

2016

Principes clés d'une application blockchain



GODEBARGE Ferréol
ROSSAT Romain
EM Lyon Business School
15/12/2016

Remerciements

Table des matières

Introduction	4
I. Présentation des Blockchains.....	5
I.1. Le concept en quelques mots	5
I.2. Précisions techniques en partant de l'origine des Blockchains : le Bitcoin.....	6
I.2.a. Introduction.....	6
I.2.b Les transactions	7
I.2.c L'horodatage.....	9
I.2.d Preuve de travail	9
I.2.e Le réseau	13
I.2.f Incitation.....	13
I.2.g Economiser l'espace disque	14
I.2.h Vérification de paiement simplifié	17
I.2.i Vie privée	17
I.3 - Principes clés d'une blockchain	18
I.3.a De nombreux objets utilisables par le concept de blockchain	18
I.3.b Etapes de validation par le réseau.....	21
I.3.c Récompense des mineurs	22
I.3.d Confidentialité.....	22
I.4 Synthèse du concept de la blockchain	24
II. Une nouvelle façon d'appréhender des besoins d'entreprise.....	25
II.1 Horizon des possibilités basées sur des « use cases ».....	25
II.1.a Document de base permettant de mener l'analyse	25
II.1.b Digital Content / Documents, Storage & Delivery.....	26
II.1.c Authentication & Authorization	26
II.1.d Digital Identity	27
II.1.e Marketplace.....	28
II.1.f Smart Contract	29
II.1.g Real Estate.....	29
II.1.h Diamonds	30
II.1.i Trading Platforms	30
II.1.j Reviews / Endorsement.....	31
II.1.k Blockchain in IoT	31
II.1.l App Development	32
II.1.m Network Infrastructure & APIs.....	32

II.1.n Currency Exchange & Remittance.....	33
II.1.o P2P Transfers	34
II.1.p Ride Sharing.....	34
II.1.q Data Storage	34
II.1.r Gaming	35
II.1.s Others.....	35
II.2 Synthèse des applications possibles.....	39
II.2.a Facteurs d'utilisation de la blockchain.....	39
II.2.b Données infalsifiables.....	39
II.2.c Sécurité par cryptographie.....	40
II.2.d Baisse des coûts de transaction	40
II.2.e Authentification des données par consensus.....	41
II.2.f Organisation communautaire.....	42
II.2.g Registre de compte public	42
II.2.h Rapidité des transactions	42
Conclusion	44
Lexique	45
Bibliographie	47

Introduction

La notion de transaction peut se définir de différentes manières. Elle peut être considérée comme une opération commerciale ou boursière, un contrat, un accord, ou encore, en informatique, une opération élémentaire de saisie ou de consultation d'information. Plusieurs modèles existent de nos jours. Cependant, tous reposent sur certaines caractéristiques : les deux ou plusieurs parties qui permettent de réaliser une transaction, et un tiers de confiance, permettant de certifier la validité de cette transaction. Depuis la naissance de la notion de propriété, plusieurs transactions étaient notées dans des registres, et ces documents étaient la preuve physique de l'authenticité de la transaction. Puis l'utilisation de monnaies fiduciaires, qui ne sont plus des pièces métalliques, mais des billets, ou du papier possédant une certaine valeur autre que physique, oblige la société à se servir d'institutions afin de garantir la valeur de ces nouveaux moyens de transaction. Ainsi, la confiance devient, à travers le contrôle de ces institutions, une base fondamentale pour toute transaction.

L'internationalisation des transactions, dès l'après-guerre, implique de nouvelles modalités de transactions, le nombre de transactions augmentant de manière exponentielle. Le risque lié à l'authenticité des transactions s'accroît et de nouveaux tiers de confiance sont nécessaires. A titre d'exemple, le système interbancaire SWIFT en 1977 ou l'OMC en 1995 ont été créés afin de réguler les transactions. Ces tiers de confiance doivent permettre une sécurisation des transactions d'une part, ainsi qu'une fluidité qui serait la même pour les acteurs économiques que s'ils agissaient sans institutions, ne générant donc pas de perte économique éventuelle.

Avec des progrès technologiques de plus en plus pointus, notamment en cryptographie et en gestion de réseaux, ce modèle pourrait être remplacé par un nouveau système. Il pourrait, entre autres choses, supprimer le rôle du tiers de confiance. Cependant, ces progrès technologiques ont été, pour de nombreuses personnes, la possibilité de remettre au goût du jour une philosophie qui préexistait, prônant l'égalité par l'économie et la technologie notamment. Ainsi, l'idéologie de cette nouvelle technologie, appelée Blockchain, est l'héritière des idéologies « Cyberpunk », qui voient la technologie comme un moyen de s'affranchir de contrôle humain inégalitaire.

Ce Projet de Fin d'Etudes a pour but de présenter le système de transactions basé sur les Blockchains, et d'illustrer ce modèle à l'aide d'exemples concrets et innovants afin de définir les nouveaux principes d'application de la blockchain pouvant s'appliquer à de nombreux secteurs.

I. Présentation des Blockchains

L'objet de cette partie est de présenter les blockchains d'une manière conceptuelle dans un premier temps, avant de préciser ensuite les mécanismes techniques liés à cette technologie, en s'appuyant sur la création de la première blockchain : celle du Bitcoin.

I.1. Le concept en quelques mots

La Blockchain est une chaîne de blocs de codes informatiques. Chaque bloc contient des attributs relatifs à une ou plusieurs transactions (expéditeur, destinataire, montant...), ou autres objets qui seront précisés ultérieurement. Il contient également des informations liées au bloc prédécesseur sur le Blockchain, et il est encrypté, c'est-à-dire qu'il est sécurisé à l'aide de procédés cryptographiques (algorithmes informatiques).

Lorsque les transactions récentes sont enregistrées, elles sont regroupées en bloc, et chaque transaction sera validée par les « mineurs », qui vont analyser la chaîne de blocs entière. Ci-dessous est présenté un schéma très général correspondant à l'ajout d'un bloc de données transactionnelles sur le Blockchain.

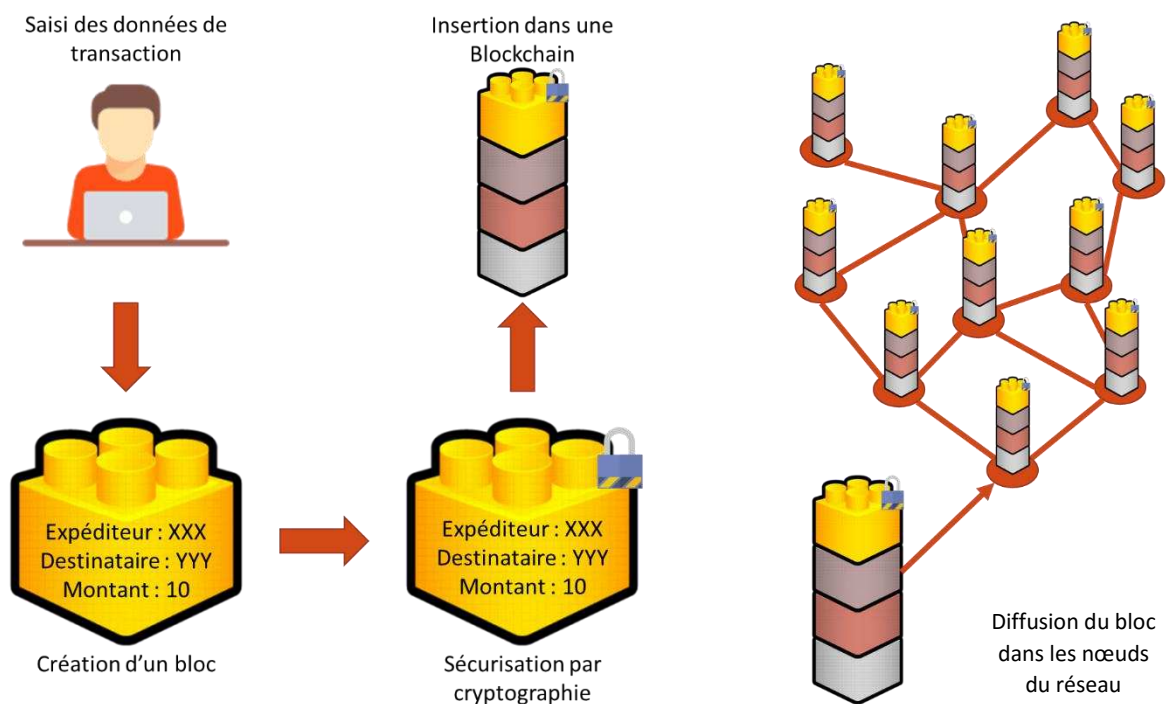


Figure 1: Ajout d'un bloc contenant une transaction dans un Blockchain

I.2. Précisions techniques en partant de l'origine des Blockchains : le Bitcoin

I.2.a. Introduction

Afin de mieux comprendre le fonctionnement technique de la Blockchain, nous nous intéresserons au système sous-jacent au Bitcoin, expliqué par Satoshi Nakamoto, dans sa publication « Bitcoin : A Peer-to-Peer Electronic Cash System », disponible sur le site www.bitcoin.org.

Tout d'abord, le Bitcoin est une crypto monnaie inventée en 2008, et dont le logiciel open source est publié en 2009. Une monnaie cryptographique, ou crypto monnaie, est une monnaie électronique sur un réseau Peer-to-Peer ou décentralisé (chaque client, appelé nœud, est également un serveur). Afin de sécuriser cette monnaie, le système de transaction repose sur le concept de blockchain, basé en partie sur des procédés de cryptographie.

L'intention de Satoshi Nakamoto a été de créer un système de paiement électronique, pouvant se passer de l'intervention des institutions financières. De nos jours, le commerce en ligne est dépendant d'institutions financières. Ces institutions ont pour objectif d'effectuer le traitement des paiements. Cependant, ce système présente des faiblesses, dont notamment celle de devoir accorder sa confiance à ces dites institutions. Par exemple, une transaction purement irréversible n'est pas possible dans ce système, puisque l'institution gère les conflits de transactions. De plus, ces institutions possèdent un coût de fonctionnement pour effectuer ce travail de médiation. Ce coût se répercute donc sur les transactions effectuées, empêchant ainsi la possibilité de réaliser des transactions à faible coût. Ces deux problématiques, que sont l'irréversibilité et le coût forment deux enjeux majeurs de cette technologie. La possibilité d'inversion de transaction pour un service irréversible génère un coût supplémentaire. Cela requiert une confiance accrue, des justificatifs requis, et une possibilité d'avoir un risque de fraude non nul. Il s'agit donc, pour Satoshi Nakamoto, de permettre l'utilisation d'une monnaie virtuelle, limitant les problématiques énoncées plus haut.

Il propose ainsi un système basé sur des preuves cryptographiques, censées remplacer la confiance accordée aux institutions financières. Ce système a pour objectif de répondre à plusieurs enjeux :

- Une transaction entre deux parties sans tiers de confiance
- Des vendeurs protégés contre d'éventuelles fraudes grâce à une impossibilité de supprimer ou modifier une transaction
- Des acheteurs protégés avec un système de comptes séquestres (terme juridique : indisponibilité d'un bien pendant une courte période)
- Pas de double dépense possible grâce à l'horodatage des transactions

Ce système est cependant possible uniquement si la puissance de calcul des nœuds « honnêtes » du réseau est plus importante que celle des nœuds agissant pour réaliser une attaque combinée sur le réseau. Ce concept sera explicité ultérieurement.

I.2.b Les transactions

Une pièce électronique est définie comme une chaîne de signatures numériques. Un propriétaire peut transférer cette pièce de cette manière :

- 1) Vérifier et signer numériquement l’empreinte / hachage de la transaction précédente (1 et 1')
- 2) Vérifier et signer numériquement la clé publique du nouveau propriétaire (2)

Ces signatures sont ajoutées en fin de transaction (3). Les bénéficiaires ont la possibilité de vérifier la chaîne.

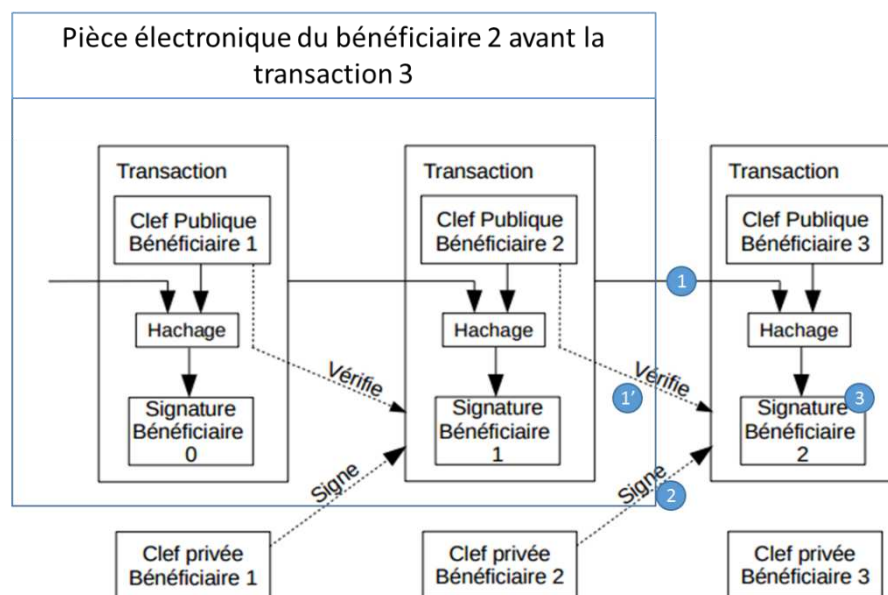


Figure 2 : Système de transactions (source : <https://bitcoin.fr/bitcoin-explique-par-son-inventeur/>)

Ce système seul soulève notamment un problème majeur : un bénéficiaire ne peut pas vérifier si un précédent bénéficiaire a réalisé une « double dépense » avec la pièce. Une solution pourrait être de créer une autorité de surveillance des transactions, ou tiers de confiance. Ainsi, chaque pièce devrait être retournée à cette autorité, qui en crée une nouvelle. Seules les pièces provenant de cette entité sont alors acceptées. Cela évite ainsi qu'une pièce soit utilisée deux fois. Cependant, cette solution repose sur ce tiers de confiance. C'est justement cela que voulait éviter Satoshi Nakamoto.

