

BLOCKCHAINS

Janvier, 2018

Le document a été réalisé dans le cadre d'un projet d'étude par des étudiants de licence Miashs.

Réalisés par : Robin Couret, Justine Raynouard, Etienne Thomas
Tuteur.es : Daniel Bardou et Frédérique Brenet.

Notes des Auteurs

Nous avons réalisé ce document avec le double objectif d'acquérir des compétences de gestion de projet et de faire découvrir et vulgariser la blockchain. Cette technologie nous a fasciné et nous croyons qu'elle deviendra un des piliers de la révolution numérique. Nous ne sommes pas des experts sur le sujet, nous avons cependant trouvé intéressant de diffuser le résultat de nos recherches sur le sujet. Les sources utilisées, pour produire nos écrits, ne proviennent pas du domaine universitaire. Une partie importante d'entre-elles est issue de sites encyclopédiques et de médias, spécialisés dans la blockchain. En effet, le développement et la multiplication des blockchains se font dans un monde ouvert où les développeurs partagent leurs innovations, les ressources authentiques et techniques sont ainsi facilement accessibles.

Nous sommes des étudiants d'informatique, nous avons concentré nos efforts pour que nos explications soient accessibles au plus grand nombre. Il est cependant possible que certaines parties du document manquent d'éléments pour une compréhension juste. Des inexactitudes ou des raccourcis sont sûrement présents, ils peuvent provenir d'un souci de vulgarisation ou d'erreurs de notre part. Nous espérons que ce document vous facilitera la compréhension du sujet et qu'il aiguiseera votre curiosité.

Nous remercions particulièrement nos tuteurs pour leur patience et leur aide, ainsi que Maxime Beynet pour les réponses à nos questions.

Bonne lecture !

Etienne, Justine et Robin.

Sommaire

Introduction

I - Aspects Techniques ([P8](#))

- ❖ La blockchain, un fonctionnement en réseau ([P9](#))
- ❖ Le hachage ([P10](#))

Le Saviez-vous ? Paradoxe des anniversaires; Arbre de Merkle ([P12](#))

Pour aller plus loin... Le SHA-256 ([P13](#))

- ❖ Chiffrer l'information : la cryptographie asymétrique ([P15](#))
- ❖ Valider l'information ([P17](#))

Pour aller plus loin... Le minage du Bitcoin ([P20](#))

- ❖ Les problèmes techniques de la blockchain ([P21](#))

II - Cas d'usage ([P24](#))

- ❖ Blockchain “registre” simple ([P26](#))
 - Les Crypto-monnaies ([P27](#))

Pour aller plus loin ... Un fork : deux blockchains. ([P29](#))

- Traçabilité des aliments et des biens de consommation ([P30](#))
- Prêts entre particuliers ([P31](#))
- Gestion des certifications et documents légaux ([P32](#))

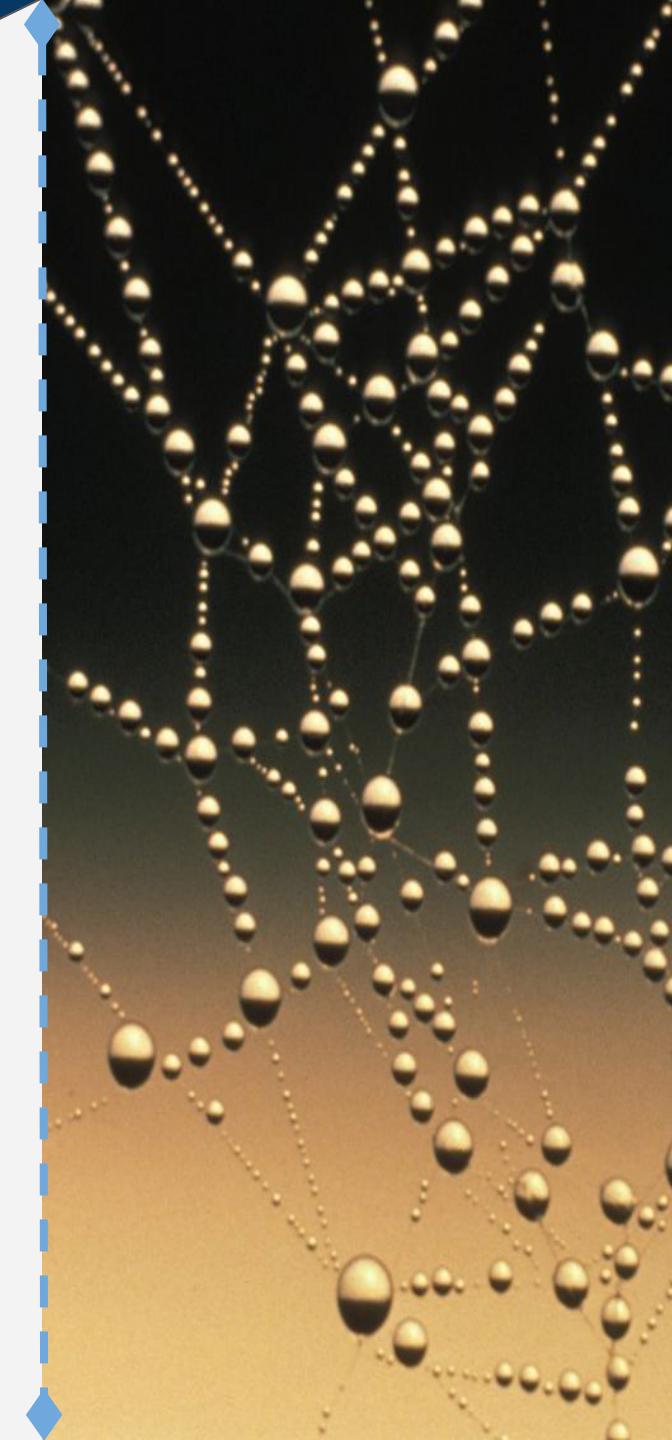
Sommaire

- ❖ Blockchain “programmable” ([P33](#))
 - Smart Contract ([P34](#))
 - Ethereum ([P35](#))
 - Les Organisations Autonomes Décentralisées ([P36](#))
 - La BitNation : Gouvernance Décentralisée ([P37](#))
Pour aller plus loin ... À propos de Gouvernance. ([P39](#))
 - Gestion des Énergies ([P40](#))
- III - Interview, la Blockchain pour les jeux vidéos ? ([P42](#))

Introduction

“The main advantage of blockchain technology is supposed to be that it's more secure, but new technologies are generally hard for people to trust, and this paradox don't really be avoid.”

Vitalik Buterin



Dans le milieu de la programmation réseau et web, la blockchain est une révolution, au même titre qu'internet. Internet est une révolution des communications, la blockchain, une révolution de la confiance.

Elle ouvre des possibilités infinies aux développeurs, qui cherchaient un moyen de sécuriser les données en ligne depuis des dizaines d'années. En effet, le Web avait permis de partager toutes sortes de contenus au monde entier mais le risque de modifications ou de falsifications par d'autres utilisateurs empêchait les développeurs de décentraliser le code ou même les décisions. De plus, les transferts d'argent étant visibles de tous, il fallait un organe de contrôle puissant pour assurer le bon déroulement des transactions. En bref, il est impossible de faire confiance aux utilisateurs. La blockchain est une réponse parfaite : personne n'a besoin d'avoir confiance dans les autres, il suffit d'avoir confiance dans le protocole. Ce protocole est le même pour tout le monde, n'importe qui peut en lire le code, aucun utilisateur ne peut nier s'être servi du protocole et une information écrite en amont ne peut plus être modifiée.

La blockchain n'est pas vraiment une nouvelle technologie mais plutôt un nouveau modèle de collaboration combinant plusieurs technologies (telles que le P2P, la cryptologie, les structures de données par chaîne de blocs, etc.) Celle-ci constitue, dans sa forme la plus simple, une base de données publique et distribuée permettant de réaliser des transactions informatiques entre tous les utilisateurs. La structure de cette technologie est développée en blocs successifs d'informations liés les uns aux autres. Tous les utilisateurs valident ensemble l'authenticité et la fiabilité des données. Ils doivent donc établir un consensus afin d'avoir à la fin un ensemble cohérent d'échanges valides.

Pour appréhender ce concept, il est nécessaire d'aborder les aspects techniques de cette blockchain (réseau, cryptographie, hachage, etc) mais aussi de voir certains domaines d'applications de ce protocole.

Aspects techniques

When asked to explain this space, I often ask people to forget pretty much everything you've heard about blockchains, crypto-currencies, and bitcoin, and instead dumb it down a lot and think about something no more complex or intimidating than good old-fashioned database technology.

Blythe Masters



La blockchain, un fonctionnement en réseau

La blockchain est une technologie **décentralisée** d'échange de données. Elle fonctionne en réseau distribué. Chaque utilisateur de la blockchain constitue un **nœud** et les informations transitent de nœud à nœud sans passer par un tiers de confiance. On parle alors de technologie **peer-to-peer** (P2P ou pair à pair en français).

La décentralisation du réseau possède l'avantage de ne requérir que peu de confiance entre les nœuds. Mais sans un organisme central garant de la validité et de la sécurité des échanges, le problème se pose de la fiabilité du système dans le cas de nœuds malveillants, altérés ou détruits. Il s'agit alors de trouver une solution pour assurer la sécurité et l'intégrité du réseau en présence de panne. Un problème mathématique expose clairement ce problème : on parle du **problème des généraux byzantins**. La blockchain est souvent considérée comme le premier algorithme à avoir réellement résolu le problème des généraux byzantins.

Un des moyens employés pour sécuriser le réseau est la duplication du registre. En effet, parmi les nœuds du réseau, il existe des nœuds complets et des nœuds partiels. Les nœuds complets possèdent une copie de l'ensemble des données enregistrées dans le registre tandis que les nœuds légers ne possèdent que les *headers* (*Voir article hachage*) des blocs anciens et les derniers blocs validés. Les nœuds légers peuvent ainsi faire des économies de mémoire tout en possédant la globalité des informations. Mais l'ensemble de ces nœuds validateurs sont tout de même en mesure à tout moment de vérifier la fiabilité du registre et assurent sa mise à jour permanente.

Ainsi, si certains nœuds sont corrompus ou détruits, le réseau est capable de remarquer qu'une partie de l'information est incorrecte et ignore les nœuds qui transmettent beaucoup de données inexactes. L'intégrité et la cohérence du registre sont ainsi préservées.

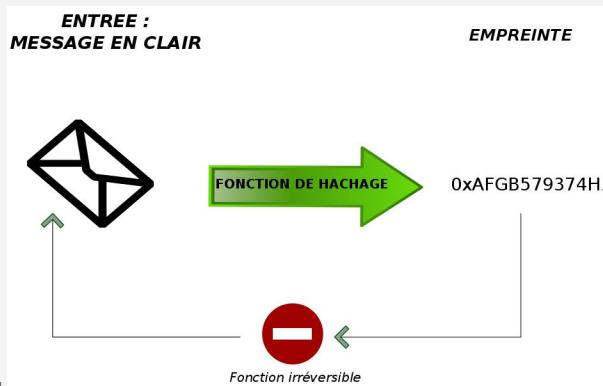
LE SAVIEZ VOUS ?

Le problème des généraux byzantins est un problème mathématique modélisant un réseau où la plupart des nœuds fonctionnent correctement mais quelques nœuds sont corrompus, c'est-à-dire qu'ils transmettent des messages erronés. On ne sait ni quels sont les nœuds défectueux, ni combien il y en a. Le but est d'arriver à ce que le réseau ne retienne que les données cohérentes et valides. Le problème des généraux byzantins met en scène cette question par une petite histoire : N généraux de l'armée byzantine

font le siège d'une cité ennemie, ces généraux communiquent à l'aide de messagers fiables pour se mettre d'accord sur un plan de bataille commun (se retirer ou attaquer). Mais certains de ces généraux sont des traîtres et sèment la confusion en diffusant des messages erronés. Les généraux doivent ainsi trouver un consensus afin que les généraux loyaux parviennent à se mettre d'accord sur le même plan d'action sans que les traîtres parviennent à interférer dans le choix des généraux loyaux.

