lequel on peut **automatiser des mises à jour** et par lequel on peut **transférer de la valeur**.

Le caractère infalsifiable du **registre** ont permis à la start-up Blockpharma, d'utiliser la blockchain pour assurer la **traçabilité** des médicaments, elle permet également à Walmart de mettre en place un système de traçabilité des produits agricoles vendus dans ces magasins chinois

Le fait d'avoir un système de paiement **distribué** a permis par exemple à un smart-grid de Brooklyn de mettre en place un système d'achat et de revente d'énergie renouvelable entre particulier.

Une des principales utilisations à l'heure actuelle, restons honnête, c'est la **spéculation**. Il y a plusieurs plateformes (Kraken, coinhouse…) qui permettent d'échanger des monnaies « traditionnelles » contre des « cryptomonnaies ». Le nombre de Bitcoin, Ether ou autre étant limité, plus les gens vont acheter de ces cryptomonnaies, plus le cours augmente.

Les réflexions sur **l'identité digitale**, la cryptographie assymétrique, pourront server dans **l'internet des objets** pour éviter les problématiques d'attaques par usurpation d'identité, elles pourront servir également à la gestion de **droits d'auteur** ou au vote électronique.

Enfin la logique des **smart contracts**, des contrats prédéfinis et automatisés devraient amener des changements en profondeur dans notre manière d'appréhender le **droit des obligations.**

Si on regardait les choses un peu plus concrètement on ne devrait pas parler de « La » Blockchain mais des blockchains puisqu'il y en a plusieurs.

On peut citer par exemple la blockchain Bitcoin, la blockchain Ethereum et d'autres projets similaires comme les cryptomonnaies Dash, Monero etc.. Ces blockchains sont des **blockchain publiques**, c'est-à-dire qu'elles n'ont pas d'autorité centralisatrice.

En parallèle à ça il y a également des projets de **blockchains privées** qui ont été développés par des consortium d'entreprises comme Hyperledger, Ripple ou encore R3.

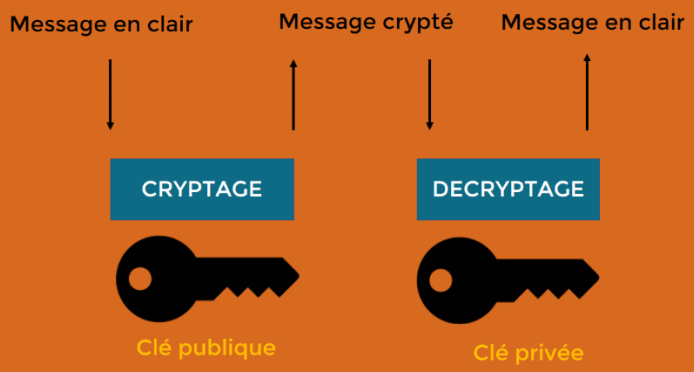
HYPERLEDGER

LE BITCOIN : COMPRENDRE LE PHENOMENE

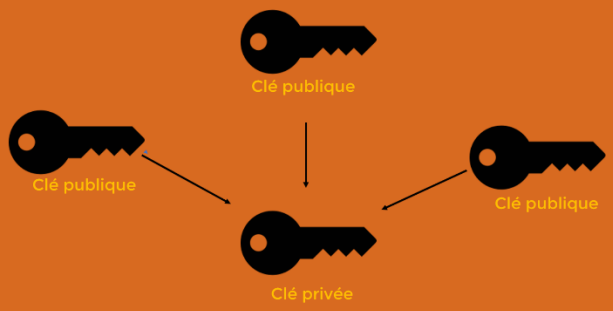
Pour bien comprendre leurs fonctionnement, il faut d'abord comprendre comment fonctionne la première d'entre elle, le Bitcoin.

Cette monnaie est née en 2009, juste après la crise. C'est un inconnu, caché derrière le pseudonyme de Satochi Nakamoto qui a inventé ce système sur la base de ce qui avait été fait avec « e-gold » (première tentative de monnaie électronique).