Dans le cas du tiers de confiance, ce dernier était au courant de l'ensemble des transactions effectuées, ce qui lui permettait de savoir si une pièce avait été utilisée dans une autre transaction ou non. Une méthode fiable et efficace permettant de connaître l'historique de toutes les transactions de manière partagée doit donc être trouvée. Parmi toutes les nouvelles transactions mettant en jeu cette pièce électronique, seule la plus ancienne doit être celle que le système doit valider. Il faut donc que l'ensemble des transactions soient rendues publiques, et le système doit faire en sorte que tous ses participants mettent en évidence un historique commun de transactions. Le bénéficiaire a donc besoin de savoir que la majorité

des nœuds a établi cet historique (condition qui valide le bloc de transactions), et ceci pour chaque temps de transaction.

Le concept des transactions repose en réalité sur la cryptographie asymétrique. Cette dernière lie deux éléments clés : la clé publique et la clé privée. Elles permettent de garantir l'intégrité des données transmises en chiffrant les données envoyées, ainsi que l'authentification de l'origine de la transaction.

Lorsque quelqu'un se lance dans le processus de création d'une transaction, il génère, à l'aide d'un logiciel dédié, une clé publique et une clé privée. La clé privée n'est transmise à personne et la clé publique est, quant à elle, disponible pour tout le monde.

Présentation succinct du concept :

La cryptographie asymétrique repose principalement sur les « fonctions à sens unique », fonctions mathématiques qui sont quasiment impossible à inverser (cela demande énormément de puissance et de temps de calcul). Elles ont pour particularité d'avoir cependant une brèche, c'est-à-dire un moyen, pour celui qui l'a construit, d'inverser la fonction. Cette brèche est appelée clé privée, et la fonction à sens unique, clé publique.

Fonctionnement :

Imaginons que A veuille pouvoir recevoir des messages indéchiffrables de tous sauf lui, de la part de n'importe qui.

A envoie ainsi à tous la fonction à sens unique (clé publique) et garde pour lui-même la fonction de décodage. B reçoit le message et applique la fonction à sens unique, avant d'envoyer le résultat à A.

A a la capacité de décoder le message de B grâce à la fonction de décodage (clé privée). Le message était donc bien codé pour l'ensemble du réseau, avant d'arriver à A. Par ailleurs, A peut, après avoir déchiffré le message, envoyer à B une information qui permet d'être sûr que le message a bien été déchiffré. Cette information, c'est l'identité du message, appelé « hash » et qui sera explicité dans les parties suivantes.

Ainsi, ce concept permet :

- De chiffrer un message
- D'authentifier l'expéditeur

Plusieurs fonctions à sens unique existent, et certaines sont plus efficaces que d'autres. Il faut s'assurer que ces fonctions soient suffisamment « sécurisées » (i.e. dont la brèche est difficile à trouver).

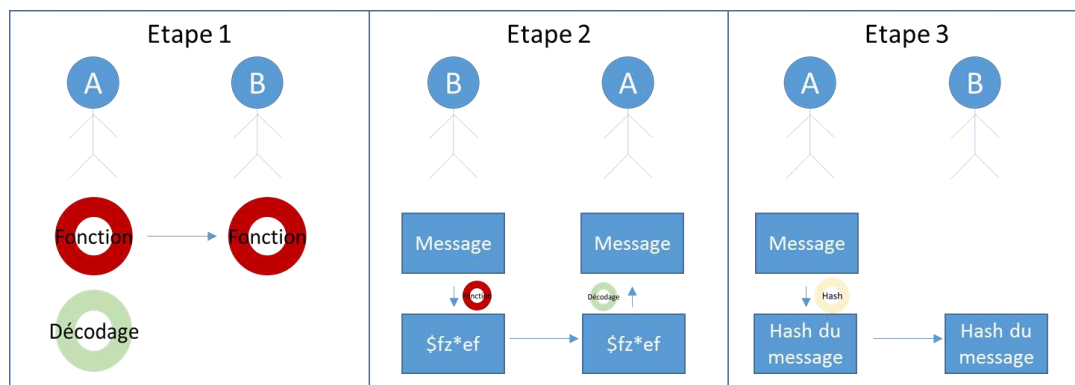


Figure 3 : Principe de fonctionnement de la cryptographie asymétrique

Dans ce schéma, on peut ainsi voir :

- *Etape 1 : A possède la fonction à sens unique (ici « fonction ») et la brèche (fonction de décodage). Il transmet ensuite à B la fonction.*
- *Etape 2 : B écrit un message, et, à l'aide de la fonction, il chiffre le message, avant de l'envoyer à A. A utilise donc sa fonction de décodage pour le déchiffrer.*
- *Etape 3 : A calcule le « hash » (i.e. identité propre à chaque donnée) du message et l'envoie à B. B a donc la preuve que A a bien réussi à déchiffrer son message et qu'il est donc bien à l'origine de la fonction à sens unique.*

I.2.c L'horodatage

La solution imaginée repose donc sur un service d'horodatage. Ce serveur fonctionne de la manière suivante, dans le cas général :

- Le serveur réunit un ensemble d'objets (transactions) et prend l'empreinte (Hash) de cet ensemble
- Il annonce ensuite cette empreinte sous la forme d'un message sur un forum Usenet (système de réseau de forums)
- Chaque horodatage contient l'horodatage précédent, ce qui constitue une chaîne de blocs horodatés, d'où le terme de Blockchain

Ainsi, chaque nouvel élément vient confirmer l'élément précédent.

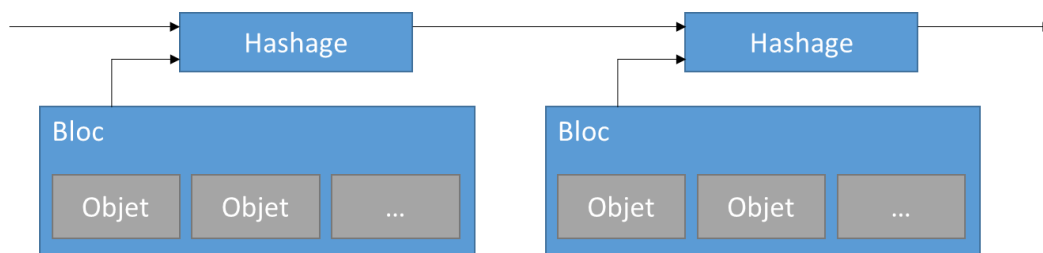


Figure 4 : Illustration de l'horodatage

Le principe de l'empreinte (hash) est défini dans le paragraphe suivant. Afin de comprendre le schéma précédent, l'empreinte d'une donnée (un fichier, un dossier, une image, ...) est unique. Ainsi, deux blocs avec des transactions identiques, mais qui possèdent des prédécesseurs différents n'ont pas la même empreinte. De même, si deux blocs possèdent les mêmes transactions, mais dans un ordre différent, alors ces deux blocs n'ont pas la même empreinte. Ainsi, une blockchain est identifiable par son empreinte unique.

I.2.d Preuve de travail

Le paragraphe précédent présente le concept de la solution proposée par Satoshi Nakamoto. En réalité, le système (l'ensemble des nœuds du réseau participant à l'élaboration de la blockchain), a besoin d'avoir une preuve de la véracité des informations du bloc qui doit être ajouté. Ceci passe ainsi par le concept de « preuve de travail ». Afin de créer un serveur d'horodatage dans un système qui est celui imaginé, c'est-à-dire un système reposant sur un

réseau peer-to-peer distribué, la preuve donnée par un message sur un forum Usenet ne convient pas. Il faut donner une preuve de l'authenticité d'un bloc suffisante. La preuve de travail est donc l'algorithme permettant le consensus de l'ensemble des nœuds du réseau sur le bloc qui fait foi.

Ainsi, afin d'être authentifié, une transaction doit être intégrée à un bloc contenant d'autres transactions. La validation de ce bloc est réalisée par le procédé cryptographique appelé preuve de travail. Ce procédé a pour but de trouver un double hash en SHA-256 correspondant au bloc en cours, à partir du bloc qui le précède. Un hash correspond à l'identité, appelée également empreinte d'un fichier. Un bloc possède donc un unique hash. SHA-256 est une fonction qui, à chaque donnée, associe un unique nombre, qui est l'identité de ces données. Le moindre bit modifié dans les données de départ change le résultat de la fonction SHA-256.

Ainsi, afin d'ajouter un nouveau bloc à la chaîne de blocs, les nœuds participant à la création de la chaîne (les mineurs) doivent lancer un procédé cryptographique : le calcul du hash du bloc. Ce procédé a pour but de convertir des données en une suite pseudo-aléatoire de chiffres. Il est impossible de modifier les données en entrée de l'algorithme pour obtenir un résultat précis. Ceci est dû au caractère aléatoire de l'algorithme.

Voici comment marche un algorithme de Hachage : c'est une fonction mathématique qui, à partir de données (par exemple, un fichier Word), retourne une chaîne de caractères (64 dans le cas du Bitcoin). A un fichier correspond un unique hash, une unique empreinte, et il est impossible de retrouver l'information contenue dans le fichier à partir de son hash. Ainsi, la preuve de travail consiste à demander aux mineurs de calculer le hash des données constituées du bloc en cours de création (contenant l'empreinte / hash du bloc précédent), des données du mineur et d'un nombre aléatoire, afin de trouver un hash qui commence par un nombre de zéros défini.

Dans l'exemple suivant, la complexité (nombre de zéros en début de hash requis pour attribuer un hash à un nouveau bloc) est de 10. Le schéma ci-dessous montre l'activité des mineurs pour l'ajout d'un bloc sur la blockchain.

Ainsi l'algorithme proposé est le suivant :

- 1) Calcul de :

$$\text{fonction hash}(\text{Bloc}, \text{infos mineur}, \text{hash bloc précédent}, \text{nbre aléatoire } 1) < C$$

Avec C : la valeur dépendant de la complexité. Par exemple, si la complexité est de 10, il faudra trouver un h inférieur à 0000000000ff. Le calcul s'effectue en hexadécimal (base 16), c'est-à-dire en une base allant de 0 à f. La fonction hash est aléatoire, ainsi la seule méthode de résolution de cette inéquation est de recommencer le calcul jusqu'à trouver la solution.

- 2) Recommencer le calcul de l'inégalité précédente en modifiant uniquement le nombre aléatoire, tant que la condition n'est pas réalisée
- 3) Lorsqu'une solution est trouvée, le bloc ainsi formé peut être envoyé à tous les nœuds du réseau



Figure 5 : Réalisation de la preuve de travail trouvée en N essais

Afin d'arriver au nombre de zéros requis, le mineur doit réaliser un certain nombre de fois le calcul du hash de la combinaison bloc + informations liées au mineur + nombre aléatoire correspondant à l'essai. Une fois que le résultat donne le hash avec la difficulté requise, le mineur qui a réussi l'opération envoie cette information au réseau distribué.

Si plusieurs mineurs arrivent à un résultat à un temps très proche, une nouvelle branche pourra être créée :

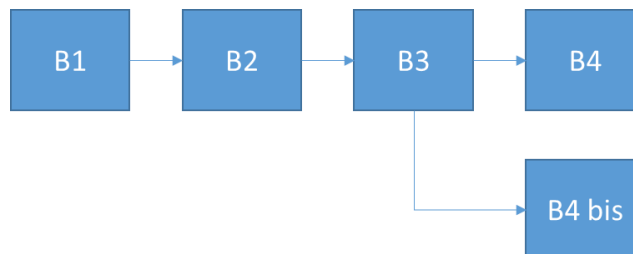


Figure 6 : Exemple d'une nouvelle branche pour la chaîne de M2

Dans ce schéma, on peut imaginer que deux mineurs M1 et M2 ont trouvé un résultat satisfaisant pour le 4^{ème} bloc de cette chaîne, M1 était en avance sur M2 de quelques millièmes de secondes. L'information de la réussite de M1 n'est pas parvenue à M2 à temps, et M2 a trouvé également une solution (un autre hash). B4 représente le bloc miné par M2 et B4 bis, celui miné par M1.