Le hachage

Le hachage est une notion très importante utilisée par la blockchain. Voyons un peu de quoi il est question et comment cela fonctionne. Une fonction de hachage (ou *hash* en anglais) est une fonction permettant la transformation d'un message donné de longueur variable en une chaîne de caractères de longueur fixe (cette chaîne de sortie est appelé signature, empreinte, hash ou encore condensé). Les fonctions de hachage sont des fonctions irréversibles, c'est-à-dire qu'il est très difficile, voire impossible de retrouver le message de départ à partir de l'empreinte.



Le hachage a plusieurs fonctions. Tout d'abord, l'empreinte est généralement d'une longueur inférieure au message d'entrée mais contient tout de même exactement les mêmes informations. Le hachage assure donc un stockage optimisé : il permet de **compresser des données** sans perte d'informations. De plus, les signatures sont considérées comme uniques : chaque message d'entrée possède sa propre empreinte.

Ainsi si deux empreintes sont identiques, cela signifie que les messages d'entrée sont identiques. Le hachage permet donc de **comparer des données**. En outre, le fait que la signature désigne un fichier unique garantit la fidélité des données : toute modification du fichier initial, aussi minime soit-elle, entraînera un changement complet de la signature finale. Pour être sûr que les données d'entrée n'aient pas été modifiées, il suffit de vérifier que la signature des données est bien identique à celle attendue. Le hachage permet ainsi la **vérification des données**.

Un problème se pose lorsque des données placées en entrée produisent par hachage la même empreinte. On parle de **collision**. Les collisions peuvent devenir très gênantes car cela signifie que l'on peut falsifier les données d'entrée de telle façon qu'on obtienne la même empreinte : on ne peut donc plus assurer l'intégrité des données. Pour pallier à ce problème, les blockchains ont recours à des fonctions de hachage très puissantes avec de faibles taux de collisions. La solidité d'une fonction de hachage repose alors en partie sur l'impossibilité de trouver de tels conflits en un temps raisonnable. Pour prendre conscience de la complexité des fonctions de hachage utilisées par les blockchains, se référer au « Pour aller plus loin » traitant du SHA-256.

Afin de mieux quantifier cette résistance aux collisions, voyons ce qu'est le **paradoxe des anniversaires**. Ce concept demande combien de personnes doivent être réunies pour avoir une chance sur deux d'obtenir deux personnes avec la même date de naissance.

Pour répondre à la question posée par le paradoxe des anniversaires, l'intuition nous guide d'abord vers 183 personnes (la moitié des jours de l'année) puis pour les personnes au contact des probabilités vers un nombre inférieur mais tout de même assez élevé. La réponse est 23 : il ne faut que 23 personnes pour avoir une chance sur deux d'avoir deux personnes avec la même date d'anniversaire. De même, pour arriver à plus de 99% de chances d'obtenir ce résultat il ne nous faut que 57 personnes.[\(Voir Le Saviez-vous ?\)](#)

En hachage, la question du paradoxe des anniversaires devient : combien doit-on essayer de messages d'entrée avant de trouver la même empreinte avec une probabilité de 50% ? Par exemple, l'algorithme de hachage SHA256 détaillé plus loin, on a besoin de 2^{128} messages pour avoir une chance sur deux d'obtenir la même empreinte, ce qui correspond à peu près à 3,4 fois le nombre d'atomes estimé dans l'univers observable (10^{80}).

Le hachage est notamment utilisé pour lier les blocs entre eux : tout nouveau bloc possède une référence au bloc précédent qui lui-même possède une référence au bloc le précédent, etc. Toute modification ne serait-ce que d'un caractère d'un des blocs entraînerait donc une modification de tous les hashs des blocs suivants et serait donc facilement repérable; où la réputation d'infalsifiabilité de la blockchain.

La référence au bloc précédent est calculée de la façon suivante. Le message d'entrée de la fonction de hachage est constitué par le *header* du bloc précédent. Le header est l'en-tête d'un bloc et contient ses caractéristiques: sa version (son type et les règles suivies), son horodatage de création, la référence (*hash*) au bloc précédent, sa racine de l'arbre Merkle ([Voir Le Saviez-Vous ?](#)), la difficulté du bloc et un nonce. Le nonce est un nombre aléatoire permettant de donner le nombre de zéro précédent le hash demandé.

Le BitCoin utilise le hachage dans deux situations : pour obtenir le hash des blocs et pour créer les adresses bitcoin (on verra plus loin qu'on parle aussi de clé privée). Deux algorithmes de hachage sont utilisés pour le BitCoin : le SHA-256 et le RIPEMD-160.

Pour élaborer les adresses BitCoin, on calcule un SHA-256 suivi d'un RIPEMD-160.

Pour effectuer le hash des blocs, on utilise un double hash en SHA-256. Le hash final doit commencer par un nombre donné de 0. Plus il y a de 0, plus le hash est dur à trouver. Ainsi quand beaucoup de nœuds (= utilisateurs) tentent de calculer ce hash, il est possible d'augmenter la difficulté du calcul en demandant un hash précédé de beaucoup de 0 afin que le temps de résolution soit toujours égal à 10 min

Le Saviez-Vous ?

Paradoxe des anniversaires

Calculer la probabilité que deux personnes aient leur anniversaire le même jour est équivalent à calculer la probabilité que toutes les personnes réunies aient leur anniversaire un jour différent.

Pour une personne 365 dates sont possibles, donc pour N personnes 365^N dates. Mais tous les anniversaires doivent avoir une date différente. La première personne a donc 365 dates possibles, la seconde 364, la troisième 363, etc.

On a donc à calculer :

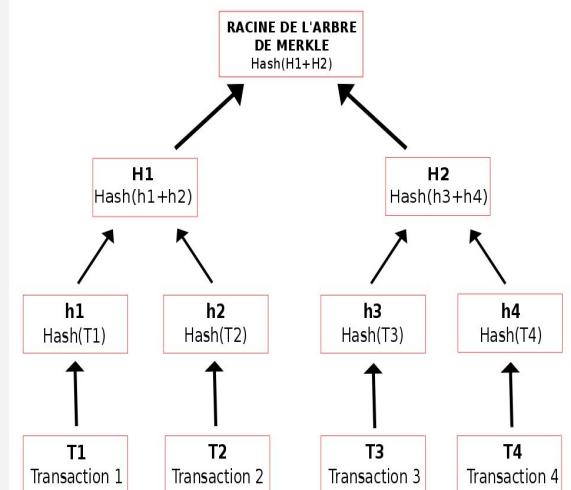
$$P = \frac{365!}{365^N \cdot (365-N)!}$$

Avec N = 23 personnes, on obtient $P = 0.49$, probabilité que les 23 personnes aient toutes des anniversaires à des dates différentes. Ainsi, la probabilité qu'au moins deux personnes soient nées le même jour est de $1-P = 0.51$, soit 51% de chance d'obtenir ce résultat.

L'arbre de Merkle

L'arbre de Merkle est un mécanisme de compression utilisé pour stocker et vérifier un grand volume de données efficacement et de manière sécurisée. Il se présente sous la forme d'un arbre binaire permettant de calculer une racine résumant toutes les données. Si une seule donnée est corrompue, la racine de l'arbre de Merkle est différente, l'existence d'une erreur est ainsi mise en évidence facilement. Pour identifier l'erreur, l'arbre de Merkle présente également une caractéristique intéressante : en plus de vérifier l'intégrité de l'intégralité des données, il est possible de tester la fiabilité d'une petite partie des données sans devoir nécessairement posséder tout le fichier. Cela présente un avantage non négligeable. Par exemple, sur le réseau Bitcoin, il existe des nœuds complets possédant et vérifiant continuellement l'intégralité de la blockchain mais il existe également des nœuds légers qui ne téléchargent que les *headers* des blocs mais peuvent tout de même vérifier les transactions grâce aux racines de l'arbre de Merkle.

Fonctionnement de l'arbre de Merkle : Imaginons que nous avons affaire à un bloc ne comportant que 4 transactions. La racine de son arbre de Merkle sera calculée comme suit :



Dans le cas du Bitcoin : $\text{Hash}(x) = \text{SHA256}(\text{SHA256}(x))$

Temps	10 minutes (comprend tout le processus de vérification)
Niveau de difficulté	Difficile : 2^{128} bits ¹
Ingrédients	<ul style="list-style-type: none"> - 1 message 2^{64} bits maximum : prenons M=« Bonjour » - 64 valeurs constantes de mots de 32 bits représentant les 32 premiers bits de la partie décimale des racines cubiques des 64 premiers nombres premiers. - 8 variables : $H_0^{(0)} = 0x6a09e667$; $H_1^{(0)} = 0xbb67ae85$; $H_2^{(0)} = 0x3c6ef372$; $H_3^{(0)} = 0xa54ff53a$; $H_4^{(0)} = 0x510e527f$; $H_5^{(0)} = 0x9b05688c$; $H_6^{(0)} = 0x1f83d9ab$; $H_7^{(0)} = 0x5be0cd19$
Ustensiles	<p>SHRⁿ(x) : décalage binaire à droite (x mot de 32 bits ; $0 \leq n \leq 32$)</p> <p>ROTRⁿ(x) : rotation binaire par la droite (x mot de 32 bits ; $0 \leq n \leq 32$)</p> <div style="background-color: #f0f0f0; padding: 10px;"> $Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$ $Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$ $\Sigma_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$ $\Sigma_1^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$ $\sigma_0^{\{256\}}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$ $\sigma_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$ </div>

Le SHA-256

Pour bien comprendre la complexité d'un algorithme de hachage et ainsi sa robustesse, voyons plus en détail l'algorithme de SHA-256 créé par la NSA (*National Security Agency*) en 2010. C'est un peu comme une recette de cuisine. Au début on a des ingrédients bruts (des données), on suit les étapes de la recette et à la fin on obtient un beau gâteau : un *hash* de 256 bits. Tout d'abord il faut commencer préparer le message initial afin qu'il soit exploitable, c'est un peu comme dans un gâteau à la noix de coco il faut d'abord ouvrir et râper la noix de coco avant de pouvoir l'utiliser dans la recette. Ici, il s'agit de remplir le message avec des bits (selon des règles qui nous verrons plus loin) afin qu'on puisse le découper en groupe de 512 bits (on verra plus loin pourquoi 512). Ensuite, vient la recette à proprement parler qui consiste à calculer le condensé de chaque groupe de 512 bits.

¹ résistance aux collisions

Préparation du message

1- Conversion du message initial M en binaire par la table ASCII

« Bonjour » -->

010000100110111101101110011010011011110111010101110010

2- Ajout d'un 1 à la fin de M

0100001001101111011011100110100110111101110101011100101

3- Ajout à la suite du 1 ajouté précédemment d'un nombre k de « 0 de bourrage » à calculer. Il y a 56 caractères dans

010000100110111101101110011010011011110111010101110010,

$$\Rightarrow \text{On pose : } l = 56$$

k se calcule de la façon suivante : $l + 1 + k = 448 \bmod 512$ où k est la plus petite solution non négative de l'équation .

$$\Rightarrow k = 391$$

\Rightarrow On ajoute à la fin de notre message 391 « 0 » de bourrage.

4- Ajout de 64 bits représentant l en binaire à la suite des 0 de bourrage

$l = 7$ (en décimal) = 111 (en binaire) = 0000...0000111 (en binaire sur 64 bits)
61 zéros

\Rightarrow On obtient bien un message de 512 bits : $56 + 1 + 391 + 64 = 512$

5- Découpage du message en 16 morceaux de 32 bits ($512 = 16 * 32$)

01000010011011110110111001101010

01101111011101010111001010000000

...