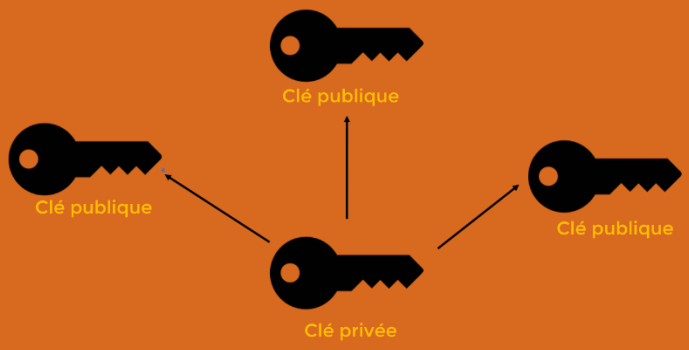
Un des intérêts du bitcoin c'est son système de cryptographie asymétrique qui repose sur des clés de chiffrement publiques et privées.



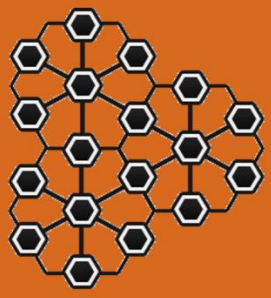
Habituellement dans un tel système, on utilise une clé publique qui est une clé de chiffrement et une clé privée qui est une clé de déchiffrement. Comme ça on a une identité connue de tous et on peut recevoir des messages qu'on est seul à comprendre. C'est le système qui a été mis en place par Wikileaks par exemple pour recevoir des informations.



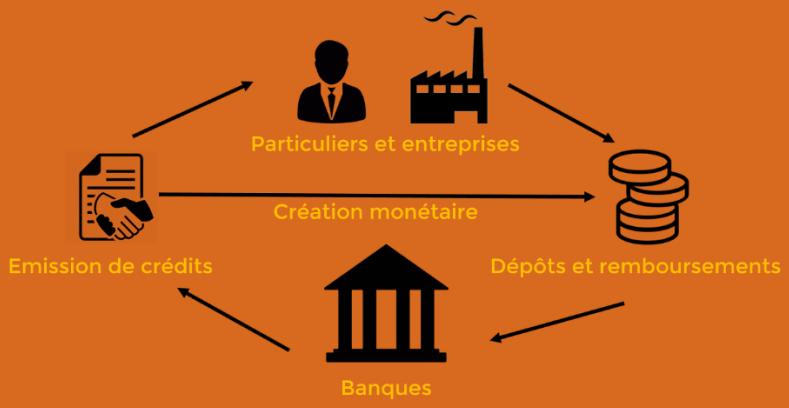
Le principe est inversé avec le Bitcoin. La clé de chiffrement est privée, du coup l'auteur d'une transaction est anonyme et la clé de déchiffrement est publique comme ça tout le monde peut être au courant qu'il y a eu une transaction et tout le monde peut potentiellement en vérifier l'intégrité (que la personne possède bien l'argent, que le message n'est pas altéré etc..).



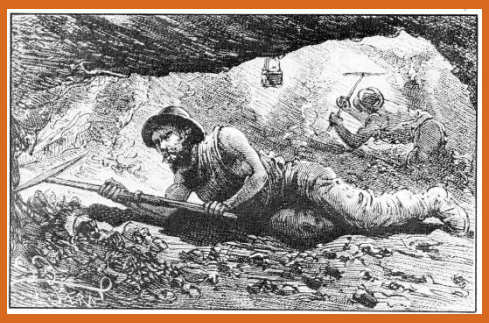
Du coup, là où dans un cadre « normal », les banques seules vont prendre la responsabilité de la fiabilité du système, le système du Bitcoin est un système qui peut être **« distribué »** où tous ceux qui le souhaitent peuvent voir les transactions.