PRINCIPES CLES D'UNE APPLICATION BLOCKCHAIN

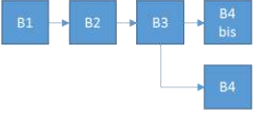
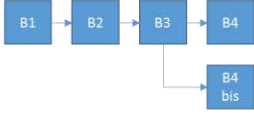
	Les nœuds ayant reçu B4 bis (provenant de M1 en premier)	Les nœuds ayant reçu B4 (provenant de M2 en premier)
Configuration de la blockchain	 <pre> graph LR B1 --> B2 B2 --> B3 B3 --> B4 B3 --> B4bis </pre>	 <pre> graph LR B1 --> B2 B2 --> B3 B3 --> B4bis B3 --> B4 </pre>
% des nœuds	51%	49%

Tableau 1 : Différence de configuration de la blockchain en fonction de la diffusion d'un bloc valide dans le réseau

Dans le cas ci-dessus, il y a 51% de chance qu'un nœud ayant reçu l'information de M1 en premier mine le bloc suivant, et seulement 49% de chance que ce soit un nœud ayant reçu l'information de M2 en premier. Lorsqu'il y a un bloc supplémentaire sur une branche plutôt qu'une autre, alors la branche secondaire est abandonnée, et seule la branche principale prévaut. Par exemple, imaginons qu'un nœud ayant reçu B4bis en premier réalise le prochain bloc, ce qui est le plus probable (51% de chance). Il diffusera donc à l'ensemble des nœuds le nouveau bloc qui aura comme prédécesseur B4bis. Le logiciel du Bitcoin prévoit que seule la chaîne la plus longue sera gardée. Ainsi, la branche contenant B4 sera supprimée. Il y avait 51% de chance que ce scénario arrive.

A quoi sert donc cet algorithme ?

Imaginons qu'un nœud malintentionné (mineur malveillant) veuille modifier une transaction validée par un précédent mineur. Il devrait ainsi ajouter une nouvelle branche qui soit plus longue que celle de la branche principale, contenant l'élément qu'il veut modifier. Ainsi, il devrait générer suffisamment de blocs pour faire de la branche qu'il crée la branche principale. Or la chance de réaliser la création de blocs est proportionnelle à la puissance de calcul des mineurs. Ainsi, un acteur malveillant devrait posséder la majorité de la puissance de calcul disponible sur le réseau. Cet algorithme ne permet pas de vérifier la validité des transactions (d'autres règles présentées dans le paragraphe suivant permettent d'éviter ce problème), mais assure l'impossibilité de modifier les transactions passées d'une part, et la possibilité d'obtenir un consensus sur la branche à suivre en cas de création de branches (appelées également forks). En résumé, il permet d'avoir une chaîne de blocs unique et non modifiable partagée sur le réseau.

D'autre part, la complexité demandée aux mineurs pour les calculs augmente ou diminue selon la puissance globale des mineurs. En effet, tous les 2016 blocs, la complexité est recalculée afin que le temps moyen de génération des 2016 blocs suivants soit de 2 semaines. Un bloc se crée en moyenne toutes les 10 minutes. Les blocs seront donc de plus en plus difficiles à miner au fur et à mesure que les capacités de calcul augmenteront.

I.2.e Le réseau

Les différentes règles suivies par les nœuds du réseau sont :

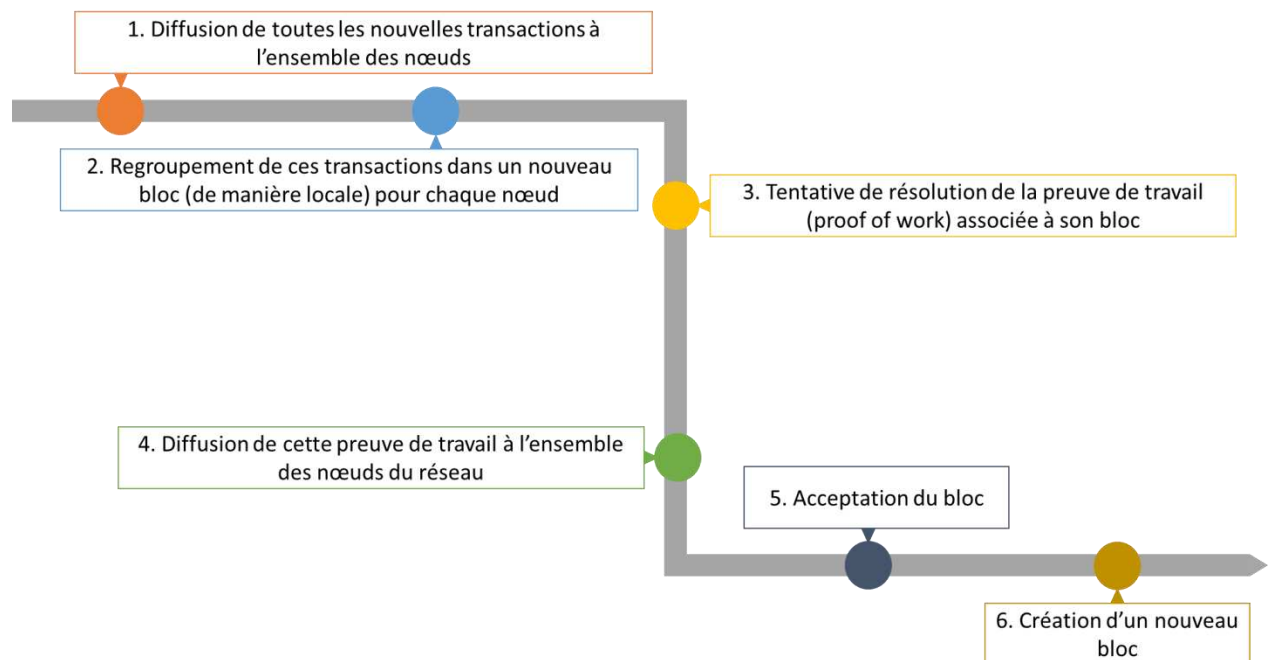


Figure 7 : Règles imposées et respectées par les nœuds du réseau

Les nœuds accepteront le bloc proposé uniquement si les transactions qu'il contient sont valides (par exemple, selon l'historique de la blockchain du Bitcoin, il n'y a pas de transaction de monnaie que l'expéditeur ne possède pas ou plus). L'acceptation d'un bloc s'effectue via le travail du nœud sur un nouveau bloc, en ayant comme prédécesseur le bloc qu'il vient d'accepter.

La chaîne la plus longue est toujours la chaîne qu'il convient de conserver et qui est légitime.

I.2.f Incitation

Afin de récompenser le calcul coûteux en énergie et en temps effectué par le mineur qui a réussi la preuve de travail, la première transaction du bloc créé est une transaction spécifique qui génère une certaine quantité de crypto monnaie appartenant au créateur du bloc. Cette incitation à réaliser le minage permet de pousser les nœuds à participer au réseau, et permet de distribuer la crypto monnaie.

On peut également financer les mineurs par des frais de transaction. Ainsi, une fois qu'une quantité maximale de crypto monnaie déterminée au préalable sera injectée dans le réseau, le système de frais de transaction sera l'unique modèle économique sur lequel se basera les mineurs. La récompense délivrée aux mineurs était de 50 Bitcoins (btc) par bloc miné initialement (en 2008). En 2012, la rémunération a été divisée par 2, soit 25 btc par bloc miné.

Tous les 210 000 blocs minés (soit environ 4 ans), la rémunération est divisée par 2. Ainsi, le minage rapportera de moins en moins de btc et les frais de transaction seront le principal moyen de pouvoir générer de nouveaux Bitcoins.

Le graphique ci-dessous représente le nombre de bitcoins créés en fonction du temps. On remarque notamment que la quasi-totalité des bitcoins sera créée avant 2040, soit environ 21 000 000 de bitcoins.

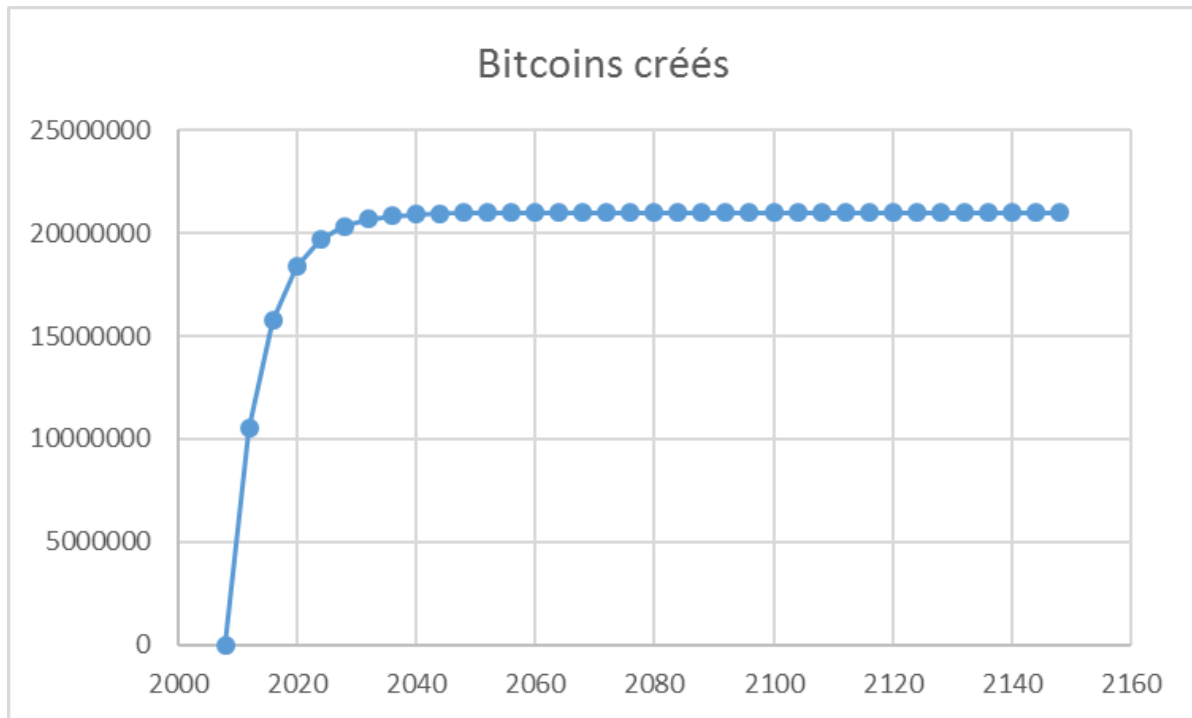


Figure 8: Génération théorique de Bitcoin dans le temps

I.2.g Economiser l'espace disque

On peut aisément comprendre qu'une blockchain peut prendre des proportions, en termes de mémoire, assez impressionnantes. Le système de la blockchain du Bitcoin imaginé par Satoshi Nakamoto prévoit d'économiser de l'espace disque en utilisant des procédés tels que les arbres de Merkle. Lorsque des transactions sont réalisées et confirmées depuis plusieurs générations de blocs successifs, ces dernières peuvent être supprimées des nœuds qui voudraient faire des économies de mémoire. Il existerait ainsi 2 types de nœud différents :

- Un type « nœud complet » qui contiendrait l'ensemble des transactions et des blocs
- Un type « nœud simple » qui contiendrait les derniers blocs validés complets, ainsi que l'empreinte (hash) des transactions et blocs plus anciens

Cela permettrait de vérifier l'authenticité de la blockchain sans avoir forcément l'ensemble des données distribuées sur chacun des nœuds du réseau.

De manière schématique, on obtiendrait ainsi ces deux blockchains différentes :

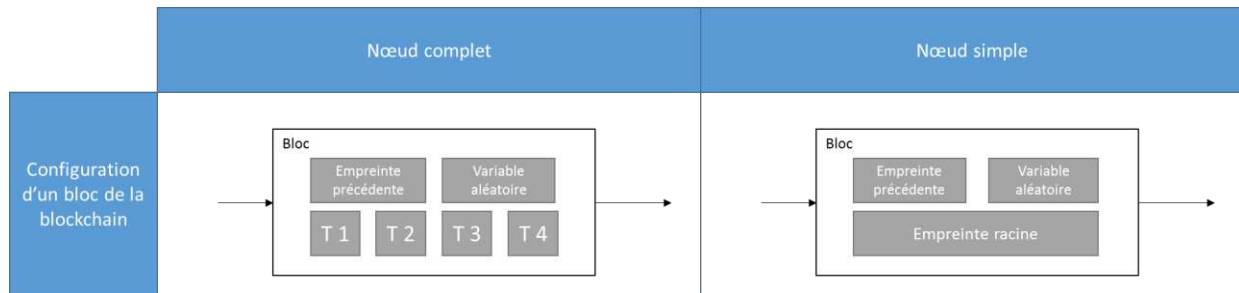


Figure 9 : Différence entre un nœud complet et un nœud simple

On peut considérer que le deuxième nœud correspond à un en-tête de bloc, et non à un bloc entier, puisqu'il ne contient plus l'ensemble des transactions.

Voici comment se calcule l'empreinte racine :

Imaginons que nous avons, dans notre bloc, 4 transactions : T1, à T4.

Posons : $hash(x) = SHA256(SHA256(x))$

Ainsi, notons :

$hi = hash(Ti)$, avec i prenant les valeurs entre 1 et 4.

On obtient ainsi $h1$, $h2$, $h3$, et $h4$

Désormais, posons $h5 = hash(h1+h2)$ et $h6 = hash(h3+h4)$. Le « + » correspond à la concaténation des deux chaînes.

Et enfin, $h7 = hash(h5+h6)$. $h7$ est appelé la racine de Merkle du bloc.