00000000000000000000000000000000111

Hachage du message

1- On calcule les valeurs de W

$$W_t = \begin{cases} M_t^{(i)}, & 0 \leq t \leq 15 \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16}, & 16 \leq t \leq 63 \end{cases}$$

2- On initialise a, b, c, d, e, f, g et h avec les valeurs de $H_i^{(0)}$

a= $H_0^{(0)} = 0x6a09e667$; b= $H_1^{(0)} = 0xbb67ae85$; c= $H_2^{(0)} = 0x3c6ef372$;
d= $H_3^{(0)} = 0xa54ff53a$; e= $H_4^{(0)} = 0x510e527f$; f= $H_5^{(0)} = 0x9b05688c$;
g= $H_6^{(0)} = 0x1f83d9ab$; h= $H_7^{(0)} = 0x5be0cd19$

3- On calcule pour t de 0 à 63

$$\left\{ \begin{array}{l} T_1 = h + \Sigma_1^{\{256\}}(e) + Ch(e, f, g) + K_t^{\{256\}} + W_t \\ T_2 = \Sigma_0^{\{256\}}(a) + Maj(a, b, c) \\ h = g \\ g = f \\ f = e \\ e = d + T_1 \\ d = c \\ c = b \\ b = a \\ a = T_1 + T_2 \end{array} \right. \quad \}$$

4- On calcule les valeurs de hachage intermédiaires:

$H_0^{(1)} = a + H_0^{(0)}$; $H_1^{(1)} = b + H_1^{(0)}$; $H_2^{(1)} = c + H_2^{(0)}$; $H_3^{(1)} = d + H_3^{(0)}$; $H_4^{(1)} = e + H_4^{(0)}$;
 $H_5^{(1)} = f + H_5^{(0)}$; $H_6^{(1)} = g + H_6^{(0)}$; $H_7^{(1)} = h + H_7^{(0)}$

5- On concatène les valeurs trouvées ci-dessus et on obtient le condensé de 256 bits du message « Bonjour »

$H_0^{(1)} || H_1^{(1)} || H_2^{(1)} || H_3^{(1)} || H_4^{(1)} || H_5^{(1)} || H_6^{(1)} || H_7^{(1)}$

Ici, nous n'avions qu'un groupe de 512 bits mais dans le cas où le message est l'ensemble des transactions contenu dans un bloc, on obtient de nombreux groupes de 512 bits. Il faut alors itérer les étapes détaillées plus haut pour tous les blocs.

Chiffrer l'information : la cryptographie asymétrique

La blockchain est considérée comme très sécurisée. Un des moyens de sécuriser le stockage et la transmission de données vient de l'emploi de la **cryptographie asymétrique**. La cryptographie est une science qui rend un message inintelligible à toute personne non concernée. Elle garantit la **confidentialité**, l'**authenticité** et l'**intégrité** des données. On la qualifie d'*asymétrique* en opposition à la cryptographie *symétrique* qui utilise une seule clé pour chiffrer et déchiffrer un message. En cryptographie asymétrique, on est en présence de deux clés : une **clé privée** et une **clé publique**.

En effet, pour effectuer un échange via la blockchain, il faut posséder ces deux clés : une privée et une publique. La clé privée est secrète et permet de prouver qu'on est l'auteur de l'échange et qu'on est bien en droit de le faire (par exemple dans le cas d'une transaction sur une blockchain financière, il faut posséder un fond suffisant), il ne faut donc jamais divulguer cette clé. La clé publique, quant à elle, est diffusée à tout le monde et permet de recevoir le fruit de l'échange. On verra plus loin exactement comment se déroule un échange. Voyons d'abord comment sont générées les clés à travers le protocole de génération de clés du Bitcoin.

Dans le système du Bitcoin, l'utilisateur a besoin d'une clé privée, d'une clé publique et d'une adresse Bitcoin. Ici, on voit apparaître en plus de ce qui a été vu précédemment une adresse. En fait, la clé publique et l'adresse Bitcoin remplissent la même fonction (recevoir les Bitcoins) mais ne désignent pas rigoureusement la même chose : l'adresse Bitcoin est une version plus courte et plus lisible de la clé publique.

Générer les clés et l'adresse se fait de manière successive et dépendante : on crée la clé privée qui sert de base pour créer la clé publique qui permet à son tour de créer l'adresse Bitcoin. La clé privée est un nombre choisi au hasard de 51 caractères commençant par 5. Une fois cette clé privée choisie, on utilise l'algorithme ECDSA (*Elliptic Curve Digital Signature Algorithm*) pour générer la clé publique : la clé publique est donc la multiplication de la clé privée par une courbe elliptique de formule donnée. L'avantage de cette opération est qu'une multiplication par courbe elliptique est une **fonction unique** : à partir de la clé publique, il est pratiquement impossible de trouver la clé privée. Pour calculer l'adresse Bitcoin, on part de la clé publique. On calcule le SHA-256 de la clé publique puis on calcule le RIPEMD-160 du SHA-256 de la clé publique et on obtient ainsi 34 caractères commençant par un 1 ou un 3 qui correspond à l'adresse Bitcoin. Encore une fois, l'avantage du passage par ces deux fonctions de hachage est que ce sont des **fonctions irréversibles**, avec uniquement l'adresse Bitcoin, on ne peut calculer la clé publique.

Pour bien visualiser comment se déroule un échange de données, prenons l'exemple d'Alice et Bob, deux personnages souvent utilisés pour expliquer la blockchain, voulant échanger des bitcoins en passant par la blockchain.

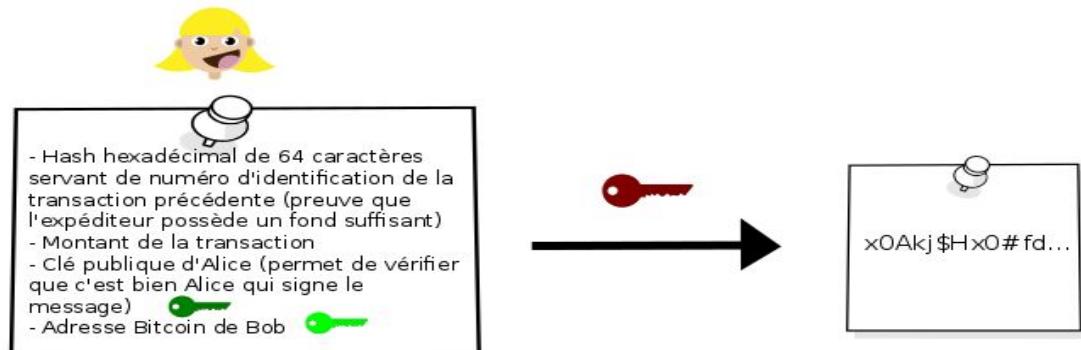
<https://www.ethereum-france.com/comprenre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-12/>

Bob et Alice ont chacun une clé privée et une clé publique.

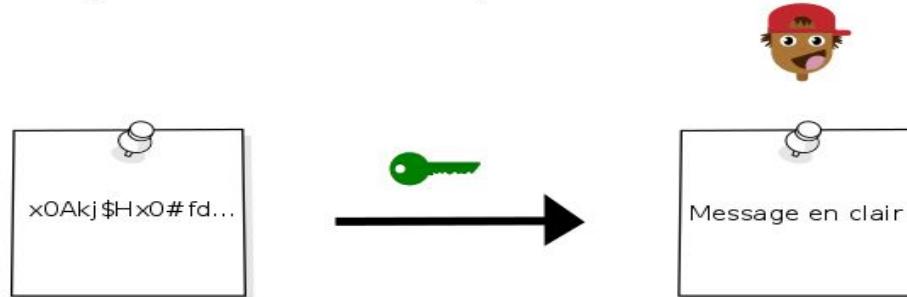


Alice veut envoyer de l'argent à Bob.

1- Alice crypte la transaction par sa clé privée: on dit qu'elle **signe** la transition.



2- Bob décrypte la transaction avec sa clé privée.



Valider l'information

Un des enjeux de la blockchain est de parvenir à garantir la **fiabilité** de l'information mise sur la blockchain, c'est-à-dire que l'auteur de cette information soit bien celui qu'il prétend être et qu'il est en droit de mettre cette information sur la blockchain (par exemple dans le cas d'une blockchain monétaire le donneur doit posséder la somme qu'il souhaite échanger pour pouvoir inscrire la transaction sur la blockchain, la blockchain ne tolérant pas le découvert). Il faut donc mettre en place un processus de validation sûr. C'est le rôle de certains nœuds du réseau qui vérifient, enregistrent et sécurisent le réseau.

Ces nœuds du réseau valident ensemble les données de manière distribuée. Ils doivent donc établir un **consensus** (accord unanime au sein d'un groupe permettant de se mettre d'accord sur la validité d'une information sans vote préalable ou délibération particulière) afin d'avoir à la fin un ensemble cohérent de données confirmées comme fiables. Il existe deux principaux consensus : la **proof-of-work** (preuve de travail en français) et la **proof-of-stake** (preuve de participation ou d'enjeu en français).

La proof-of-work (souvent abrégée Pow) fait intervenir le concept de **minage** : un protocole de consensus distribué et décentralisé utilisant la **puissance de calcul** de certains nœuds du réseau.

Ces utilisateurs sont appelés les **mineurs**. Les mineurs effectuent tout un processus de vérification des informations ajoutées à la blockchain qui se conclut par la recherche d'une solution d'un calcul très complexe.

Lorsqu'une information est ajoutée à la blockchain, elle est diffusée de nœud en nœud à la totalité du réseau. En attendant d'avoir un nombre d'informations validées suffisant pour former un bloc, un mineur regroupe les informations qu'il reçoit en un bloc provisoire en attente d'être validé. Quand le mineur reçoit une nouvelle information à valider, il l'ajoute donc à ce bloc provisoire et commence le processus de vérification. Tout d'abord, il vérifie que c'est bien l'expéditeur qui a signé l'information. Pour cela, il utilise la clé publique incluse dans le message pour le déchiffrer : s'il parvient à déchiffrer à l'aide de la clé publique de l'expéditeur le message signé par la clé privée de l'expéditeur alors cela confirme l'identité de l'expéditeur. Ensuite, il vérifie que l'expéditeur est bien en droit de déposer cette information sur la blockchain. Dans le cas d'une crypto-monnaie, le mineur doit remonter l'historique des transactions de l'expéditeur afin de vérifier qu'il possède bien l'argent qu'il souhaite dépenser et qu'il ne l'ait pas déjà dépenser ailleurs (problème des doubles dépenses). Si ces deux critères (identité de l'expéditeur et droit à déposer l'information) sont vérifiés, l'information est alors considérée comme valide. Une fois un certain nombre d'informations validées, il faut ensuite valider le bloc qui les contient.

Pour valider le bloc, les mineurs tentent de calculer le hash du bloc correspondant à un niveau de difficulté donné. Ils doivent trouver le nombre qui, ajouté à l'ensemble des caractères du bloc, donne par hachage un hash valide. La seule manière d'obtenir un hash valide est donc de calculer ce hash par itinération du nonce jusqu'à obtenir un hash correspondant au niveau de difficulté demandé. En effet, rappelons que le hash d'un bloc se calcule grâce à des fonctions irréversibles comme par exemple l'algorithme du SHA-256 dans le cas du Bitcoin ([Voir Pour aller plus loin: SHA-256](#)) : il est donc impossible de trouver le nonce à partir d'un hash avec le nombre de 0 correspondant.

En fait, un hash valide se doit d'être inférieur à un certain seuil donné que définit la difficulté comme nous allons l'expliquer. Un hash étant composé de 64 caractères, sa valeur est donc majorée par. Le seuil fixe une limite inférieure afin qu'un bloc soit généré selon un intervalle de temps donné entre la création de deux blocs (il est de 10 minutes dans le cas du Bitcoin). Le niveau de difficulté du hash est régulièrement adapté au nombre de nœuds et à la puissance de calcul mise à disposition afin que cet intervalle de temps soit maintenu. Par exemple, si on place un seuil à 1658, l'ordinateur devra calculer des hash en incrémentant le nonce à chaque échec, jusqu'à en trouver un inférieur à 1658, c'est-à-dire qui commence par 000000 (64-58=6 zéros). Ainsi, plus le seuil est bas, plus le nombre de 0 requis en début de hash est important et plus le niveau de difficulté du hash est élevé. Une fois le hash du bloc trouvé, il est ajouté à la blockchain et tous les nœuds du réseau possédant l'historique de la blockchain le reçoivent. Ces nœuds peuvent ensuite vérifier

la validité du bloc en vérifiant la validité de la preuve de travail. En effet, bien que trouver le hash soit un problème relativement dur à résoudre, vérifier son exactitude est assez facile.