Le Bitcoin cherche également à contester la place des banques dans le mécanisme de creation monétaire. Ce processus se fait par le crédit accordé par les banques aux particuliers et entreprises, sous le contrôle d'une Banque Centrale (qui favorise ou non l'émission de crédits par ces taux directeurs).



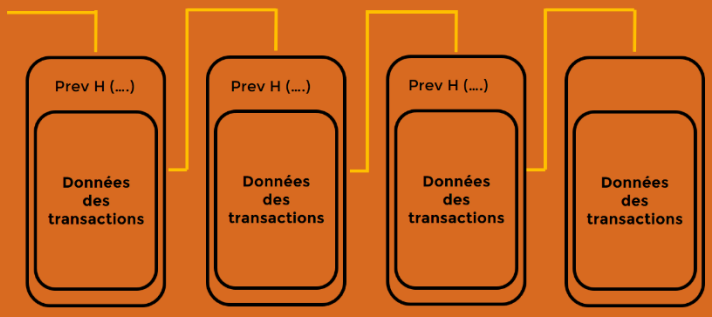
Par opposition à ce système qui laisse une trop grande importance aux institutions bancaires et qui est trop déconnecté de l'économie réelle, le système du Bitcoin a été construit pour retrouver l'esprit du système de l'étalon-or. Dans ce système la quantité de monnaie était liée à la réalité concrète de la quantité d'or disponible. L'augmentation de la masse monétaire ne pouvait donc se faire que lorsque les mineurs partaient chercher physiquement de l'or et permettaient d'augmenter la masse totale d'unité disponible.



Par analogie, ceux qu'on appelle, les **« mineurs »** dans le bitcoin, sont ceux qui vont permettre de sécuriser le système en vérifiant les nouvelles transactions avant de les intégrer dans le registre (dans ce qu'on appellee les full nodes pour être plus précis). Pour inciter les gens à le faire, malgré l'importante puissance de calcul que ça nécessite, les premiers mineurs à valider une transaction vont recevoir les nouveaux bitcoins fraichement créés.

Concrètement, ce travail de validation, qu'on appelle la preuve de travail (ou ***proof of work***) c'est le cœur de la « **blockchain** ».

Chaque bloc contient des informations sur les nouvelles transactions. Ces données passent par une fonction à sens unique (ou hash) pour donner un code de longueur fixe et ce code est repris dans le bloc suivant.



De cette manière, il devient impossible de modifier l'historique d'une chaine de bloc. Le moindre changement d'un tout petit bout de donnée dans un bloc provoquerait un grand changement sur toute la chaine et serait donc rapidement identifié.

Cette explication est volontairement simpliste, si vous souhaitez voir un peu plus en detail à quoi ressemble concrètement un bloc, vous pouvez le voir sur le site Block Explorer.

L'idée à retenir c'est donc qu'on a un **système distribué et sécurisé** et c'est ce qui fait l'intérêt de la technologie.

Petit bemol néanmoins, l'augmentation de la puissance de calcul necessaire pour effectuer le minage (notamment liée à l'explosion de la masse de données) devient tellement importante que des alliances se mettent en place pour réaliser les preuves de travail. Résultats, il y a une tendance à la concentration de la puissance de calcul par quelques associations de mineurs comme Antminer et Slushpool. A terme, cette situation laisse planer le risque d'une attaque dite des 51%. En effet, si un mineur dispose de plus de la moitié de la puissance de calcul il lui serait théoriquement possible de refuser de valider certaines transactions, valider les doubles dépenses voir même mener des attaques par dénis de service… bref de tuer la base de la blockchain : **la confiance**.

DU BITCOIN AUX BLOCKCHAINS PUBLIQUES

D'autres cryptomonnaies existent et elles permettent de corriger des imperfections du bitcoin ou de se spécialiser sur d'autres formes d'usages.