De manière schématique, voici le procédé :

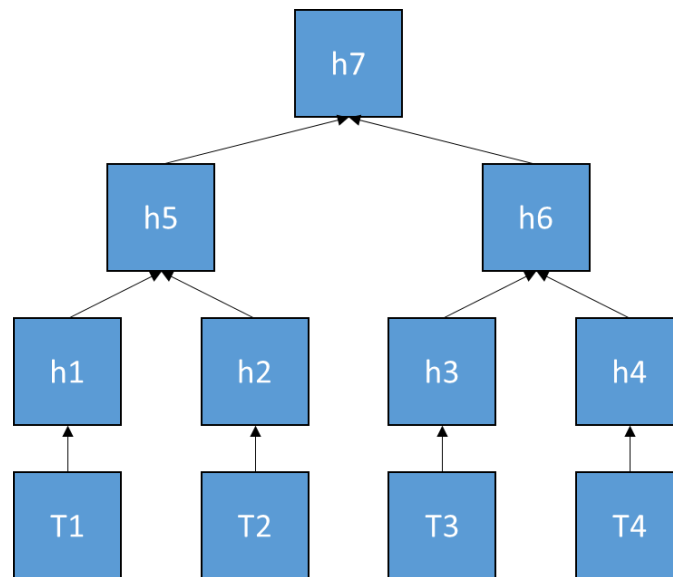


Figure 10 : Calcul de l'empreinte racine, ou racine de Merkle du bloc

Cette technique permettrait ainsi d'économiser de l'espace mémoire sur les nœuds qui le souhaitent. Ci-dessous est présenté un graphique représentant la taille de la blockchain du bitcoin depuis son origine :

Taille de la blockchain
89.83 GB

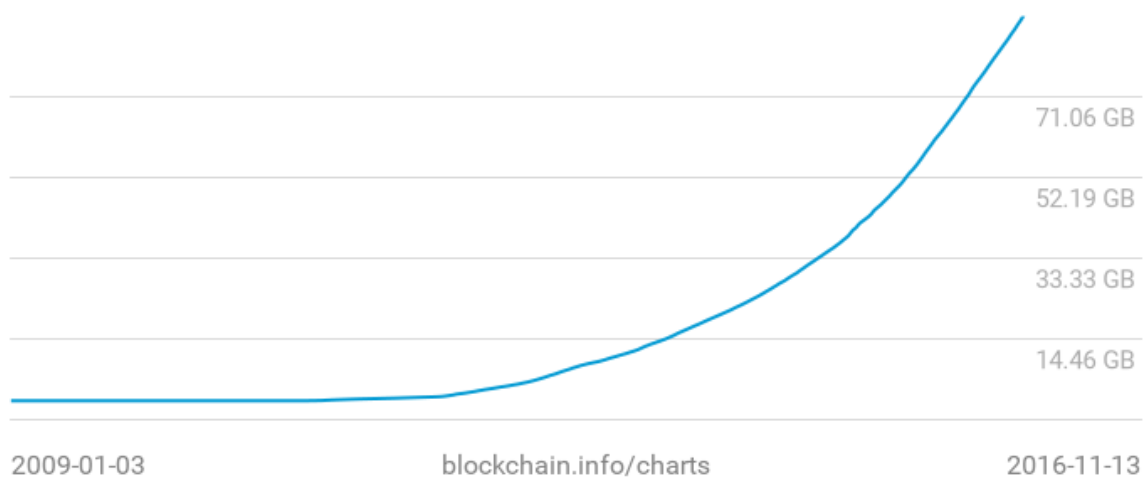


Figure 11 : Evolution de la taille de la blockchain au cours du temps (<https://bitcoin.fr>)

Aujourd'hui, cette technique d'économie d'espace disque n'est pas mise en place.

I.2.h Vérification de paiement simplifié

Ainsi, à partir de ce qui a été vu dans la partie précédente, il est possible de vérifier les transactions en utilisant uniquement les en-têtes des blocs, sur un nœud simple, et non un nœud complet.

Un utilisateur sur un « nœud simple » pourrait conserver uniquement les en-têtes des blocs de la chaîne la plus longue. Cette opération peut facilement être menée à l'aide de requêtes réalisées auprès d'autres nœuds du réseau.

Les nœuds simples ne pourront pas vérifier les transactions, mais compte tenu du fait que les autres les ont acceptées, il considérera que le bloc considéré est valide.

I.2.i Vie privée

Les identités des personnes réalisant les transactions sont gardées secrètes, malgré une diffusion publique des transactions elles-mêmes.

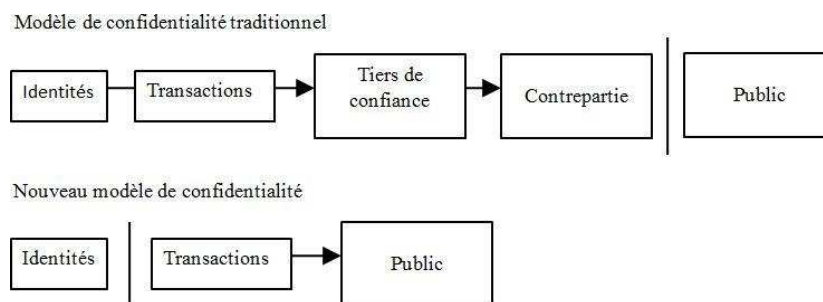


Figure 12 : Modèle de confidentialité de la blockchain (source : http://blog.octo.com/wp-content/uploads/2016/01/bitcoin_fr.pdf)

I.3 - Principes clés d'une blockchain

Dans le paragraphe précédent, nous avons expliqué le fonctionnement technique d'une blockchain particulière, qui est celle du Bitcoin. Cependant, chaque blockchain fonctionne avec des procédés différents, des méthodes de sécurisation différentes. Nous allons donc tenter, dans ce paragraphe, de synthétiser les grands principes techniques qui régissent une blockchain, et ce qui est susceptible d'être modifié. Pour cela, nous allons reprendre chaque étape de l'explication de la blockchain du Bitcoin et en tirer la synthèse. Nous illustrerons par ailleurs les différences entre la blockchain du bitcoin et les autres blockchains à l'aide d'exemples.

Ainsi, nous pouvons énoncer l'ensemble des principes clés sur lesquels repose la blockchain du Bitcoin. Ces principes sont :

- Définition des transactions
- Etapes de validation par le réseau (dont l'horodatage et la proof of work)
- Récompense des mineurs
- Confidentialité

Dans les parties suivantes, nous nous intéresserons à chacun de ces éléments en détournant les principes inhérents à n'importe quelle blockchain.

I.3.a De nombreux objets utilisables par le concept de blockchain

Le type d'objets d'une blockchain peut être variée selon sa nature. L'objet déposé sur une blockchain peut d'ailleurs être autre qu'une transaction (objet dans l'exemple du Bitcoin). L'exemple le plus connu est sans doute celui des smart-contracts.

Un smart-contract est un programme informatique inséré dans un bloc qui s'exécute lorsque certaines conditions sont remplies, ou certains événements se produisent. Cela implique que le système de la blockchain doit permettre de recueillir des informations qui peuvent être en dehors de la blockchain, et qui s'assurent des conditions d'un contrat.

On peut par exemple imaginer une personne qui choisit de donner 1 btc à son frère lorsque ce dernier deviendra père. Ainsi, un smart contract pourra être généré. Un smart contract est rattaché à un compte. Il existe deux types de compte :

- Des comptes détenus par des tiers, qui sont contrôlés et sécurisés via des clés privées
- Des comptes de contrat, contrôlés et sécurisés uniquement par leur code

Un compte de tiers ne peut effectuer une transaction que « manuellement », c'est-à-dire en utilisant sa clé privée. En revanche, dans le cas d'un compte de contrat, chaque fois que ce dernier reçoit un message, son code s'exécute et ses fonctions s'appliquent. Cela peut créer un nouveau contrat, générer une transaction ou encore appeler un autre contrat.

Ainsi, dans notre exemple de don d'un btc à son frère, il faut, pour remplir les conditions, vérifier que le frère du créateur du smart contract a un enfant ou non. Il faut donc une entité, extérieure à la blockchain, qui dépose l'information à une adresse préétablie (dont le contenu sera vérifié à chaque message envoyé à l'adresse du smart contract). Cette entité est appelée Oracle.

En effet, du fait de la caractéristique immuable et compte tenu du besoin de sécurité de la blockchain, cette dernière n'a pas la possibilité d'interagir avec des éléments extérieurs. En revanche, une entité extérieure peut générer une « transaction » sur la Blockchain. Dans notre exemple, l'oracle, qui est un organisme externe automatisé ou non, pourra rechercher sur une base de données regroupant les naissances si le frère a bien un enfant. L'oracle peut très bien être également une personne tierce, ou le créateur du smart contract. Tout dépend du code lui-même. Il écrira ensuite à l'adresse prévue le résultat de sa recherche, ce qui conditionnera le résultat du smart contract.

Le principe de l'oracle et du smart contract peut être schématisé de la manière suivante :



Figure 13 : Illustration de l'exemple de smart contract

On voit ici que le résultat du smart contract dépend principalement des informations fournies par l'oracle. En effet, si l'oracle décide de donner une mauvaise information, le smart contract sera exécuté en prenant en compte cette information erronée. De même, si l'oracle ne délivre aucune information à l'adresse indiquée dans le code du smart contract, alors les conditions de ce contrat ne seront jamais remplies. Ainsi, le système repose de nouveau sur un tiers de confiance.

Plusieurs structures ont ainsi été imaginées afin de parer aux problèmes liés à l'introduction des oracles dans l'écosystème de la blockchain :

- Dans le cas où les données nécessaires sont disponibles sur un serveur, des organisations proposant des services dits « provable-honest » proposent de rechercher les données demandées, accompagnées d'une preuve de sa validité. Par exemple, la société Oraclize, qui fonctionne notamment sur une blockchain appelée Ethereum (dont la crypto monnaie est l'ether) fonctionne selon le schéma suivant :

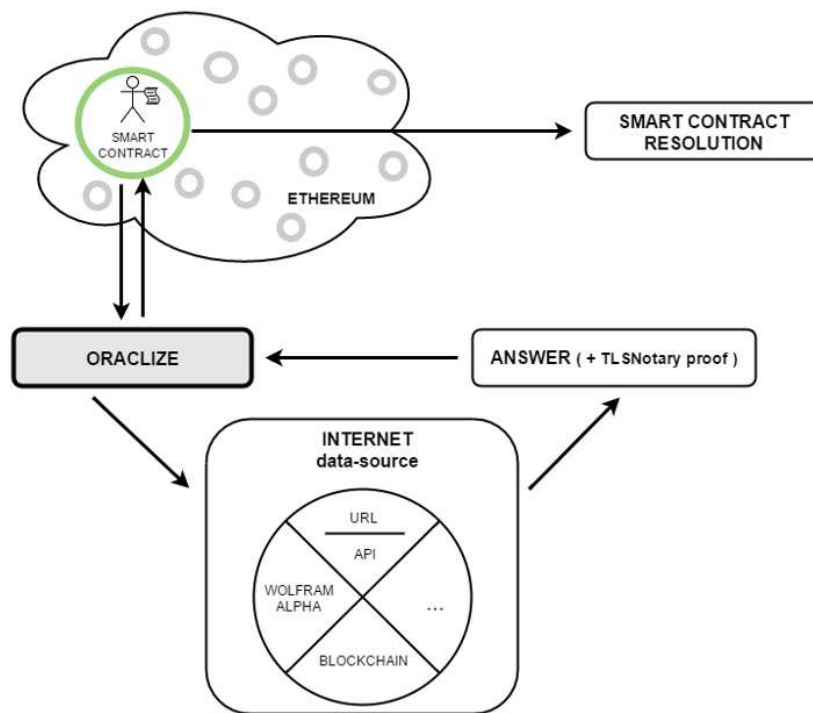


Figure 14 : Fonctionnement d'Oraclize (source : <https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/>)

Oraclize délivre en plus de la donnée une « preuve d'honnêteté » qui permet de savoir si la donnée est bien celle disponible sur le serveur. Cette donnée étant déposée sur la blockchain, elle est facilement vérifiable. Ainsi, si l'oracle donne une information erronée, la réputation de l'oracle sera mise en jeu. C'est donc sur la fiabilité des oracles que se fonde ce type d'organisation.

- Il existe également des oracles basés sur le consensus. Il s'agit d'un principe similaire à celui d'un vote. L'information requise par le smart contract est demandée à un grand nombre de participants, qui sont incités à donner la réponse correcte (par un système de récompense par exemple). Ce système est décentralisé, et par essence, parfaitement compatible avec un système de blockchain.
- On peut également citer des oracles physiques. Certaines informations peuvent être relevées de manière automatique sur des données physiques. On peut imaginer un capteur de température, et un smart contract qui lui est lié. Pour aller plus loin, on pourrait imaginer un ensemble de capteurs physiques qui puisse, en quelque sorte, déceler un sinistre localisé. Ainsi, un smart contract pourrait directement indemniser un assuré ayant souscrit à ce contrat.

On peut trouver également sur la blockchain des organisations particulières, appelées DAO pour Decentralized Autonomous Organization, qui sont des entités autonomes. Nous pouvons illustrer le principe de ces entités par un exemple. Une entité telle que celle-ci pourrait, par exemple, rendre un service d'assurance d'un nouveau type. Tous les participants à cette organisation pourraient verser des mensualités à cette organisation via des smart contracts. Lorsqu'un des participants subit un accident et souhaite être indemnisé, il effectue une demande. Soit le smart contract s'appuie sur des oracles capables de confirmer le sinistre, et ainsi indemnise automatiquement l'assuré, soit l'indemnisation est soumise au vote de l'ensemble des assurés, qui décident, si oui, ou non, l'assuré peut toucher l'indemnisation. Ainsi, chaque participant peut avoir un pouvoir décisionnaire sur les actions des smart contracts. Ainsi, la gouvernance d'une application telle qu'une DAO dépend du ou des smart contracts qui ont été codés.