Ainsi, pour chaque création de nouveau bloc, des milliers de nœuds lancent des calculs mais un seul trouve la solution qui la valide. Ils sont ensuite rémunérés au prorata de la puissance de calcul qu'ils apportent au réseau. Par exemple, sur Bitcoin, les mineurs étaient rémunérés par 50 bitcoins par bloc validé puis ce nombre est divisé par deux tous les quatre ans : les mineurs sont donc rémunérés actuellement par 25 bitcoins. Pour l'instant, il n'existe aucune véritable blockchain qui ne fonctionne sans incitation économique à sécuriser le réseau.

La proof-of-stake (souvent abrégée PoS) fait intervenir le concept de **minting** (= forgeage) : un protocole de consensus distribué et décentralisé demandant aux nœuds voulant valider des blocs de prouver la propriété d'un certain montant de crypto-monnaie. Ces nœuds sont appelés des **forgeurs**.

Pour pouvoir valider un bloc, un forgeur doit mettre en dépôt ses actifs pendant le temps de minting. L'algorithme de proof-of-stake sélectionne ensuite aléatoirement un forgeur : l'aléa étant pondéré par le montant total mis en dépôt. Par exemple un forgeur ayant déposé 100 tokens aura dix fois plus de chances d'être choisi qu'un forgeur avec 10 tokens en dépôt. Le forgeur sélectionné a ensuite un temps déterminé pour créer le prochain bloc à partir des échanges qu'il a validé. S'il ne crée pas de bloc pendant le temps imparti, l'algorithme sélectionne un autre forgeur.



www.crypto-france.com

Proof of work

VS



www.iconfinder.com

Proof of stake

Que ce soit par l'algorithme de proof-of-work ou par celui de proof-of-stake, il se peut que deux blocs soient créés et ajoutés à la blockchain en même temps. À partir de là, la blockchain part en deux branches. Au bout de quelques blocs, la chaîne la plus longue est considérée par défaut comme la chaîne valide. Ce principe permet de conserver la cohérence et la continuité globale de la blockchain.

Les consensus de PoS et PoW posent cependant certains problèmes notamment de rapidité et de centralisation. D'autres systèmes de consensus ont alors été développés. Par exemple, un autre consensus intéressant est celui du Peercoin. Cette crypto-monnaie utilise un système de preuve de travail **et** de preuve d'enjeu : l'algorithme adapte le niveau de difficulté du hash à calculer en fonction de la quantité d'actifs déposés.

De même, EOS (une blockchain destinée au développement d'applications décentralisées) utilise une *delegated proof of stake* (DPoS). Le principe est que les utilisateurs **délèguent** leur participation à des délégués rémunérés pour valider les échanges et les ajouter dans des blocs : plus un utilisateur détient un intérêt dans le réseau, plus son vote pour un délégué pèse lourd.

Le minage de Bitcoin

Durant les premières années de Bitcoin (le processus a commencé en 2009), le minage pouvait être réalisé par toute personne possédant un ordinateur. Pour miner, il suffit d'installer le logiciel adéquat et de connecter son ordinateur au réseau. Le logiciel calcule le hachage en exécutant des opérations sur le CPU. Toutes les dix minutes un bloc est miné, l'ordinateur qui résout le problème mathématique remporte alors une somme de 12,5 bitcoins (celle-ci évolue avec le temps). Il n'est aujourd'hui plus rentable de miner du bitcoin pour un particulier. Du fait de la popularisation du bitcoin et de sa valeur d'échange en euro montante, une véritable industrie est apparue autour du minage. Des ordinateurs spéciaux appelés ASIC sont dédiés au minage de bitcoins et des centres où des centaines d'ASIC ont été mis en place par des entreprises privées.

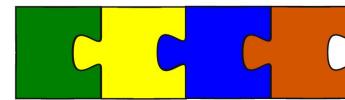
La concurrence entre mineurs sécurise le réseau, il faudrait posséder plus de 51% du réseau Bitcoin pour falsifier des transactions. Cependant, plus il y a de mineurs plus la consommation d'énergie augmente. Cela devient un vrai problème écologique sur la blockchain Bitcoin. En effet aujourd'hui (novembre 2017), il est estimé que le minage de bitcoin représente 23,07 terawatt/hours ce qui correspond à la consommation en énergie de l'Equateur. Ces chiffres sont sujets de controverses entre la communauté bitcoin et les médias populaires. Des solutions de validation drastiquement moins énergivores sont cependant proposées sur d'autres blockchains, par exemple le proof of stake.

Problèmes techniques de la blockchain

La blockchain doit tout de même faire face à certains problèmes.

Tout d'abord, un des défis à relever est celui de la scalabilité de la blockchain. Ce terme désigne la faculté d'un système à s'adapter à un changement d'échelle, c'est-à-dire de conserver ses fonctionnalités et ses performances même en cas de forte demande. La technologie de la blockchain gagnant de plus en plus de succès, la quantité d'informations stockées est de plus en plus importante mais ne peut s'augmenter infiniment et cela commence à devenir problématique sur certaines blockchains. De même, la blockchain se trouve de plus en

plus confrontée à des problèmes de rapidité de validation de l'information. Ainsi sur Bitcoin la limite est de 3 à 5 transactions secondes et sur Ethereum de 15 à 25 contre plus de 2500 transactions par seconde dans le système interbancaire Visa.



LE SAVIEZ VOUS ?

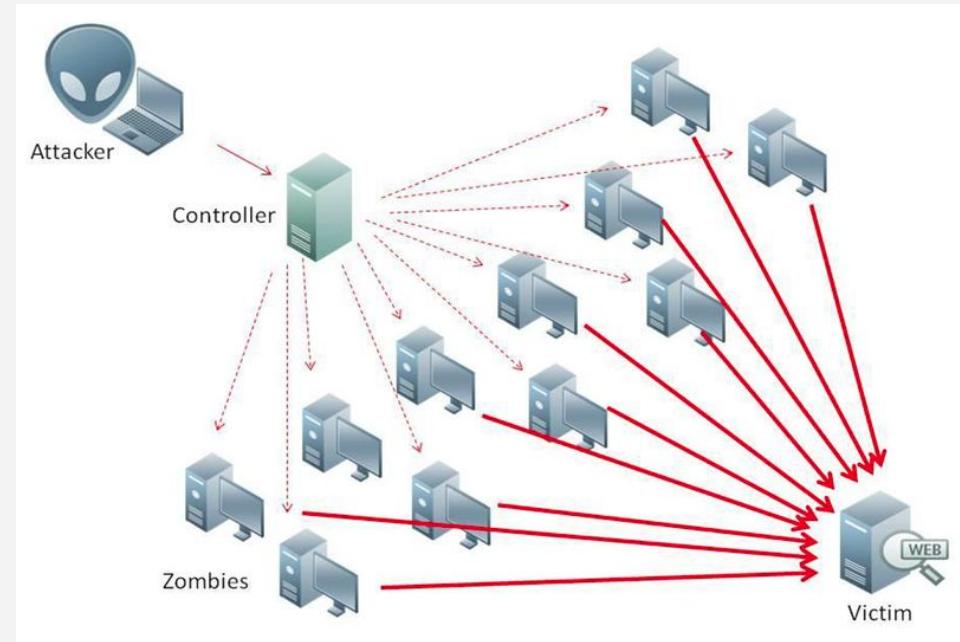
Avant l'année 2017, les blockchains avaient une popularité plutôt faible. Ainsi le nombre de transactions par jour a presque doublé en un an, pour atteindre presque ½ millions certains jours en fin d'année (on parle ici de Bitcoin). Il s'est fait alors ressentir un ralentissement sur le réseau : une transaction pouvait durer près de 24H. Ce problème est répandu sur l'ensemble des blockchains publiques et

représente à ce jour un réel défi pour les développeurs. Pour répondre à ce problème plusieurs solutions sont proposées. La plus répandue, encore en développement, est le lightning network, cela correspond à créer une blockchain (ou sur-couche) pour un nombre limité d'utilisateurs. Ces derniers pourraient échanger entre eux dans ce canal, puis celui-ci se connectera à la blockchain principale. D'autres solutions sont proposées comme par exemple changer la nature de la preuve de travail.

La blockchain peut également être victime de diverses attaques à différents niveaux. Tout d'abord, au niveau des clés, nous avons vu que l'attaque des anniversaires était pratiquement impossible à mener dans un temps raisonnable.

L'attaque par déni de service distribué (DDoS) est également une attaque qui vise régulièrement la blockchain. Le principe de cette attaque est de submerger le réseau sous un grand nombre de requêtes afin de rendre les services indisponibles pour les utilisateurs légitimes.

Pour s'emparer d'une blockchain et ainsi inscrire des informations erronées (double dépenses, etc.), une autre attaque très connue est l'**attaque des 51%** ou *goldfinger*. Cette attaque consiste à obtenir 51% du pouvoir de décision de l'ensemble du réseau : ainsi dans une blockchain avec une consensus de proof-of-work, il faudrait posséder au moins 51% de la puissance de calcul de l'ensemble des nœuds du réseau tandis qu'avec un consensus de proof-of-stake, il faudrait réunir au moins 51% de la masse monétaire totale de la blockchain. Le coût d'une telle attaque est donc très élevée (matériel informatique, tokens) et ne reste accessible que pour des États ou des organismes très puissants. Dans le cas d'un consensus de proof-of-stake, le risque d'une telle attaque est minime car il serait paradoxal pour un utilisateur possédant une importante quantité de tokens d'une certaine crypto-monnaie de vouloir mener une attaque en vue de faire chuter la valeur de cette crypto-monnaie.



Attaque DDos

Lexique :

- **Attaque des 51%**: attaque qui consiste à obtenir 51% du pouvoir de décision de l'ensemble du réseau
- **Bloc**: ensemble d'informations
- **Clé privée**: clé secrète permettant de prouver qu'on est l'auteur de l'information déposé sur la blockchain et qu'on est bien en droit de le faire. [P32](#)
- **Clé publique**: clé diffusée à tout le monde permettant d'accéder à l'information qu'on est en droit de recevoir. [P34](#)
- **Consensus** : accord unanime au sein d'un groupe permettant de se mettre d'accord sur la validité d'une information sans vote préalable ou délibération particulière. [P25](#) , [P26](#) , [P39](#)
- **Hachage**: transformation d'un message donné de longueur variable en une chaîne de caractères de longueur fixe afin de compresser des informations sans perte, de comparer et de vérifier des données. [P25](#), [P32](#)
- **Minage/Proof of work**: protocole de consensus distribué et décentralisé utilisant la puissance de calcul de certains nœuds du réseau (mineurs) pour valider l'information. [P21](#), [P27](#) , [P29](#) , [P35](#)
- **Noeud** : nom donné à la machine et au logiciel dans un réseaux pair à pair. Chaque utilisateur de la blockchain constitue un nœud. [P25](#)
- **Proof-of-Stake**: protocole de consensus distribué et décentralisé demandant aux nœuds voulant valider des blocs (forgeurs) de prouver la propriété d'un certain montant de crypto-monnaie.
- **Scalabilité**: faculté d'un système à s'adapter à un changement d'échelle, c'est-à-dire à conserver ses fonctionnalités et ses performances même en cas de forte demande.[P29](#), [P35](#) , P39
- **SHA-256**: Algorithme de hachage utilisé notamment par la blockchain Bitcoin. <https://csrc.nist.gov/csrc/media/publications/fips/180/4/final/documents/fips180-4-draft-aug2014.pdf>

Note : Vous pouvez retrouver votre page d'accès grâce aux liens.

Cas d'usage

“ I've been in a room in Silicon Valley where on the wall they have 160 industries they think blockchain can disrupt. We picked six of them to focus on.

Patrick M. Byrne



La blockchain, ce système technologique associant techniques de réseau, cryptographie et consensus distribués, permet un large champ d'applications. Les premiers cas d'usages de la blockchain sont tournés vers les monnaies décentralisées, cependant d'après de nombreux experts l'avenir des blockchains ne réside pas seulement dans les technologies de la finance.