Parmis celles-ci on a Zcash, qui se fait un point d'honneur à protéger l'anonymat (et qui du coup aspire réellement l'argent de trafiquan ts en tout genre), Monero qui est assez bien optimisée pour la rentabilité des mineurs ou encore Litecoin, qui est un peu au Bitcoin ce que l'argent est à l'or...

ETHEREUM, L'AVENIR DES BLOCKCHAINS ?

Il y a un cas qui est particulièrement intéressant à mon sens, c'est **Ethereum**. Ce projet fonctionne sur la même base que le Bitcoin, avec un alliage de cryptographie et de systèmes distribués. Mais sa principale innovation c'est qu'il s'intéresse à une manière d'enregistrer **d'autres actifs** que la simple monnaie.

A l'origine d'Ethereum, il y a un projet, « Colored coin », qui voulait faire évoluer le Bitcoin dans ce sens. Mais le développeur **Vitalik Buterin**, qui travaillait dessus trouvait beaucoup trop de défauts au Bitcoin et il est donc parti fonder sa propre blockchain et a levé 18,4 millions pour son projet. C'était en 2014, il n'avait que 19 ans.

Le projet se construit dans un plan de développement de long terme qui se déroule en quatre étapes : **Frontier** (2015), **Homestead** (2016), **Metropolis** (2017) et **Serenity**. A chaque stade de développement correspond la mise en place de nouvelles avancées techniques.

Mais de manière plus pratique, la blockchain ethereum et l'ether, la cryptomonnaie qui va avec sont pensés pour être une blockchain à vocation généraliste, sur laquelle viennent se greffer différent type d'applications, c'est ce qu'on appel des **Dapps** (une abréviation pour dire applications décentralisées). Et plus spécifiquement, l'Ethereum est un environnement efficace pour mettre en place des **« smart contracts ».**
Ces « contrats intelligents » sont des programmes informatiques qui contrôlent directement l'usage de la monnaie en fonction de conditions prédéfinies à l'avance. Leurs applications peuvent être financières comme des actions, obligations, contrats d'assurance, produits dérivés, mais le fait de lier les smart contracts à l'internet des objets laisse imaginer d'innombrables applications.

Un autre intérêt de la blockchain Ethereum, c'est la facilité par laquelle peut se mettre en place un **ICO (initial coin offering).** Les ICO, ce sont des émission d'actifs numériques (les tokens) échangeables contre des cryptomonnaies durant la phase de démarrage d'un projet. Mais contrairement aux levées de fonds traditionnelles dont elles sont inspirées, les IPO (Initial Public Offering), ces actifs ne sont pas des parts au capital mais plutôt des **droits**, comme par exemple le droit d'usage d'un futur service. C'est vraiment une nouvelle manière d'envisager l'amorçage, beaucoup plus décentralisée que par les circuits traditionnels… et pour l'instant beaucoup moins régulée.

Les grandes entreprises travaillent beaucoup sur Ethereum, au sein de l'« Enterprise Ethereum Alliance » mis en place en février. On compte notamment les groups Intel, J.P. Morgan, BP, ING, Thomson Reuters, Accenture, BP, le Crédit Suisse, Cisco ou enfin MasterCard.

LES BLOCKCHAINS DE CONSORTIUM, LA CONFIANCE N'EXCLUT PAS LE CONTRÔLE

SI elles travaillent sur Ethereum, les grandes entreprises et les banques se penchent également sur des projets de blockchains privées dites blockchain de consortium ou « distributed ledger » dans lesquels **un nombre limité d'acteurs (voir un seul)** peut enregistrer des transactions ou disposer du registre. Contrairement aux cas que nous avons citées précédemment, ces technologies permettent d'identifier les différents protagonistes et donc de faciliter la gouvernance, notamment les audits.

Pour les « puristes », ces technologies cassent la raison même de l'existence des blockchains, c'est-à-dire la **suppression des intermédiaires bancaires**. Pour les banques c'est surtout un moyen de réduire drastiquement leurs coûts de transactions.