I.3.b Etapes de validation par le réseau

Dans la description des étapes de validation par le réseau, dans le cas du Bitcoin, l'étape de Proof of Work permet de créer un consensus entre tous les nœuds du réseau pour établir l'historique valide des transactions. Cela permet de prévenir les attaques malveillantes éventuelles, et de choisir une branche lorsqu'il y en a deux qui sont créées. La preuve de travail repose principalement sur le fait qu'il faut prouver qu'on a utilisé assez d'énergie et de ressources de calcul. Cependant, cette méthode n'est pas la seule proposée par les créateurs de blockchain.

Une autre méthode répandue, qui n'est pas celle explicitée dans le papier de Satoshi Nakamoto, s'appelle Proof of Stake, ou preuve d'enjeu. Cette méthode repose sur le fait d'avoir de la crypto monnaie.

Comparons ces deux méthodes pour mieux expliquer le proof of stake :

- Preuve de travail / Proof of Work : imaginons que chaque nœud ait la même puissance de calcul que les autres. Chaque nœud lance un dé à la même fréquence que les autres pour obtenir le chiffre souhaité (imaginons un 6). Lorsqu'un nœud obtient un 6, il le dit à tous les autres, et son bloc est ajouté à la chaîne. Ainsi, celui qui possède le plus de nœud possède le plus de chance de réussite. Maintenant, si les nœuds ont des puissances de calcul différentes, celui qui possède les nœuds, qui, en cumulé, ont le plus de puissance, aura le plus de chance de réussite (c'est comme s'il augmentait sa fréquence de lancer). On peut en conclure que la chance d'être le mineur qui réussit l'ajout d'un bloc est proportionnel théoriquement à la puissance de calcul possédée.
- Preuve d'enjeu / Proof of Stake : de la même manière, le concept de cette méthode est que la réussite d'obtenir le minage d'un bloc dépend proportionnellement de l'argent qu'on a sur son compte. Par exemple, si un compte possède 10% de la monnaie totale dans le système, alors il aura 10% de chance de proposer en premier le bloc à ajouter. Cette méthode a pour avantage de consommer beaucoup moins d'énergie, cependant elle est réputée pour être moins sécurisée que le Proof of Work.

Il existe de nombreux autres types de preuves, avec, pour chacune d'entre elles, des avantages et des inconvénients. Elles ne seront pas présentées ici.

D'autres différences sont aussi remarquables, comme le temps de génération d'un nouveau bloc (12 s pour Ethereum contre 10 min pour Bitcoin).

I.3.c Récompense des mineurs

Dans le cas du Bitcoin, les récompenses sont divisées par 2 tous les 4 ans environ. Ce principe n'est pas le cas pour l'ensemble des blockchains. Ethereum récompense de la même manière tous les ans l'ensemble des mineurs ayant participé à l'ajout de bloc, et ceci pour toujours (15,6 millions d'éther sont générés tous les ans).

I.3.d Confidentialité

Le concept originel de la blockchain incluait une validation prenant en compte l'ensemble des nœuds du réseau. Entre autres, la blockchain elle-même, ainsi que la validation des blocs qui la constituent, s'effectuait de manière totalement partagée, et donc publique.

Certaines institutions, intéressées par cette nouvelle technologie, ont cependant été méfiantes quant au caractère public proposé par la blockchain à son état d'origine.

De nouveaux concepts ont ainsi émergé, suite à ce besoin identifié. Il s'agit des blockchains « privées », ou « de consortium ».

Une blockchain de consortium est une blockchain qui se base sur un procédé de validation des blocs qui est restreint à un certain nombre de nœuds définis. La capacité de lire l'ensemble de la blockchain peut être réservée à certains nœuds particulier, la consultation sera donc privée ; elle peut être aussi disponible pour l'ensemble des nœuds, auquel cas la consultation de la blockchain est publique. La blockchain peut également être séparée en plusieurs parties : certaines données peuvent être consultées publiquement, tandis que d'autres ne sont disponible que sur un réseau privé, la consultation est, dans ce dernier cas, hybride.

Une blockchain privée, quant à elle, réserve le processus de validation à un acteur unique, les consultations pouvant être privées, publiques, ou hybrides.

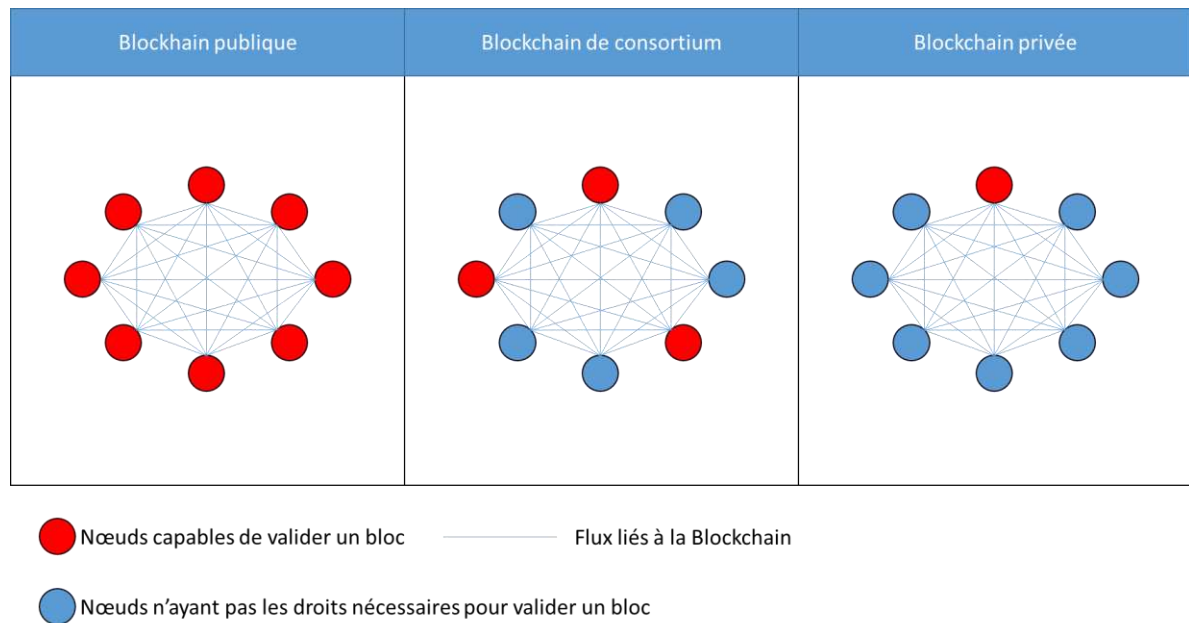


Figure 15 : Types de blockchain selon le mode de validation de blocs

Chaque point dans ce schéma représente un nœud du réseau. On peut y voir la différence de gouvernance entre les différents types de blockchain (publique, privée, ou de consortium).

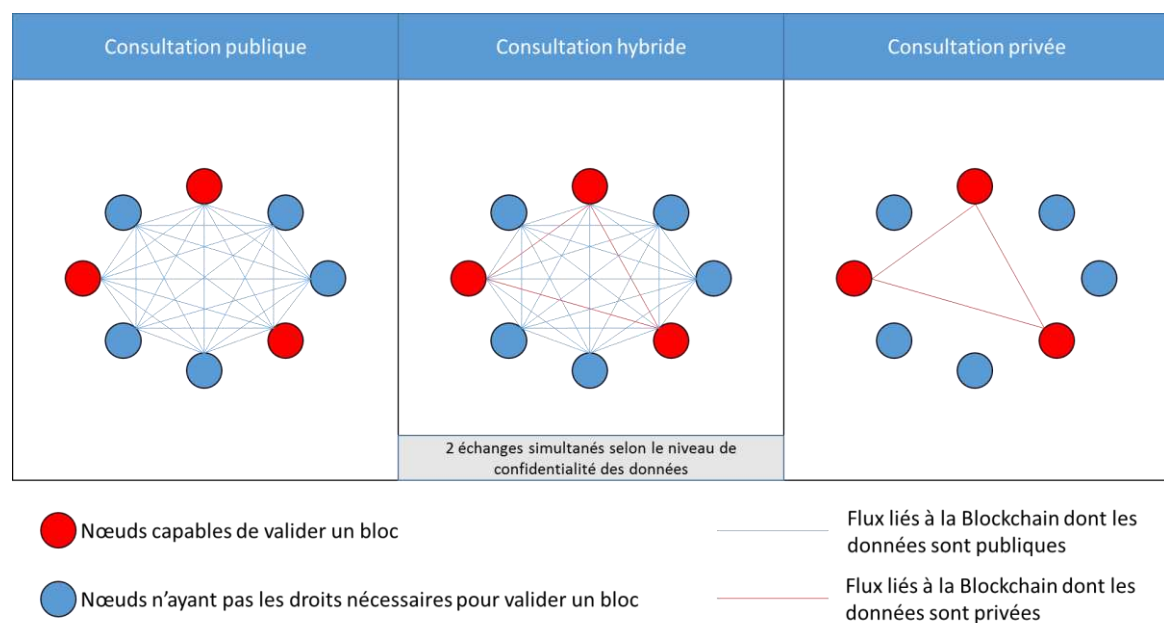


Figure 16 : Partage des données d'une blockchain de consortium sur le réseau

Des schémas similaires pourraient être faits pour la blockchain privée ou publique. Pour une blockchain publique, les consultations sont publiques uniquement.

I.4 Synthèse du concept de la blockchain

A partir de l'étude menée dans les précédentes parties, on peut dégager plusieurs points clés liés à cette nouvelle technologie qu'est la blockchain.

Les éléments clés sont dans un cas général :

- Une information répartie entre tous les participants à la blockchain :
 - Un historique disponible pour tous (dans le cas d'une blockchain publique)
 - L'émission des transactions accessible à tous
 - Une validation réalisée par n'importe quel nœud (dans le cas d'une blockchain publique)
- Un système de comptes et de nœuds :
 - Des comptes de tiers et des comptes de contrats, les uns sécurisés par une clé privée, les autres par le code qui les caractérise
 - Des nœuds qui participent directement système distribué de la blockchain et permettent l'ajout de transactions à celle-ci
- Un système de preuve à fournir par les nœuds afin d'inscrire un nouveau bloc dans la blockchain, qui se caractérise par :
 - Une résolution d'équation, ou d'inéquation
 - Une difficulté (qui peut varier au cours du temps pour s'adapter à la situation)
 - Une légitimité à pouvoir déposer un bloc sur la blockchain

Ces principes généraux sont malléables et peuvent être adaptés à des situations particulières. On peut citer comme exemple la différence entre les blockchains privées, publiques, ou de consortium.

La partie suivante s'attachera à répondre à la question suivante : en quoi cette technologie, ainsi que les éléments cités dans la première partie sont disruptifs ? Et quels sont les exemples qui permettent de déceler de possibles changements radicaux dans le fonctionnement actuel de certaines activités.

II. Une nouvelle façon d'appréhender des besoins d'entreprise

Dans cette partie, nous tenterons de décrire ce que la technologie de la Blockchain pourrait permettre en termes d'application, en se basant sur des cas d'usage précis. Nous essayerons par la suite de dégager les grands types d'utilisation théoriques de la blockchain.