En effet, si la blockchain Bitcoin se limite à l'enregistrement de transactions financières, on peut par exemple établir une blockchain stockant d'autres types d'informations datées et signées : des diplômes, des consommations d'énergies, des traçages de produits, etc. On appellera cela une blockchain de registre simple, dans le sens où elle sert de support d'enregistrement de différentes données.

Mais pourquoi se limiter au stockage de l'information ? Pourquoi limiter la blockchain à sa dimension de registre lorsque l'informatique et les technologies de l'internet ("peer to peer", internet des objets, etc.) demandent l'exécution de protocoles toujours plus complexes ? Grâce aux blockchains dites programmables, on peut voir se dessiner la silhouette d'un monde entièrement décentralisé, où la confiance entre les pairs ne serait plus garantie par une seule et même entité mais par un programme dont le code serait ouvert à tous.

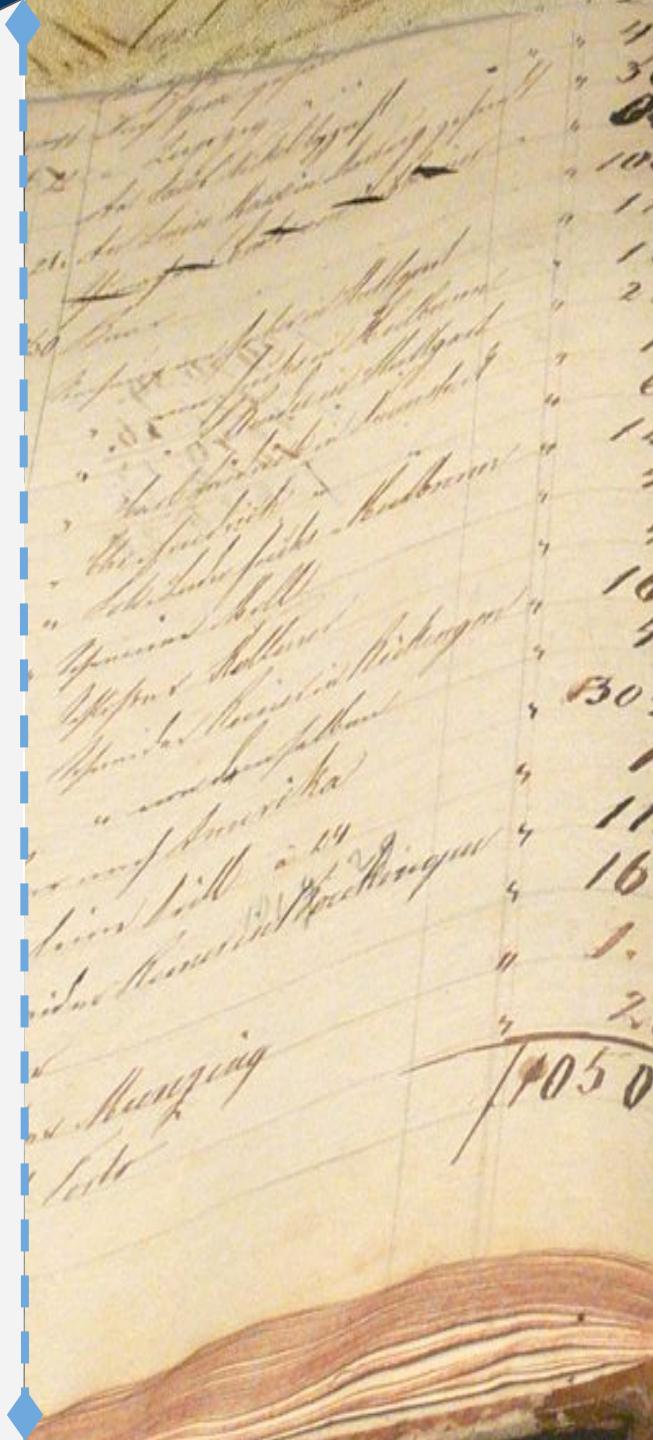
C'est sur cette catégorisation, basée sur la nature et la structure des informations contenues dans la blockchain que nous axerons les parties du dernier dossier de ce document. Nous verrons donc les cas d'usage de la blockchain avec premièrement des protocoles blockchain (dit "de registre") en prenant le cas Bitcoin puis nous traiterons plus en profondeur le cas des "blockchains programmables" en prenant le cas d'Ethereum.



Blockchain “Registre”

Par blockchains registres nous appelons toutes blockchains qui ne permettent pas l'exécution de programmes; c'est-à-dire les blockchains classiques, telle que peut l'être la blockchain Bitcoin, qui ne sont utilisées que pour le stockage d'informations de manière sécurisée et décentralisée.

En effet, grâce à la blockchain, c'est la première fois qu'un réseau décentralisé est plus sûr qu'un réseau centralisé. En fait, ici, la blockchain agit comme un tiers de confiance, une personne morale qui validerait les informations à la place d'une banque, d'un état ou même d'un organisme de contrôle. La validation de l'information est faite de façon protocolaire par un consensus partagé. Ces registres décentralisés, entièrement autonomes permettraient de désintermédier des pans entiers de l'économie et de la société. Voici quelques exemples de domaines qui pourraient adopter une solution blockchain dans les prochaines années.



Les crypto-monnaies décentralisées

Le concept de blockchain naquit avec l'invention du bitcoin, la première blockchain "registre". En 2008, un mystérieux inconnu publie un [livre blanc](#). Une multitude de projets de crypto-monnaies est apparue par la suite avec des visions alternatives au bitcoin et des technologies variantes. Certaines monnaies sont développées pour un usage anonyme (exemple : Monero, Verge), d'autres se démarquent par l'utilisation de techniques spécifiques (Proof stake, minage par GPU, etc.). La philosophie d'une monnaie dépend principalement de son équipe de développement : une entreprise privée n'aura pas les mêmes intérêts qu'une équipe de chercheurs ou que d'un groupe de développeurs indépendants.

Ces monnaies s'échangent sur des places de marché privé, ce sont des sites où les utilisateurs peuvent placer des ordres d'achat ou de vente sur les monnaies. Les échanges se font généralement en bitcoins vers une monnaie, ou d'une monnaie vers des bitcoins. Certaines places d'échange permettent d'acheter les monnaies les plus populaires avec des fiats (Euro, US Dollar, etc.). Les sites d'échanges les plus notables sont Bitfinex, Kraken, Coinbase Binance ou encore bitrex. De nouvelles solutions de places d'échanges décentralisées sont en train d'être développées. Aucune entreprise ou individu n'aura alors de responsabilité sur les échanges.

EXEMPLES



Litecoin, le petit frère de bitcoin.



Monero, une devise pour les transactions anonymes.



Verge, propose des transactions rapides et l'intégration de Tor.



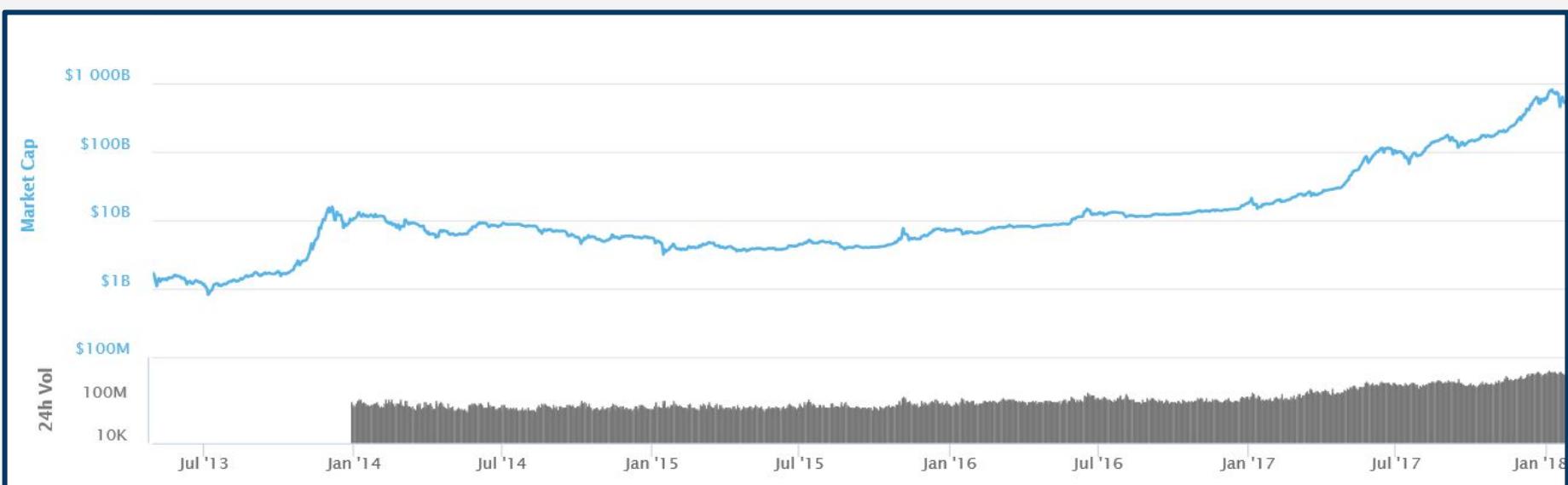
Tether, Une crypto-monnaie qui représente les monnaies fiduciaires, chaque Tether est soutenue par 1 USD

La plupart des monnaies ont un nombre d'unités fini connu à l'avance et créé durant les processus de validation ([proof of work ou proof of stake](#)). Cela entraîne un modèle de monnaie déflationniste, c'est-à-dire que le nombre de biens pouvant être acheté avec une unité de monnaie augmente avec le temps. C'est l'inverse des monnaies fiats qui sont inflationnistes. Les crypto-monnaies sont aujourd'hui peu utilisées comme monnaies pour acheter des biens, mais plus comme actif financier, ou comme outil de spéculation. Différents services et vendeurs permettent l'utilisation du bitcoin, les autres monnaies n'ont pas encore (ou très peu) un usage commercial.

Retrouvez comment dépenser des bitcoins :

<https://bitcoin.fr/depenser-ses-bitcoins>

Généralement, la classification des monnaies se fait en fonction de leur capitalisation dans le marché, c'est-à-dire le nombre d'unités de monnaie multiplié par la valeur d'échange de l'unité. Vous pouvez retrouver une classification sur <https://coinmarketcap.com/>. Ce marqueur permet d'étudier l'évolution du marché. En 2009 le bitcoin apparaît. Son évolution est faible pendant plusieurs années. En 2013, d'autres monnaies basées sur la blockchain voient le jour. Depuis la capitalisation totale n'a cessé d'augmenter de manière exponentielle :



Evolution de l'ensemble des marchés
<https://coinmarketcap.com/> (échelle logarithmique)

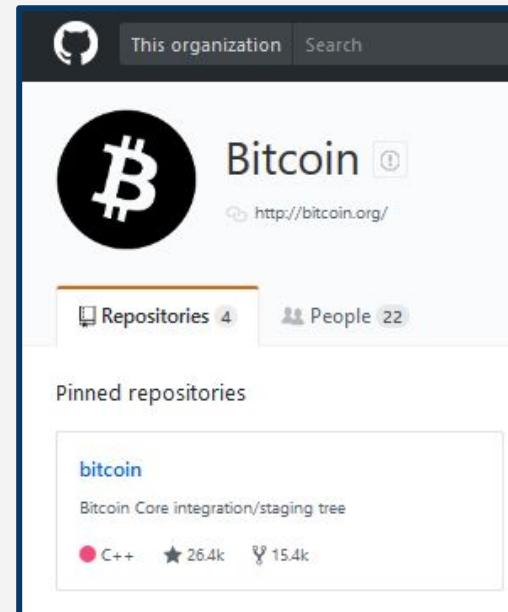
Un fork : deux blockchains

Pour aller plus loin...