Parmis les exemples les plus notables de blockchains privées on compte celle du consortium R3, qui fonctionne sur la plateforme Corda. Elle regroupe près d'une centaine d'acteurs, notamment bancaires (parmis lesquelles Goldman Sachs, JP Morgan Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Royal Bank of Scotland, State Street, UBS, BNP Paribas, Société Générale et Natixis). Ces acteurs essayent de définir un standard d'utilisation de la technologie "Blockchain" dans le système financier global. **Cette blockchain interbancaire a pour but affiché de "remplacer" Swift**, le système d'échange interbancaire existant. Ce système permet donc de vérifier les transactions entre les banques et d'automatiser l'établissement du taux interbancaire.

Pour ce faire, elle se base sur la technologie du **contrat dit « ricardien »,** qui est une sorte de smart contract, mais dans lequel des tiers signataires au contrat interviennent pour suivre son exécution. Il permet d'avoir une action contractuelle normée mais automatisée.

Parmis les autres projets structurant de blockchain privée, il faut compter le projet **Hyperledger**. C'est une plateforme open source portée par la fondation Linux dans laquelle IBM, SAP, Fujitsu, GE, Hitachi, Huawei, SecureKey ou encore Airbus sont des membres très actifs.

Elle permet de donner une structure de base aux entreprises qui veulent créer une blockchain dans leur activité. Le framework **Hyperledger Fabric** donne des clés importantes pour le développement de projets. Hyperledger permet de développer des smart contracts (qui sont pour le coup appelés « chaincode ») et de gérer des transactions (Trafigura l'a par exemple utilisé pour ses transactions pétrolières). La différence avec les blockchains « traditionnelles », c'est que les participants sont des adhérents au système.

UNE ACTIVITE EN VOIE DE REGULATION

Ce qui se met en place en toute logique avec l'émergence de ces blockchains privée c'est la volonté d'une reprise en main du phénomène par les acteurs traditionnels. On parle des banques, mais les Etats aussi sont en ébullition sur cette question. C'est normal, les cryptomonnaies se substituent à un de leurs monopoles les plus ancrés alors même qu'elles sont encore des objets « alégaux » c'est-à-dire en dehors du champs de ce qui est régulé. **Ni légal, ni illégal**. Ainsi on assiste un peu partout dans le monde à deux tendances contradictoires mais concomitantes : La volonté d'encourager le développement de cette technologie d'avenir et une forte envie de la contrôler.

Ainsi les Etats Unis, le Mexique, Israel, le Vietnam et le Japon ont reconnu les cryptomonnaies comme des **moyens de paiement légaux**. Bercy a lancé une consultation pour un projet d'ordonnance visant à faire rentrer le concept de blockchain dans le droit national. L'Inde et Russie se dirigent également sur cette voie-là. De fait, une reflexion y est même engagée pour favoriser la création de cryptomonnaies nationales. Enfin, en termes de régulation, la **Chine** est particulièrement concernée puisqu'elle représente 70% du minage et une grande partie des détenteurs de cryptomonnaies. Cela s'explique par le faible cout de l'électricité des barrage et par la sous-évaluation chronique du yuan. Ainsi, elle propose un positionnement original. Pour endiguer les risques d'une explosion de bulle, les institutions bancaires n'ont pas le droit de posséder et d'échanger des cryptomonnaies. De même, les ICO ont été provisoirement interdites. En revanche les particuliers peuvent posséder des cryptomonnaies. Finalement seul l'Equateur et la Bolivie ont officiellement interdit la pratique.

Bref, la solution avance et quel que soit ce qu'on en pense, le phénomène est vraiment intéressant à observer. Certes la blockchain est une formidable réussite technique qui risque de transformer radicalement un bon nombre d'activités mais il convient néanmoins de rester prudent sur ce sujet.

Certaines blockchains comme Bitconnect ne sont ni plus ni moins que des pyramides de Ponzi, et certaines ICO amènent des levées de fonds en complète deconnexion avec la valeur intrinsèque des projets.