II.1 Horizon des possibilités basées sur des « use cases »

II.1.a Document de base permettant de mener l'analyse

Nous allons partir d'un document réalisé par « Let's Talk Payments » qui a recensé l'ensemble des use cases associés à la Blockchain :

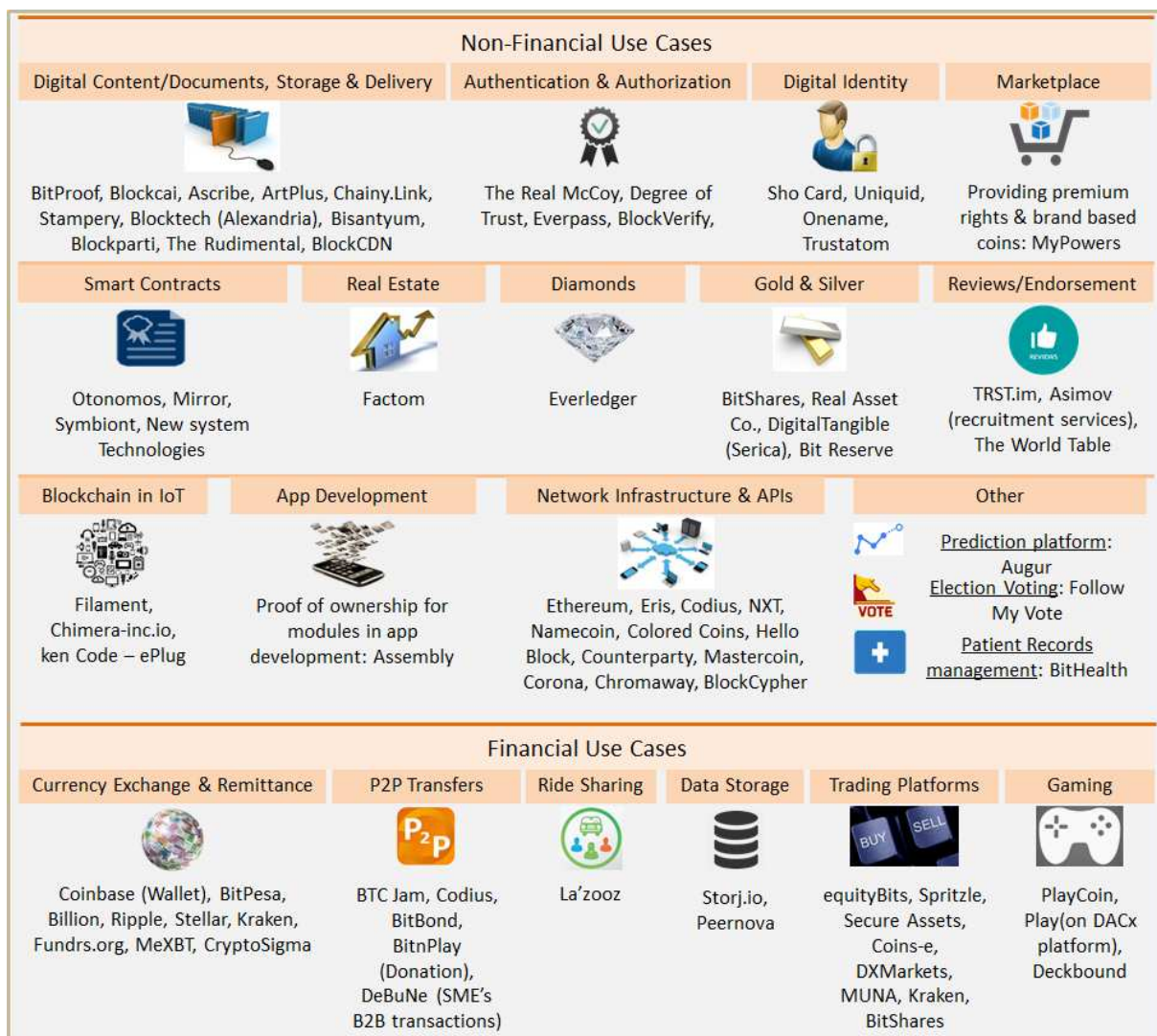


Figure 17 : Ensemble des use cases associés à la Blockchain (<https://letstalkpayments.com/blockchain-use-cases-part-ii-non-financial-and-financial-use-cases/>)

A partir de ce recensement, nous allons d'abord expliciter chacun des items présents sur cette représentation avant d'essayer de la synthétiser en grandes idées directrices (voir la partie II.2).

II.1.b Digital Content / Documents, Storage & Delivery

Ces cas d'usage rassemblent les activités de digitalisation de documents ou de contenus (de tout type), d'envoi, puis de stockage. Cela peut se traduire par exemple par la génération d'un diplôme officiel, de le numériser et de l'envoyer à un élève l'ayant obtenu. Ainsi, l'envoi du document sur la blockchain constitue une preuve de la validité du diplôme. Cette preuve est infalsifiable, et est, de manière intemporelle, sur la blockchain. Cela peut également convenir pour de nombreux autres types de documents (brevets, propriétés intellectuelles...).

A titre d'exemple, Bitproof propose à ses clients d'inscrire leurs contrats indéfiniment sur une blockchain. Cette start-up a notamment pour but de lutter contre la fraude aux diplômes. De la même manière, l'entreprise Seezart génère des certificats d'authenticité d'œuvres d'art, et de permettre de vérifier la provenance d'une œuvre dans le registre décentralisé et mondial que constitue la blockchain.

D'une façon plus générale, tous les types de documents sont susceptibles d'être certifiés à l'aide d'une blockchain, et de nombreux services émergent dans ce sens.

En France, une école d'ingénieur, l'ESILV, va certifier ces diplômes à l'aide de cette solution.

II.1.c Authentication & Authorization

Une application de la blockchain peut également être l'identification et la certification de biens ou de transactions.

L'entreprise Block Verify est une société qui repose sur le potentiel de la blockchain afin d'implémenter des mesures permettant notamment d'endiguer des problèmes liés à la contrefaçon. Leur service est basé sur quatre facteurs clés de succès :

- Aider les entreprises à identifier des biens contrefaits
- S'appuyer sur la blockchain, ce qui permet d'avoir un environnement ne permettant pas, par essence, la reproduction de produits, et s'abrogeant de la notion de confiance
- Proposer à l'entreprise un moyen de création d'un registre qui leur est propre, enregistrant chaque produit et permettant leur supervision
- Proposer une solution globalisée, compte tenu du caractère connecté de la blockchain

Les produits que Block Verify propose d'authentifier peuvent être de plusieurs types :

- Produits de contrefaçon : déjà en possession d'un utilisateur, et qui est reconnu comme étant contrefait

- Produits déroutés : le système est capable d'identifier un produit dont la destination prévue a été modifiée
- Marchandise volée : le système peut tracer et localiser ces produits
- Transactions frauduleuses : traçage de transactions frauduleuses de tout type sur le système

Les cas d'usage identifiés par l'entreprise sont, entre autres, des cas liés à l'industrie pharmaceutique (permettre au consommateur de s'assurer de la provenance du produit pharmaceutique), liés aux produits de luxe, aux diamants, ou encore aux équipements électronique (smartphone...).

Ci-dessous sont présentés les services de vérification des blocs :

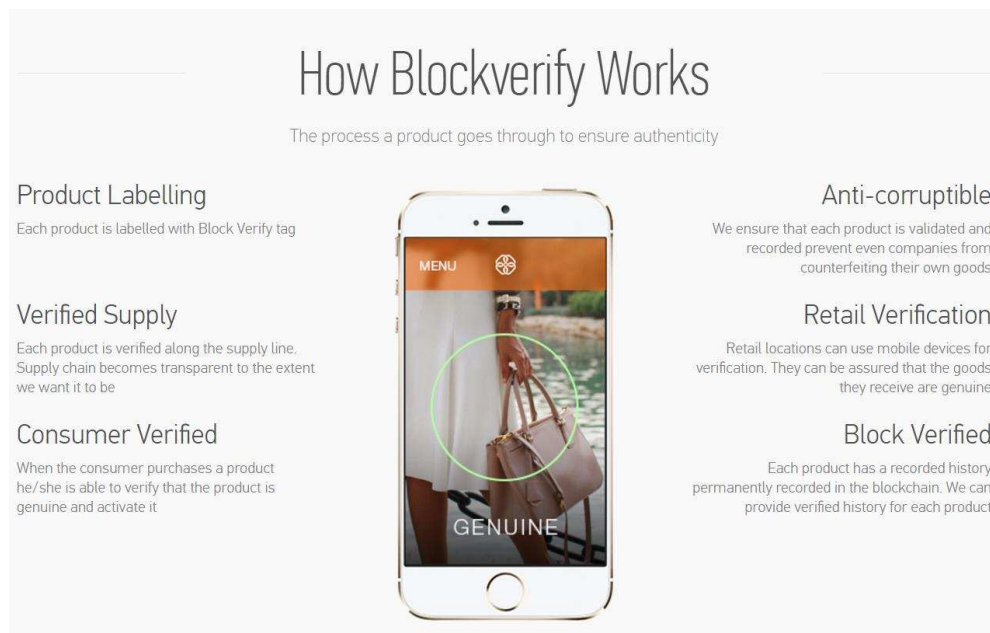


Figure 18 : services proposés par BlockVerify (blockverify.io)

II.1.d Digital Identity

Certains autres services développés par des entreprises utilisant le concept de la blockchain sont centrés autour de la gestion des autorisations et des authentifications. En effet, il est tout à fait possible d'utiliser la blockchain afin de s'identifier sur différents sites, ou pour partager son identité.

L'entreprise américaine OneName propose de créer une identité sur la blockchain, qu'on est susceptible de réutiliser lorsqu'on veut s'authentifier, ou s'inscrire à un nouveau service. On peut comparer cette solution à la solution Facebook Connect, qui permet de s'authentifier avec les données de connexion de Facebook sur des applications tierces. Cependant, dans le cas de OneName, les informations d'identification ne sont pas stockées sur les serveurs d'une entreprise en particulier, mais sur la blockchain elle-même de manière cryptée. Ainsi, seul le propriétaire de cette identité peut y accéder, à l'aide de sa propre clé

privée. OneName crée une adresse contenant l'identité sur la blockchain, et à la possibilité de transmettre cette adresse à un demandeur. OneName a changé de nom, et s'appelle désormais BlockStack, dont l'architecture et le principe est présenté ci-dessous :

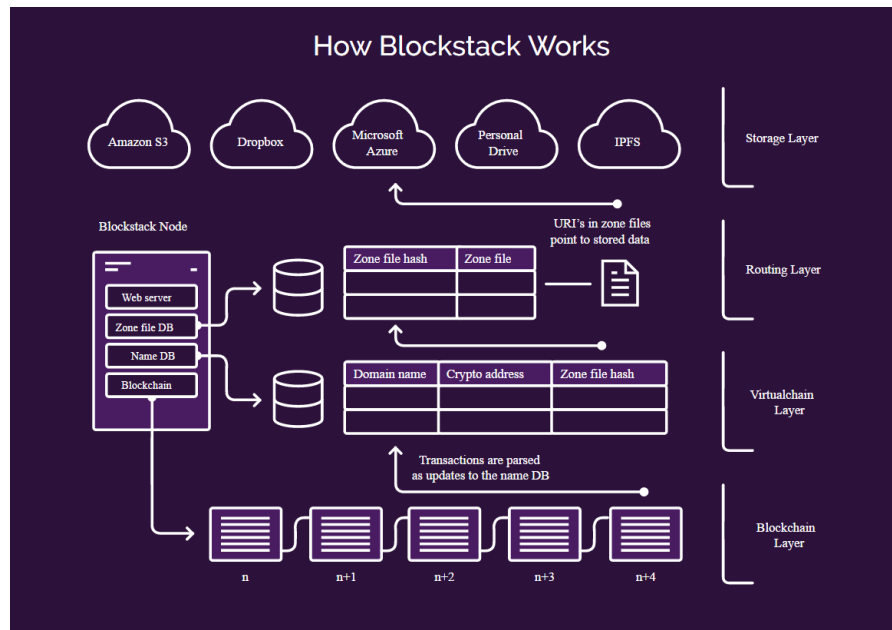


Figure 19 : Fonctionnement SI de Blockstack (blockstack.org)

II.1.e Marketplace

Certains fondateurs de start-up se sont penchés sur l'achat de biens de consommation sur internet. A l'instar d'eBay, la société MyPowers utilise la blockchain du Bitcoin afin de créer un eBay-like, en utilisant de la monnaie virtuelle. L'entreprise permet d'avoir un système de transactions sécurisées et rapides, et qui sera susceptible d'intéresser massivement de potentiels utilisateurs. Tout ce qui peut être une transaction sur internet pourrait être vendu par l'intermédiaire de cette société reposant sur la blockchain du Bitcoin.

Par ailleurs, l'entreprise Ledgys, à travers son produit Ledgys Smart Networks (LSN), permet de créer un réseau de données, sécurisées et qui peuvent faire l'objet d'un audit. Elle permet donc à ses clients, voulant se lancer dans une « compétition collective », d'échanger ou de vendre des données et des informations. A ce titre, le produit LSN permet de contrôler l'accès aux données, de permettre un audit, et de les sécuriser. Ledgys propose donc à ses clients une plateforme permettant de créer leur propre « business applications », avec des communautés associées. Cela permet de créer de nouvelles places de marché. A titre d'exemple, la société Ledgys travaille sur le cas d'entrepôts de codes informatiques mutualisés entre plusieurs acteurs, chaque acteur étant récompensé pour sa contribution par la communauté.

II.1.f Smart Contract

Nous avons déjà vu dans la partie I la définition et le fonctionnement d'un smart contract. Nous allons donc voir ici son application concrète. Rappelons le principe d'un smart contract. C'est un code informatique lié à un compte de la blockchain. Ce code possède des instructions et fonctions particulières qui permettent d'établir des règles de fonctionnement. Par exemple, lorsque quelqu'un envoie un message sur l'adresse du compte lié au code informatique, ce dernier s'exécute avec, comme paramètre, le message envoyé.

L'entreprise Otonomos aide les entreprises se lançant dans l'aventure de la blockchain à créer une entité juridique à Singapour, en remplissant un questionnaire en ligne. L'entité créée est alors possédée par le ou les détenteurs à l'aide d'une adresse cryptographique et d'une clé privée et publique. Otonomos propose ainsi un système de gestion P2P des actions ou parts de l'entreprise. Ce système peut également établir des règles de gouvernance via l'implémentation de smart contracts.