La majorité des projets blockchain est développée de manière open-source, la gestion de projet se fait alors sur des logiciels de versionning tel que github. Ces logiciels sont conçus de manière à ce que plusieurs versions du logiciel soient développées en parallèle, ensuite la communauté choisit la nouvelle version à adopter. Quand la nature d'une version fait débat il est possible que la communauté ne se mette pas d'accord sur laquelle choisir, dans ce cas le projet peut se scinder en deux, on appelle cela un fork.

Le bitcoin, par exemple, a connu différents forks dans son évolution, le plus marquant est celui du bitcoin cash au courant de l'été 2017. Le débat était alors de choisir la taille des blocs en Mo pour résoudre des problèmes de scalabilité. Bitcoin Cash proposait des blocs de 4 Mo contre 2 Mo dans un bloc de Bitcoin. Un autre fork intéressant est celui de Bitcoin Gold, ce dernier propose un minage par GPU (cartes graphiques) et non par CPU, cela permet de diversifier le nombre de mineurs car la centralisation du minage est de fait plus compliquée. Dans le cas d'un fork ce sont les mineurs, essentiels dans le fonctionnement de la blockchain, qui tranchent en choisissant quelle version de Bitcoin miner. Dans les exemples donnés les nouvelles blockchains coexistent avec les anciennes.

Il est possible d'accéder au code source de Bitcoin :
<https://github.com/bitcoin/bitcoin>



Traçabilité des aliments et des biens de consommation

Un des premiers cas d'usage de ces blockchains "registres" est le traçage des aliments au sein de chaînes de production et de distribution. Le New York Times publiait au printemps 2017 un article intitulé "la blockchain : une nouvelle façon de traquer les côtes de porc, les actions et le mauvais beurre de cacahuète". Cette article revenait sur le nouveau projet d'IBM (géant de l'informatique) qui consiste à mettre en ligne une blockchain permettant de tracer les aliments du producteur au marchand et ce, sans avoir à centraliser toutes les informations concernant chaque produit.

Le principe est assez simple, IBM met en place la blockchain sur laquelle l'ensemble des collaborateurs de productions d'un produit pourront inscrire les modifications apportées, les personnes impliquées, ainsi que les dates de modification du produit. Le tout étant instantanément écrit sur la blockchain, personne ne peut remettre en cause sa propre participation mais surtout ces informations deviennent instantanément lisibles par tous les **noeuds du réseau** (les autres producteurs, les associations de consommateurs, etc.).

Cette idée est révolutionnaire dans le sens où elle résout tous les problèmes liés à la transparence des chaînes de production. Mais pas seulement, elle permet aussi de remonter beaucoup plus vite les chaînes de production en cas de fraudes ou de problèmes sanitaires.

Dans un monde hyper-mondialisé où les aliments font parfois plusieurs tours du monde avant de finir dans l'assiette du consommateur, il est nécessaire de pouvoir faire confiance en la provenance des produits.

De plus, cela résout aussi le problème des contrôles aux frontières. Aujourd'hui, un container peut avoir besoin de 30 signatures, de 30 organismes différents avant d'être accepté (taxes, organismes sanitaires, etc.) la blockchain permet de limiter les papiers et les signatures nécessaires pour approuver le passage d'un produit.

En 2017, la solution en était encore à l'essai et l'enjeu était alors de mettre en ligne l'ensemble des étapes de production d'un seul et même produit, en allant des producteurs de matières premières jusqu'à la mise en rayon dans les supermarchés en passant par le transport en bateau.

Au final, une solution blockchain est facilement applicable à ce genre de situation et dans ce type de domaine. La solution développée par IBM entraîne cependant quelques questions à propos de sa gouvernance (la place de l'entreprise étant centrale dans la prise de décision) certains se demandent si le pouvoir n'est alors pas trop centralisé dans ce système et si en cela il ne serait pas plus facile à le compromettre qu'une blockchain distribuée classique.

Prêts entre particuliers

Un des domaines les plus prometteurs en matière de décentralisation est le prêt d'actif et le crowdfunding. La blockchain est l'outil de décentralisation parfait quand il s'agit de prêter des fonds à une entité dont l'honnêteté est mise en doute. Elle permet à deux personnes totalement étrangères de se faire confiance sans intermédiaire. Ainsi il est possible de créer une plateforme d'échange décentralisée permettant directement l'échange et le prêt entre particuliers. La confiance est assurée par le protocole car personne ne peut répudier ou modifier un contrat écrit plus haut.

Cela est à double tranchant et si un contrat, même inégalitaire, est accepté par les deux parties il est impossible de revenir en arrière. Ainsi, il faut être prudent sur ce genre de système qui peut très vite profiter à des personnes mal intentionnées ([the DAO](#)).

Pour limiter ce genre d'escroquerie, il serait nécessaire de mettre en place des sanctions juridiques et de légiférer à propos de ces technologies car les seules sanctions sont économiques ou financières (confiscation des actifs, fermeture des portefeuilles, etc.).

LE SAVIEZ VOUS : Blockchain privée ou publique ?

Le premier cas d'usage de la blockchain est un registre décentralisé, distribué publiquement. De plus en plus d'entreprises et d'états s'intéressent à ce système d'enregistrement immuable et inviolable. Les organisations trouvent dans ce système un moyen de lutter contre la dégradation temporelle des registres mais aussi contre les malversations liées à ces enregistrements (fraude, détournement). Elles doivent cependant limiter leurs accès, n'importe qui ne peut pas inscrire quelque chose sur ces registres et n'importe qui ne peut pas valider un bloc. C'est pour cela que l'on parle de blockchain privée ou de consortium.

Ainsi une blockchain publique n'a pas de restriction, n'importe qui peut écrire une transaction et n'importe qui peut lire une transaction. De plus, n'importe qui peut valider un bloc du moment qu'il respecte le consensus imposé par la blockchain.

A l'opposé, un registre privé ne pourra être écrit et lu que par un nombre restreint de noeuds. De plus, seul l'administrateur de cette blockchain se voit octroyer le droit de valider un bloc.

Entre les deux, la blockchain de consortium (ou semi-privée ou semi-publique ou protégée) est un registre distribué à un certain nombre d'administrateurs qui ont la possibilité de valider des blocs. En général, l'écriture est limitée à quelques noeuds du réseau et la lecture reste publique (pour la traçabilité des produits, par exemple : seuls ceux qui participent à la création du produit peuvent écrire, toutes les organisations de consommateurs doivent pouvoir lire sur la blockchain et seul l'organisme de contrôle est capable de valider un bloc). Mais ce n'est pas le seul cas possible. L'inverse peut s'avérer utile notamment pour l'échange d'informations (déclarations d'impôts, etc.) .

Gestion des certifications et documents légaux

D'autres domaines peuvent être révolutionnés grâce à une solution blockchain. Par exemple dans le domaine de la gestion des certificats, une blockchain permettrait de limiter les fraudes et les falsifications, de garder une trace inaltérable de la certification et de protéger les personnes de la perte de leurs certificats. On peut noter deux exemples concrets d'application blockchain : les diplômes et les dossiers ou certificats médicaux.

Techniquement, cela se traduirait par la mise en place d'une blockchain à accès limitée telle qu'une blockchain de consortium. Pour le stockage de diplômes, l'accès serait limité en écriture, seules les université ou écoles pourraient y inscrire un nouveau diplôme. Et l'accès serait public en lecture pour que chacun (entreprise, particulier, autre université) puisse vérifier que la personne en question ait bien ses diplômes.

En France, seule une université a commencé à délivrer ses diplômes sur une blockchain : l'école supérieure d'ingénieurs Léonard-de-Vinci.

Elle délivre la certification de deux manières à ses élèves: à la fois le document classique de certification et à la fois le hash, de la transaction blockchain correspondant à la mise en ligne de son diplôme. Lorsque l'étudiant postule pour un poste il donne les "deux versions" de son diplôme, ce qui prouve que la version classique n'a pas été falsifiée : il l'a réellement passé quelques années auparavant. Une solution est proposée par Bitproof, une plateforme qui permet d'établir numériquement des documents légaux et des certifications infalsifiables et vérifiables par tous.

Autres documents importants, les certificats médicaux. Il est possible d'imaginer une blockchain pour l'ensemble des dossiers médicaux. Tous les patients sont référencés par une clef. L'accès en écriture et en lecture serait limité uniquement au médecin qui pourrait avoir un aperçu du passé du patient en un seul clic et ce, sans les problèmes de pertes et de falsifications possibles avec les certificats papier et les dossiers médicaux informatiques classiques.

Blockchain “Programmable”

Nous vous avons présentés les blockchain dite de “registre” qui utilisent les chaînes de bloc seulement pour stocker des données. Une innovation importante de la technologie blockchain est que selon sa construction elle peut être programmable. Les informations ne sont pas seulement stockées mais peuvent être travaillées de manière interne à la blockchain. Ce type de blockchain propose aux développeur un langage de programmation pour qu'ils y intègrent leurs algorithmes et il permet l'exécution de code de manière autonome.

```
13:09:23] accepted: 13/13 (100.00%) yes!
13:09:33] CPU #6: 70.87 kH/s
13:09:33] accepted: 14/14 (100.00%) yes!
13:09:36] CPU #1: 61.33 kH/s
13:09:43] CPU #6: 71.57 kH/s
13:09:43] accepted: 15/15 (100.00%) yes!
13:09:51] CPU #0: 45.67 kH/s
13:09:51] CPU #7: 71.18 kH/s
13:09:56] CPU #3: 68.62 kH/s
13:09:56] accepted: 16/16 (100.00%) yes!
13:10:00] CPU #0: 53.55 kH/s
13:10:00] accepted: 17/17 (100.00%) yes!
13:10:02] CPU #2: 64.77 kH/s
13:10:11] CPU #1: 65.83 kH/s
13:10:11] accepted: 18/18 (100.00%) yes!
13:10:14] CPU #0: 55.69 kH/s
13:10:14] CPU #4: 69.19 kH/s
13:10:14] accepted: 19/19 (100.00%) yes!
13:10:15] CPU #3: 65.05 kH/s
13:10:15] accepted: 20/20 (100.00%) yes!
13:10:18] CPU #6: 71.54 kH/s
13:10:18] accepted: 21/21 (100.00%) yes!
13:10:20] CPU #0: 56.55 kH/s
13:10:20] accepted: 22/22 (100.00%) yes!
13:10:22] CPU #5: 71.25 kH/s
13:10:23] CPU #5: 71.32 kH/s
13:10:23] accepted: 23/23 (100.00%) yes!
13:10:23] CPU #3: 67.19 kH/s
13:10:23] accepted: 24/24 (100.00%) yes!
13:10:37] CPU #3: 67.43 kH/s
13:10:37] accepted: 25/25 (100.00%) yes!
13:10:39] CPU #2: 64.67 kH/s
13:10:39] accepted: 26/26 (100.00%) yes!
13:10:50] CPU #2: 64.35 kH/s
13:10:50] accepted: 27/27 (100.00%) yes!
13:10:51] CPU #7: 71.16 kH/s
13:10:56] CPU #1: 63.28 kH/s
13:10:56] accepted: 28/28 (100.00%) yes!
```

Smart contract

La majorité des blockchains intègrent dans leur fonctionnement des tokens, voire des crypto-monnaies. Cette intégration permet le développement de contrats intelligents ou smart contract. Comme vous le savez, un des avantages de la blockchain est l'immuabilité de ce qui y est inscrit. Alors que la blockchain originelle, c'est-à-dire bitcoin est utilisé seulement comme un grand livre de comptes, les blockchains programmables offrent la possibilité d'intégrer dans celui-ci des contrats. Ils s'exécutent selon des variables pouvant être de différentes natures. Illustrons cela par l'exemple d'un contrat d'assurance : Un ensemble d'agriculteurs participent à un contrat d'assurance développé sur une blockchain, ils envoient périodiquement des fonds à l'adresse ou clef publique relative au contrat. Dans le contrat, il est stipulé (ou plus exactement codé) que si une sécheresse est en cours, des fonds leur seront redistribués c'est-à-dire transférés à leur adresse. Le contrat s'exécutera quand

des agriculteurs seront concernés par une sécheresse. Pour cela, le contrat dépend de données spécifiques à la météo.

Un "smart contract" peut prendre la forme souhaitée par les participants, il ne peut être modifié une fois lancé et son code est accessible à tous.

Il est possible de développer des applications utilisant exclusivement ou partiellement des smart contracts, elles sont appelées dApp (application décentralisée). Ce type d'application peut être développé comme équivalent à toutes applications actuelles nécessitant un contrôle centralisé : par exemple l'envoi de SMS (<https://www.birdchain.io/>). Cela ouvre aussi la porte à de nombreux nouveaux concepts d'applications dans le monde du numérique.

<https://www.ethereum-france.com/quest-ce-quune-dappquelques-exemples-simples/>

LE SAVIEZ VOUS ?

La qualité d'un smart-contract est qu'il est immuable. Son programmeur ne doit donc faire aucune erreur dans la rédaction de celui-ci. C'est pourtant ce qu'il s'est passé lors du déploiement de la première DAO, un codeur malveillant a alors siphonné une partie des ethers investis dans le projet en utilisant astucieusement le code open-source. Les tokens volés représentaient une valeur de 50 millions de dollars.

Un fork a eu lieu par la suite. Comme toute l'activité d'une blockchain est conservée, une partie des utilisateurs a choisi de revenir en arrière, l'autre partie a gardé dans la blockchain le hack créant Ethereum Classic. La blockchain Ethereum s'est scindée en deux.

Ethereum

Ethereum est le cas le plus populaire d'une blockchain programmable. Elle a été créée en 2013 par un jeune et talentueux programmeur nommé Vitalik Buterin. Aujourd'hui la capitalisation totale des tokens de ce projet équivaut à plus de 100 milliards de dollars.

Ethereum est une machine virtuelle décentralisée, c'est-à-dire un programme informatique simulant les caractéristiques d'un ordinateur. Ici la spécificité est qu'elle ne fonctionne pas sur une machine mais sur l'ensemble des machines du réseau. En utilisant la blockchain, elle exécute des programmes de manière sûre et transparente, ainsi les utilisateurs des smart-contracts ou Dapp.

FUN FACT

La blockchain Ethereum, comme beaucoup d'autres, a des problèmes de scalabilité. Récemment (décembre 2017), elle a vu son exécution ralentir car le nombre de calculs à réaliser était trop important. Le fait amusant est que cela provenait d'une application d'échange de cartes à collectionner virtuelles nommée crypto kitties. Les problèmes de scalabilité devront être résolus si la blockchain veut perdurer dans le temps.

Exécuter un programme nécessite des calculs qui engendrent des coûts. Le programmeur développant un "smart contract" devra prendre en compte cela. En effet chaque instruction atomique correspond à une unité de gaz (plus exactement "gas" en anglais). Ces unités de carburant sont référencées sur la valeur de l'ether (le token d'Ethereum). Ce sont les mineurs qui fixent le prix auquel ils sont prêts à effectuer le calcul.



<https://www.ethereum.org/>



Cet animal virtuel s'échange à plus de 4000\$!

Organisations autonomes décentralisées

Avec l'apparition de la Blockchain, les développeurs ont cherché à décentraliser une des relations les plus emblématiques de notre siècle : le contrat. En effet, la blockchain est l'outil de désintermédiation ultime, elle permet à n'importe qui de signer un contrat avec un inconnu et ce, en toute confiance. Les organisations autonomes décentralisées (ou DAO) sont donc nées : les premières organisations gérées par protocole informatique.

Le principe est simple : les règles sont définis au préalable par le concepteur. Elles sont transparentes et immuables. L'exécution de ces règles est entièrement protocolaire et décentralisée. Le premier exemple de ce type d'organisation est "The DAO", un fond d'investissement sans contrôle et décision centrale.

Dans la pratique, ce concept entraîne quelques problèmes pour la prise de décision. Une DAO se doit de poser un système de réputation robuste et fiable afin d'identifier de manière précise et fiable la compétence et le niveau d'implication de chacun.

En effet, chaque décision ne peut pas être soumise à tous les utilisateurs (trop long / pas efficace) et doit donc procéder à une évaluation systématique et objective des comportements. Une des solutions est d'associer un système de tokenisation à la DAO.

Cela permettrait de quantifier la "confiance" ou l'implication d'un participant : les acteurs de la DAO ont un poids décisionnel plus ou moins fort suivant leur investissement et/ou la réputation qu'ils ont au sein de l'organisation.

Vis à vis des institutions déjà en place, la DAO n'a aucun cadre législatif, elle n'a pas de valeur juridique, elle n'a pas de statut en dehors de la blockchain. Son impact dans le monde est donc assez limité, elle ne peut pas par exemple recruter des salariés, acheter des biens, attaquer en justice sous son nom ... Pour avoir un impact, la DAO fait appel à des consultants.

C'est d'ailleur l'un des gros risques, si une DAO utilise tous ses fonds auprès d'un prestataire de service qui ne réalise pas la prestation demandée elle n'a aucun moyen de faire valoir ses droits. D'une autre manière, si la DAO n'a pas mis en oeuvre suffisamment de mécanismes de contrôle sur la blockchain pour s'assurer de la bonne exécution du service, les participants ne peuvent pas revenir sur une clause inscrite sur le contrat de la DAO. On peut trouver des formes de DAO très différentes : sur les formes de rémunérations (crypto-monnaies, ...), sur les formes de décision, sur le projet final, etc.

La BitNation : gouvernance décentralisée

Le dernier cas d'usage survolé par ce dossier est peut-être l'ultime application de la blockchain : la gouvernance décentralisée (ou non-géographiquement lié). L'idée est de créer une nation virtuelle, un gouvernement exécuté sur blockchain de manière protocolaire. Les innombrables possibilités de gouvernance rendues possible par la blockchain ne seront pas explorées dans leur ensemble de si tôt. C'est pourquoi l'étude de cas paraît être la meilleure manière pour analyser les composants nécessaires à la mise en place d'une telle gouvernance. Nous étudierons donc la BitNation, basée sur la blockchain [Ethereum](#), figure de proue dans le domaine de la gouvernance décentralisée.

Ainsi comme elle se déclare elle même, la BitNation est : "un Agrégateur de Services de Gouvernance Contingent Non-Géographiquement Lié", c'est-à-dire qu'elle permet le développement et le recensement de services globaux de gouvernance. Cette définition comprend plusieurs notions clefs : elle avance l'idée d'état détaché de la nation (pas de frontières géographiques, ethniques, culturelles ou religieuses), les états seraient entièrement "volontaires" (c'est-à-dire que les états sont développés directement par les utilisateurs) et enfin toutes les "institutions" de ces gouvernements doivent être décentralisées (donc implémentées sur blockchain).

La BitNation se voit comme une plateforme sur laquelle n'importe qui peut, dans un langage de programmation simple, implémenter son idée de gouvernement sur la blockchain. Elle permet de répondre à des besoins assez larges en matière de gouvernance puisqu'elle propose des services de droits (Identité / Mariage & Divorce / Enregistrement de Compagnies / Enregistrement Foncier / Certificats de Naissance & Décès), d'assurance civile (Santé / Chômage / Pension), de diplomatie (Plaidoyer / Gestion des Crises) ou encore de sécurité.

La BitNation se revendique issue de l'idéologie libertarienne et crypto anarchiste comme elle était développée dans les débuts du BitCoin et des blockchains en général. Subira-t-elle elle aussi ce changement idéologique au profit d'une logique entrepreneuriale ? Sa conceptrice, Susanne Tarkowski Tempelhof, a fondé la BitNation seulement en 2014 et l'avenir de l'entreprise reste imprévisible. En 2016, Susanne rédige sa propre constitution sur BitNation (nommée nation Pangea). L'entreprise base sa stratégie de communication sur le fait que les informations sur la conceptrice sont assez floues et elle n'hésite pas à la présenter comme un messie qui apporte les solutions à nos problèmes de gouvernance.

En pratique, la BitNation développe plusieurs programmes d'aide dans des domaines différents. La plus efficiente et la plus concrète des fonctions de BitNation est sans doute le BRER (BitNation Refugee Emergency Response) qui permet à n'importe quel réfugié de se créer une identité virtuelle. Cette identité donne le droit à une carte de crédit et d'autres services de base mais elle permet surtout aux associations non gouvernementales de recenser plus précisément le nombre et les localisations des réfugiés.

LE SAVIEZ VOUS ?

De nombreux projets de gouvernance décentralisée voient le jour partout sur la planète. La BitNation n'est qu'un exemple parmi d'autres. On peut trouver aujourd'hui des projets à des échelles très diverses. La BitNation essaie de créer une gouvernance décentralisée et non localisée mais il existe des projets de gouvernance mondiaux, d'autres plus locaux.

Par exemple, l'IIEP (international institute for educationnal Plannig) développe des solutions éducatives dans les pays en développement. Il intervient au niveau des écoles et des états pour orienter les politiques.

D'un autre côté, des programmes liés à l'éducation et à l'entrepreneuriat sont développés comme l'Exosphère ("communauté d'apprentissage entrepreneuriale et laboratoire de résolution de problème").

L'impact réel de la BitNation reste à démontrer mais une chose est sûre : elle gagne en notoriété. Dernièrement, l'Estonie a signé un partenariat avec la plateforme pour gérer son programme d'e-résidence (nationalité numérique).

D'autres pensent que la blockchain va tuer le management tel que nous le connaissons. En effet, certains pensent à remplacer les managers par un blockchain. Cela permet l'interaction et le contrôle des membres d'une équipe sans intervention d'une autorité centrale quelqu'elle soit.

Ainsi en utilisant des principes de collaboration simples tel que la stigmergie (communication par l'environnement) ils seraient capable de faire de la gestion d'équipes ou de projets de manière totalement décentralisée.

Notons un dernier exemple, beaucoup moins médiatisé dans les pays occidentaux, le contrôle facilité des élus par les populations locales. C'est le CEFCI (Centre Féminin pour la démocratie et les droits humains en Côte d'Ivoire) qui a initié cette solution, ici pas de blockchain mais la même idée de remettre les localités et les acteurs au centre des décisions.

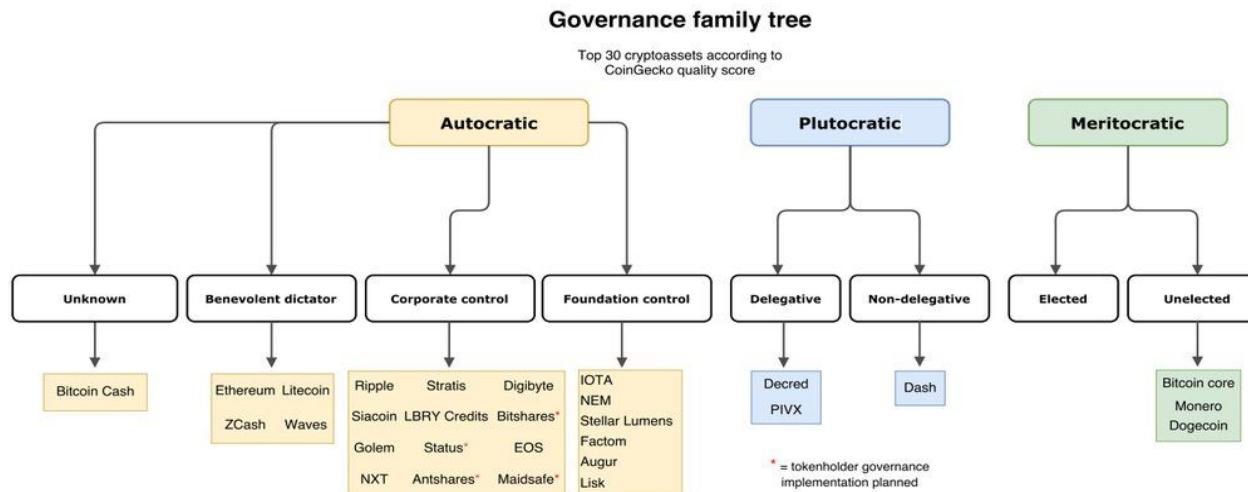
A propos de gouvernance

Pour aller plus loin...