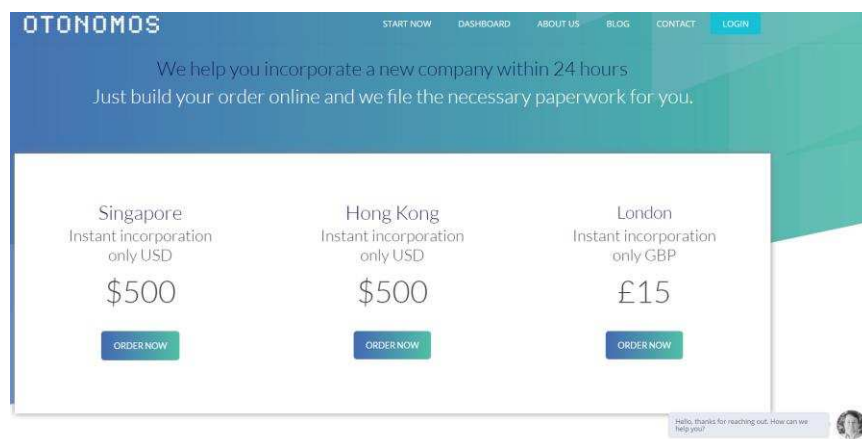


Figure 20 : Offre de création d'entreprise se basant sur la technologie Blockchain (otonomos.io)

D'autre part, la société Symbiont a établi une offre permettant de gérer des transactions dans le secteur financier de manière automatique, à l'aide des smart contracts. Par exemple, dès l'émission d'un titre sur le registre de Symbiont, ce dernier devient autonome, et permet ainsi de se passer de fonctions middle ou back office. Cette société, qui s'est associée à Gemalto afin de sécuriser et chiffrer les données de transaction, permet ainsi d'automatiser bon nombre de processus manuels en vigueur encore aujourd'hui dans le secteur financier.

II.1.g Real Estate

La start-up Factom, spécialisée dans la blockchain, serait prête à signer un contrat avec le Honduras afin de créer un cadastre officiel et numérique, fondé sur la Blockchain.

D'autres pays sont également très intéressés par cette nouvelle technologie pour y héberger leur système de gestion du cadastre, notamment pour des raisons de transparence et de sécurité. Le Ghana est un exemple : près de 90% des terres rurales ne sont pas inscrites

dans un cadastre, et des citoyens n'ont pas encore d'adresse officielle. Cette situation pose de réels problèmes administratifs et économiques, au Ghana ou dans d'autres pays. Par exemple, l'absence de titres de propriété rend impossible l'hypothèque. Ainsi, le projet Bitland a été reconnu par le gouvernement ghanéen pour pallier ce problème.

II.1.h Diamonds

Everledger est une jeune société spécialisée dans la protection des diamants. Elle intéresse notamment les compagnies d'assurance. L'objectif est de créer un registre complet de toutes les pierres précieuses afin de lutter efficacement contre le vol et la fraude (qui représente un coût de 50 milliards de dollars chaque année pour les assureurs). Le principe de fonctionnement d'Everledger est simple : chaque pierre soumise à la société possède un certain nombre d'informations (numéro de série, informations physiques, identité du propriétaire...), qui seront enregistrées sur une blockchain. Si un vol est commis, et que le diamant est retrouvé, il pourra alors être restitué à son propriétaire. 850 000 diamants devraient être prochainement enregistrée dans la blockchain.

En réalité, ce besoin aurait pu être traité à l'aide d'une base de données commune à l'ensemble des assureurs. Cependant, cela n'a jamais été fait. La blockchain et l'engouement pour cette nouvelle technologie est ainsi une opportunité de répondre au besoin des assureurs, même si le fait d'utiliser la blockchain n'est en rien une nécessité.

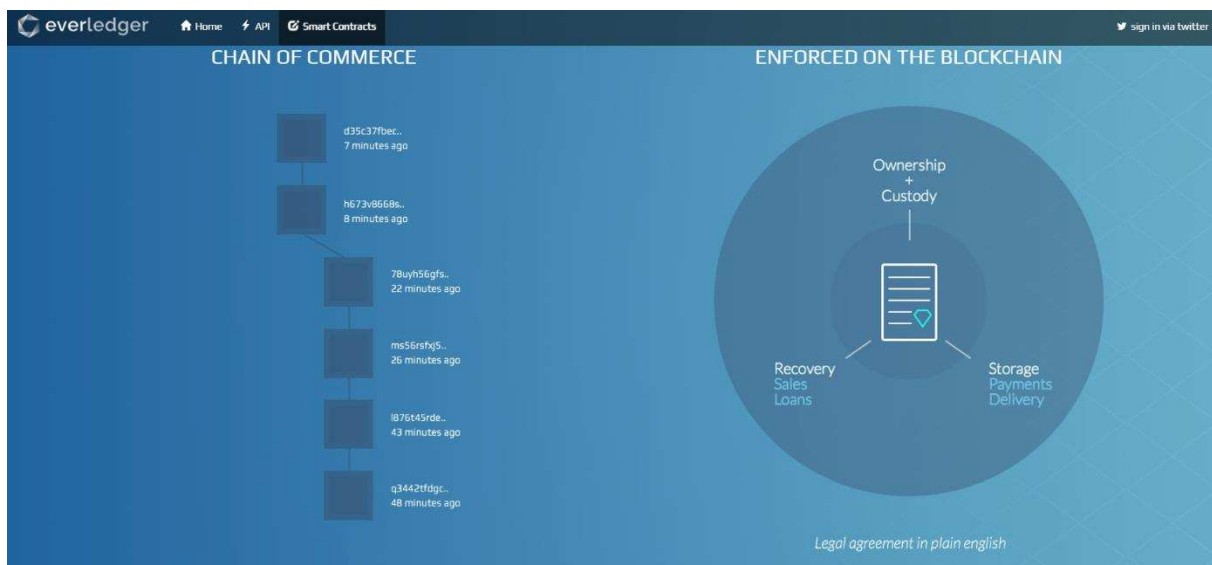


Figure 21 : Liste des derniers diamants inscrits sur la Blockchain, disponible sur www.Everledger.io

II.1.i Trading Platforms

BitShares est une DAC (Decentralized Autonomous Company) qui met en relation des potentiels vendeurs et acheteurs d'assets financiers. Le principe du BitShares est que les

assets échangés sur les marchés dédiés à ces échanges possède des valeurs qui fluctuent en fonction des marchés financiers réels.

Prenons un exemple. Un asset échangé par le système de BitShares s'appelle un BitAsset. Par exemple, le BitUSD représente un US Dollar. Un BitUSD n'est pas un USD. C'est une crypto-monnaie dont la volatilité du cours est celui de la valeur de référence (ici l'USD). Pour le BitGold, le cours est calqué sur celui de l'or, pour le BitSilver, sur celui de l'argent...

Ainsi, les BitAssets sont des actifs financiers fictifs, qui ont une correspondance avec le BitShares, la crypto-monnaie englobant l'ensemble des assets. Avec des BitShares, on peut acheter toutes les sortes de BitAssets. L'objectif est donc de faire de la spéculation sur les assets afin d'augmenter sa quantité de BitAssets ou de BitShares. Ainsi, si suffisamment de personnes utilisent ce système de BitAssets, la monnaie (le BitShare) pourrait être utilisée lors de transactions réelles, à l'instar du Bitcoin.

II.1.j Reviews / Endorsement

La Blockchain peut également être utilisée afin de recueillir les approbations d'expert concernant le niveau d'une personne. C'est ce que propose la start-up Asimov. Elle met en relation, via une plateforme (du type LinkedIn par exemple), des personnes qui demandent une certification de compétence et des experts du domaine. Seul un expert du domaine peut certifier l'aptitude d'une autre personne à être experte dans ce domaine. Cette start-up en est pour l'instant à l'état de projet, mais espère récolter des fonds, petit à petit. Ces certifications passent par une certification dans une blockchain, pour permettre l'assurance d'un historique fiable et public.

II.1.k Blockchain in IoT

L'IOT (Internet of Things) est l'appellation anglophone caractérisant les objets connectés. Aujourd'hui, la plupart du temps, les objets connectés sont des technologies avancées dont les données sont remontées de manière centralisée vers une autorité, qui est en général, l'éditeur de l'objet en question. Ainsi, ce modèle est en opposition avec le modèle théorique de la blockchain. L'activité de ces objets connectés pourrait être stockée directement dans une blockchain afin d'assurer sécurité et traçabilité. Il s'agirait ensuite de pouvoir remonter les données et de pouvoir les utiliser, à l'aide d'interfaces adaptées. D'autre part, l'intégration des données d'objets connectés dans une blockchain pourrait permettre d'assurer la confidentialité des utilisateurs d'objet. En effet, même si sur une blockchain publique, l'ensemble des données est public, l'identité d'un compte de tiers (donc a fortiori d'une personne) est chiffrée et donc l'identité d'une personne est impossible à déterminer. Les données visibles réellement diffusées seront choisies par l'utilisateur de l'objet.

Ainsi, IBM a imaginé de construire une machine à laver capable d'établir son besoin en détergent en toute autonomie, et de contacter le fournisseur le plus proche afin de se réapprovisionner. Cela requiert donc un contrat entre le fournisseur et la machine elle-même. Deux points majeurs permettent ainsi l'autonomie de la machine : la prise de décision, et l'échange d'information. Ceci peut être géré par des smart-contracts. IBM a également une plateforme complète permettant de lier les IoT à une blockchain, ce service s'appelle IoT Watson Blockchain.

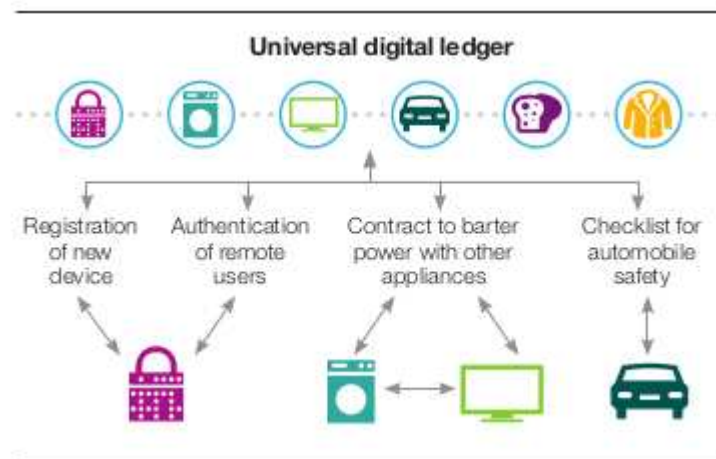


Figure 22 : Offre IBM pour la communication des Objets Connectés utilisant la technologie Blockchain (ibm.com)

II.1.1 App Development

La blockchain peut également avoir un impact sur le développement d'application. Par exemple, la start-up Assembly a mis en place une plateforme permettant à des ingénieurs, des développeurs, des marqueteurs, des designers, et d'autres de collaborer dans le cadre d'un projet, et, à la fin de chaque mois, chaque contributeur est récompensé en fonction de son apport sur le projet. Ainsi, chaque contributeur peut, via cette application utilisant une blockchain, s'assurer de la paternité d'une partie d'un projet, ce qui conditionne ses gains finaux. Il s'agit donc ici de certifier et de rétribuer au prorata du travail fourni, avec preuve à l'appui.

II.1.m Network Infrastructure & APIs

Ce type d'application de la blockchain constitue le socle de base permettant l'utilisation du procédé de Blockchain. Un exemple, dont nous avons parlé en partie I, est celui d'Ethereum. Ethereum est une chaîne de blocs publique susceptible d'intégrer des smart-contracts. Ethereum possède également une monnaie qui lui est propre, appelée Ether. Le premier bloc de la chaîne est créé en 2015 et vend 60 000 000 d'Ether (Eth) sous forme de prévente, et 12 000 000 Eth aux programmeurs. Tous les Ethers suivants créés le seront via le procédé de minage. Ethereum permet à ses clients d'utiliser une plateforme afin d'effectuer

des échanges, à l'aide notamment de smart-contracts, qui automatisent la manière dont sont gérées les transactions.



Figure 23 : Logo d'Ethereum, un des acteurs principaux dans le domaine des Blockchains

Counterparty est une initiative qui ressemble à Ethereum, puisqu'elle offre une plateforme permettant de créer des Assets, qui possède sa propre monnaie, et qui permet l'implémentation de smart-contracts dans la chaîne qu'elle utilise : la blockchain du Bitcoin. Ainsi, Counterparty est une alternative à la plateforme utilisée par Ethereum, mais en utilisant la blockchain du Bitcoin.

II.1.n Currency Exchange & Remittance

La blockchain peut permettre les transactions internationales impliquant des monnaies différentes. Par exemple, la société Bitpesa s'est intéressée à la conversion et aux échanges de monnaies Bitcoins, et de monnaies locales africaines (Kenya, Nigeria, Uganda...). Elle propose une plateforme permettant de convertir des monnaies digitales en monnaies locales. Elle possède notamment des partenaires dans le secteur bancaire.

Kraken est un exemple de plateforme de trading. En effet, Kraken met à la disposition de ses souscripteurs l'ensemble des données nécessaire au trading de Bitcoins.

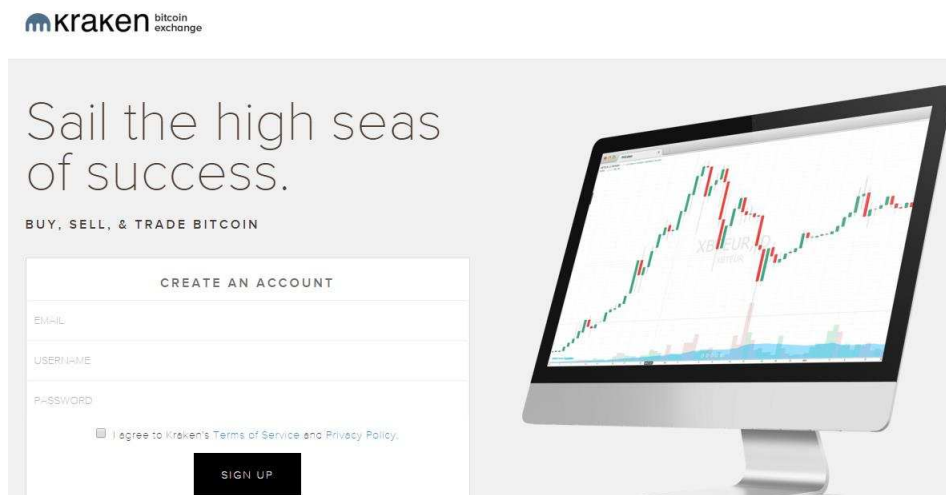


Figure 24 : Souscription à l'offre de Kraken (kraken.com)

Ripple est également un exemple d'échange de monnaie. En réalité la société Ripple a développé un protocole de paiement et un réseau d'échange qui leur est propre. L'objectif originel était de permettre à toute communauté de créer son propre système monétaire. Désormais, Ripple propose à ses clients du secteur bancaire une solution compétitive de transferts de fonds internationaux.