Le code d'une blockchain (qui implémente : le consensus, le nombre de transactions par bloc et le contenu des blocs) n'est pas aussi immuable que peut l'être l'information stockée sur les blocs. Une blockchain peut continuer à se développer bien après son premier bloc et peut revenir sur certains problèmes liés à la scalabilité ou changer le mode de consensus par exemple. Ainsi, pour répondre aux différents problèmes des développeurs travaillent à l'amélioration du code de cette blockchain. La direction prise par ces registres dépend donc du type de gouvernance auquel il est soumis. D'après une étude faite dans le cadre de l'université d'Edimbourg, il existe 3 grands types : les blockchains dites "autocratiques" (les plus répandues), dirigées par des protocoles informatiques, elles sont donc autogérées.

On peut retrouver différentes formes de contrôle du protocole : par le biais d'une entreprise, d'une association ou par des bénévoles.

Il est possible de trouver des blockchains dites "ploutocratiques", c'est-à-dire que le pouvoir décisionnel est déterminé par la quantité d'actifs dont dispose le noeud. Enfin, les blockchains "meritocratiques", bitcoin par exemple, le pouvoir décisionnel est détenu par les mineurs ou ceux qui participent au système. Chaque système a ses inconvénients et ses avantages. Si on observe aujourd'hui une recrudescence des projets à gouvernance corporative, les premières blockchains actives étaient, pour la plupart, dirigées par des bénévoles.



A Cross-Sectional Overview of
Cryptoasset Governance and
Implications for Investors
by Nic Carter
2016/2017

Gestion des énergies

Un des domaines où la décentralisation est la plus pertinente est la production et la gestion énergétique. En effet, la production et la gestion de l'électricité se font de manière centrale (par un état ou collectivité). Cela permet une meilleure gestion (réseau global, maintien des infrastructures sur le long terme, ...) à grande échelle. En France, par exemple, l'ensemble de l'électricité passe par EDF, organe central de la production énergétique, sauf quelques exceptions. Il existe cependant une autre forme de gestion des énergies : dans certains pays la production et la gestion du réseau énergétique se font de manière concurrentielle. Le réseau matériel est toujours centralisé mais l'électricité sur le réseau est produite par des sources différentes (cela permet un coût de l'électricité plus faible et une meilleure production).

Mais alors qu'apporte la blockchain dans ce domaine d'application ?

L'idée, avancée par les entreprises à la base de ces solutions, est d'utiliser l'ensemble des producteurs d'énergie d'une région qu'ils soient particuliers, entreprises ou collectivités et de créer un réseau interne implémenté sur une blockchain.

La plupart des solutions utilise un système de tokenisation différencié (par exemple, un token pour la production avec une valeur variable et un token pour la consommation avec une valeur elle aussi variable). Ces tokens permettent au consommateur lambda d'acheter son énergie de la même manière qu'auparavant (mais sans passer par un tiers de confiance telle qu'une entreprise ou EDF) et au producteur classique de vendre leur énergie de la même façon. Le consommateur qui souhaite aussi produire son énergie (grâce à des productions vertes, par exemple : solaire, éolien, hydro moteur) pourrait vendre son énergie lorsqu'il n'en consomme pas et ensuite changer ses tokens de production en token de consommation, ou directement en monnaies.

A terme, une organisation décentralisée telle que celle-ci permettrait à chacun de retrouver son indépendance énergétique (notion de plus en plus importante en cette période de crise des énergies fossiles). En effet, l'idéal serait que chacun soit à la fois consommateur et producteur d'énergie. Peut-être, la blockchain permettra à chacun de produire de l'énergie pour tous.

FUN FACT ?

En 2010, alors que Bitcoin était une invention toute récente, Hanyecz, un développeur Floridien, achète deux pizzas pour 10 000 bitcoins. Cela représenterait aujourd'hui une pizza à 50 millions de dollars. Cette évolution des prix montre bien la propriété déflationniste de cette monnaie ainsi que l'engouement des utilisateurs vers celle-ci.

Lexique II :

- **Bitcoin** : projet de cryptomonnaie, à l'origine du concept de blockchain. [P25](#), [P34](#)
 - **Blockchain de consortium** : un registre distribué à un certain nombre d'administrateurs qui ont la possibilité de valider des blocs. [P32](#)
 - **Crypto-monnaie** : monnaie numérique utilisant la technologie blockchain. [P34](#)
 - **Fork**: Séparation d'une blockchain en deux. [P34](#)
 - **Livre Blanc** : Document présentant un concept ou une idée. [P27](#)
 - **Tokens** : jetons numériques, utilisables seulement sur une blockchain, parfois échangeables (dans le cas de crypto-monnaies). [P34](#) , [P40](#)
 - **Smart-contract** : contrat inscrit dans une blockchain sous forme de code informatique. [P35](#)
 - **Dapp** : application décentralisée, programmée sur une blockchain avec l'utilisation de smart-contract. [P35](#)
 - **DAO** : Dapp représentant une organisation.
 - **"The DAO"** : première DAO, connue pour s'être faite hacker. [P31](#)
 - **Ethereum** : blockchain populaire permettant la programmation de smart-contract. [P37](#) , [P39](#)
- Note :** Vous pouvez retrouver votre page d'accès grâce aux liens.

Interview de Maxime Beynet, *participant à la création d'un studio de jeux vidéo utilisant la Blockchain.*

“

Bonjour Maxime, peux-tu te présenter ?

Je m'appelle Maxime Beynet. J'ai 27 ans. Je m'intéresse à la Blockchain depuis 2012. **A la suite de la crise des subprimes, je me suis posé la question du fonctionnement du système bancaire.** Je suis arrivé à la conclusion, après des recherches, que l'on avait déplacé le problème [et que l'on ne l'avait pas résolu]. Ces problèmes étaient essentiellement dus à l'émission de crédits et au manque de fonds propres des banques. Comment pouvais-je alors me protéger et conserver de l'épargne en dehors du système bancaire ? Après des recherches, la première étape fut d'acheter de l'or et de l'argent afin de conserver une épargne réelle. Je suis vite arrivé à la conclusion que ce n'était pas pratique. Ca ne permettait pas de payer par internet, je me suis mis alors à chercher un moyen de payer à distance sans passer par le système bancaire. **C'est à ce moment là que j'ai fait la connaissance de Bitcoin.**

*Pour savoir plus sur le Studio de Jeu :
www.incenti.net (bientôt disponible)*

Pour toi la réelle révolution, si il y en a une, est-elle dans la crypto monnaie ou dans la blockchain ?

Le tour de force intellectuel c'est Bitcoin. Il répond à des problèmes de transmission de l'information sans autorité centrale. Peu importe le type d'information que l'on transmet, cela peut être des dettes, des créances, des transferts monétaires. [...] **Je pense que le plus gros de l'innovation future sera grâce à la blockchain,** mais cela n'aurait jamais pu arriver sans l'exemple de Bitcoin et l'exemple monétaire.

[...]

Les problématiques soulevées par la blockchain, sont soulevées par **l'école autrichienne d'économie.** C'est un courant plutôt hétérodoxe qui se pose des questions sur l'indépendance, la décentralisation, la liberté, l'autorité centrale et les questions des contre-pouvoirs. Sur les aspects philosophiques, c'est la philosophie libertarienne, qui est transpirée à travers les premiers textes de Satoshi Nakamoto.

Est ce que tu peux présenter ton projet ?

On développe un studio de jeux vidéo qui s'appelle **Incentive Studio**. L'idée c'est d'utiliser la capacité de la blockchain et l'émission de smart-contract, **des contrats sur la blockchain, pour faire du jeu vidéo**. L'idée, spécifiquement, c'est d'utiliser le potentiel des cryptomonnaies et la possibilité de faire du transfert de pouvoir d'achat pour faire de l'incitation économique. On prend du jeu vidéo et on y ajoute une incitation économique grâce à la technologie blockchain. Actuellement on développe un jeu, **NodaChain**, qui est un jeu masse multijoueurs dans l'espace. Dans un avenir proche on va prendre des jeux de type classique, des jeux de plateaux, de casino. On va les "blockchainiser" et les tokeniser c'est-à-dire qu'on se servira de la capacité du token pour faire un jeton numérique, comme un jeton de casino. On se sert du smart-contract pour inscrire le jeu sur la blockchain, donc **utiliser la technologie et sa capacité de décentralisation pour faire émerger de la confiance**.

Quel est ton rôle au sein de ce projet ?

Je suis producteur exécutif. Je donne mon avis sur les choix stratégiques et sur l'orientation [du projet]. Je suis économiste de formation. Je m'occupe de tout ce qui est finances, questions juridiques et aspects monétaires et économiques de la technologie.

Appréhendez-vous des problèmes de scalabilité ?

La scalabilité est actuellement un problème, mais il existe des outils à venir : le Lightning Network sur Bitcoin, la Proof of Stake sur Ethereum. Pour nous ce n'est pas un problème pour l'instant, on va déployer la technologie une fois qu'on aura écrit nos contrats et d'ici là on a de bons espoirs, des informations, qui nous laissent penser que les réseaux seront suffisamment scalables. S'il y a un problème on fera une chaîne privée en Delegated Proof of Stake ou en Proof of Authority. Et on aura des "tuyaux" suffisamment larges pour faire tourner notre chaîne.

[Des conseils pour ceux qui sont tentés d'investir ?]

Il faut comprendre qu'il y a une valeur sous-jacente à posséder des crypto-monnaies. **Elles sont au fond des parties d'un réseau; on est alors propriétaire des droits d'accès et des droits d'usage d'une partie de ce réseau.** Cependant toutes les blockchains ne se valent pas et il n'y aura pas de place pour tout le monde. Des leaders vont émerger et remplacer de plus petites blockchains. La qualité des projets, le service qu'ils proposent, l'équipe, la taille et le dynamisme réel de la communauté sont à prendre en compte. Ne nous laissons pas berner par du joli marketing, des promesses en l'air qui n'engagent personne et l'appât du gain. L'investissement sur ce marché est risqué et il faut être prêt à assumer gains et pertes potentiels.

Bibliographie, sitographie

Leloup, P. (2017) *BLOCKCHAIN, La révolution de la confiance*. Clermont-Ferrand : La source d'Or

Blockchainfrance (<https://blockchainfrance.net>)

Blogchain Café (<http://blogchaincafe.com/>)

Bitcoin.fr (<https://bitcoin.fr/>)

BitNation (<https://bitnation.co/>)

Ethereum France (<https://www.ethereum-france.com/>)

Ethereum Project (<https://www.ethereum.org/>)

Journalducoin.com (<https://journalducoin.com/>)

Wikipedia (<https://fr.wikipedia.org/>)

Les images utilisées proviennent de wikimédia (<https://commons.wikimedia.org/>).

Le document a été réalisé par Robin Couret, Justine Raynouard et Etienne Thomas.

Pour en savoir plus sur :

Cryptographie :

- <https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-12/>
- <https://fr.wikipedia.org/wiki/SHA-2#SHA-256>

Minage bitcoin :

- https://bitcoin.fr/video-bitcoin-monnaie-ecolo/?utm_source=dlvr.it&utm_medium=twitter
- <https://www.newscientist.com/article/2151823-bitcoin-mining-uses-more-energy-than-ecuador-but-theres-a-fix/>
- https://www.youtube.com/watch?time_continue=84&v=K8kua5B5K3I
- <https://bitcoin.fr/minage>

Traçage des aliments :

- <https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html>

Pour en savoir plus sur :

Gestion des diplômes :

- <https://blockchainfrance.net/tag/diplomes/>

Smart contract :

- <https://www.ethereum-france.com/quest-ce-quune-dappquelques-exemples-simples/>

Ether :

- <https://www.ethereum-france.com/comptes-transactions-gaz-et-limites-de-gaz-par-bloc-sur-ethereum/>

Gestion des énergies :

- <http://www.strategie.gouv.fr/publications/20172027-energie-centralisee-decentralisee-actions-critiques>

Bitnation :

- <https://www.imaginer-demain.fr/bitnation-premier-etat-virtuel/>

Gouvernance des blockchains :

- <https://coinmetrics.io/papers/dissertation.pdf>