II.1.o P2P Transfers

Les transferts de pairs à pairs sont la fonctionnalité initiale prévue par la blockchain du Bitcoin. C'est en ce sens que certaines entreprises se sont par exemple lancées dans des activités de Crowdfunding ou de Crowdlending. En effet, l'entreprise BitBond a créé une interface entre emprunteurs et bénéficiaires. De la même manière Chroma.fund permet de mettre en contact des start-ups, qui recherchent des investisseurs dans leur projet entrepreneurial, et des investisseurs potentiels. Cependant, les investisseurs ne feront pas l'acquisition de parts de l'entreprise qu'ils financent, mais pourront récupérer, en fonction de leur mise, une part des revenus futurs de l'entreprise. Le système se base également sur l'utilisation de smart-contracts, qui permet d'assurer la rémunération automatique des investisseurs si un certain seuil de bénéfice est atteint.

II.1.p Ride Sharing

Une entreprise israélienne tente de renouveler le modèle, déjà révolutionnaire il y a quelques temps, d'Uber et de BlaBlaCar. En effet, cette start-up propose un service de covoiturage basé sur la blockchain. Ce service serait détenu par la communauté d'utilisateurs de la plateforme/application. Les conducteurs d'automobile peuvent, via ce service open source, se connecter au réseau en temps réel et trouver des covoitureurs sans passer par un intermédiaire, puisque la plateforme est autogérée. Des jetons, appelés « zooz » sont utilisés comme monnaie de l'application.

Afin d'obtenir un succès grandissant, la rémunération des conducteurs diminue avec le nombre de conducteurs total. Ainsi, la Zooz pense pouvoir impliquer de nombreux « early-adopters » pour permettre à l'application/plateforme de se développer et d'atteindre sa taille critique. L'application est déjà disponible sur mobile Android, et il est possible d'avoir des jetons « zooz » en étant conducteur.



Figure 25 :
L'application La'Zooz

II.1.q Data Storage

De nombreuses entreprises sont intéressées par l'activité d'hébergement, de cloud computing, d'offres d'applications disponible directement par navigateur (PaaS). En réalité,

les principaux acteurs du secteur louent leurs Data centers aux entreprises ayant besoin d'entrepôts de données, de machines virtuelles, ou encore d'applications spécifiques. Le service proposé par la start-up Storj Lab est d'inscrire les fichiers voulus sur la blockchain après les avoir encryptés. Elle met également à la disposition de ses clients un panel d'applications décentralisées. Certaines entreprises ont d'ailleurs déjà utilisé l'API disponible par Storj Lab pour créer des applications de pdf Viewer, Video & Music player, toutes disponibles sur le cloud-blockchain.

```
$ storj add-bucket cats
[info] ID: 573b4ce25da55fc8715b4c5a, Name: cats, Storage: 10, Transfer: 30
$ storj upload-file 573b4ce25da55fc8715b4c5a cat.jpg
[...] > Enter your passphrase to unlock your keyring > *****
[info] Generating encryption key...
[info] Encrypting file "cat.jpg"
[info] Encryption complete!
[info] Creating storage token...
[info] Storing file, hang tight!
[info] Encryption key saved to keyring.
[info] File successfully stored in bucket.
[info] Name: cat.jpg, Type: image/jpeg, Size: 8388624 bytes, ID: 574733fb705cbc353c48eef7
```

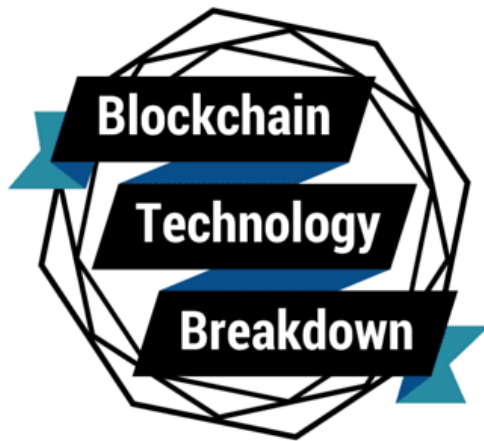
Figure 26 : Exemple de code permettant de stocker un fichier sur ce serveur

II.1.r Gaming

De nombreux jeux basés sur la technologie de la Blockchain existent et peuvent se retrouver sur internet. Les jeux qu'on peut généralement trouver sont des jeux de hasard, comme le lancer de dés, ou des jeux de casino. On peut imaginer que des smart-contracts basés sur une blockchain peuvent s'exécuter selon les règles d'un jeu spécifique. Ainsi, seuls les joueurs pourront s'échanger des montants, et ensuite, l'échange ne se fera qu'entre membres de la communauté, et non plus avec l'intermédiaire d'une plateforme payante. On peut par exemple imaginer un jeu de poker fonctionnant sur la base de smart-contract.

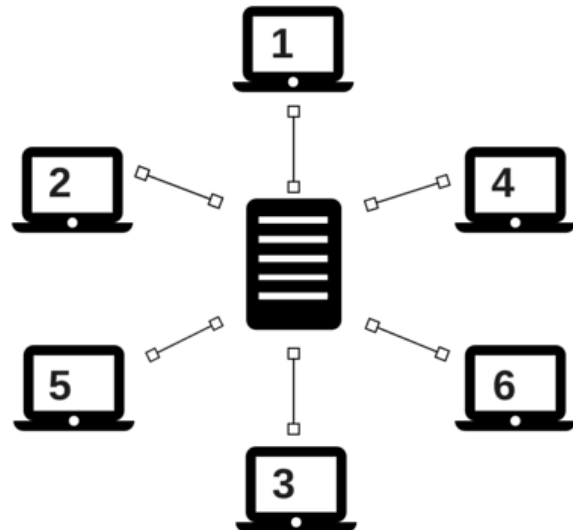
II.1.s Others

D'autres initiatives d'une catégorie différente reposant sur la Blockchain existent. La start-up Follow My Vote est une entreprise qui utilise le système de la blockchain pour proposer un moyen de voter en ligne. Cette plateforme Web fait valoir l'intérêt de la Blockchain dans un système de vote, puisqu'elle permet d'avoir un moyen sécurisé et transparent d'obtenir un consensus (ici, le résultat d'une élection). Même si les votes sont publiquement affichés sur la blockchain (donc vérifiables et infalsifiables), l'identité des personnes votant ne peut pas être connue grâce au système de clé publique / clé privée. L'identité est ainsi protégée, et les questions liées à une élection frauduleuse sont écartées. D'autres avantages sont promus par le site internet de l'entreprise : une réduction des coûts liés aux votes, un système plus accessible et moins contraignant, et qui garantit l'honnêteté d'une élection. Le document ci-dessous présente le principe de fonctionnement de la technologie utilisée par Follow My Vote.



Blockchain Technology allows for the secure management of a public ledger or database, where database transactions are verified and securely stored on a network.

 **followmyvote.com**



This database, also known as the blockchain, is managed by a network of nodes that all have their own copy of the database.

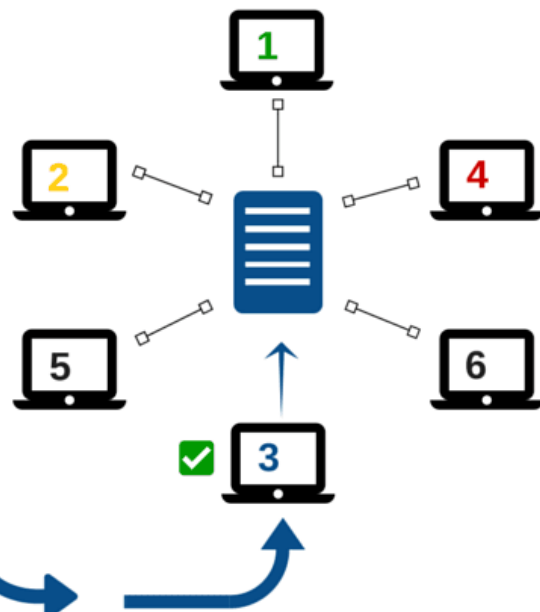
A node is simply a computer or server that is connected to a network. When a node connects to the network for the first time, it downloads a full copy of the blockchain database.



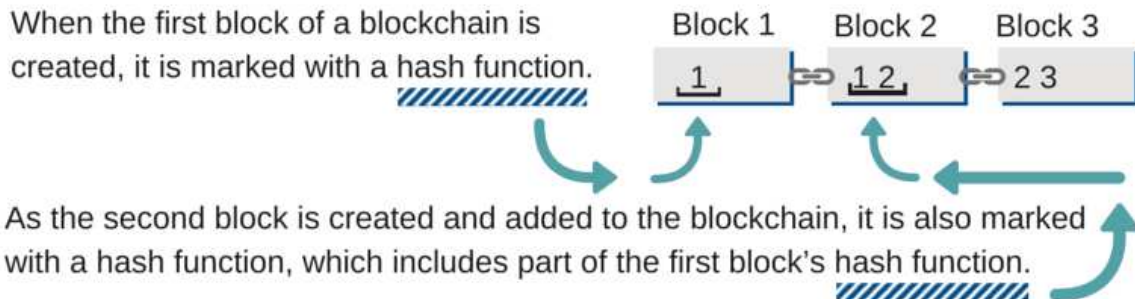
Nodes take turns pulling from a pool of pending transactions, which have been submitted to the blockchain but have yet to be officially added to the database.



Nodes then analyze the database transactions to determine whether or not they are valid based on a set of rules the network has agreed to.

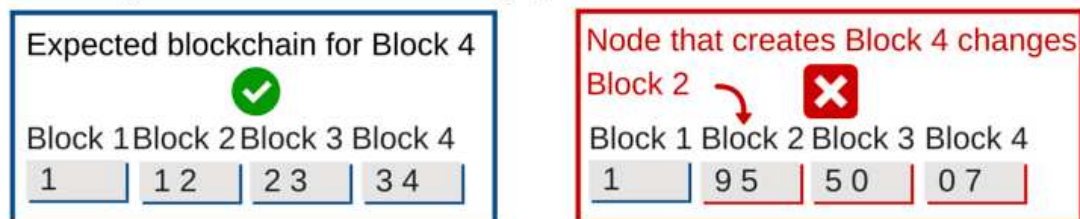


Valid transactions are grouped together and added to the database in a block, one after the other, in a way that resembles a chain, hence the name blockchain.



When a node submits a new block to the blockchain, if the node has changed any of the database transactions included within the previous block(s), the hash function of that block (and every block after) would also be changed.

Here's an example of how blockchain technology would detect and prevent a node from hacking the blockchain and changing database transactions:



When a node submits a blockchain update that contains an altered block, all other nodes will be able to detect that a change has been made and reject the update.

This fundamental functionality of blockchain technology is what makes a blockchain database secure.



Figure 27 : Principe de fonctionnement de la Blockchain par Follow My Vote (<https://followmyvote.com/>)

Le secteur de la santé est également touché par le phénomène technologique de la blockchain. Des entreprises telles que MedRec ou Bithealth se sont lancées dans la sécurisation et l'anonymisation des données médicales récoltées par des praticiens, des hôpitaux ou des objets connectés et qui seraient susceptibles d'être utilisées par n'importe qui. L'application proposée par MedRec permet de lier toutes les informations récoltées par ces sources d'origines différentes afin de les compiler dans la blockchain d'Ethereum, à l'aide de smart contract. Cela permet donc à l'utilisateur d'avoir un accès libre, sécurisé et à tout instant de son historique médical, peu importe les interventions, ou les traitements qu'il a reçus. Ainsi, MedRec propose une certaine opérabilité entre services médicaux, et une sécurisation

des données via la Blockchain. Il permet également, en utilisant un service externe à la blockchain, d'autoriser le partage de ces données selon la volonté de l'utilisateur. Les données anonymisées peuvent, par ailleurs, servir à des chercheurs en instanciant une base de données globale à but scientifique.



Figure 28 : Prototype de la plateforme permettant d'afficher l'historique des données médicales grâce à MedRec

II.2 Synthèse des applications possibles

A l'aide de l'ensemble des exemples cités ci-dessus, nous allons maintenant pouvoir détourer les facteurs qui font que la blockchain est utilisée, et quelles sont les caractéristiques-clés qui permettent aux entreprises utilisant cette nouvelle technologie de se différencier vis-à-vis d'entreprises aux services similaires, utilisant des méthodes plus traditionnelles.

II.2.a Facteurs d'utilisation de la blockchain

A l'aide des parties précédentes (partie I technique, et partie II.1 type Benchmark), nous allons pouvoir présenter les raisons de l'utilisation d'une blockchain dans un projet professionnel. Ci-dessous est présenté un schéma listant 7 éléments qui caractérisent la blockchain d'un point de vue business. Cette dernière permet :

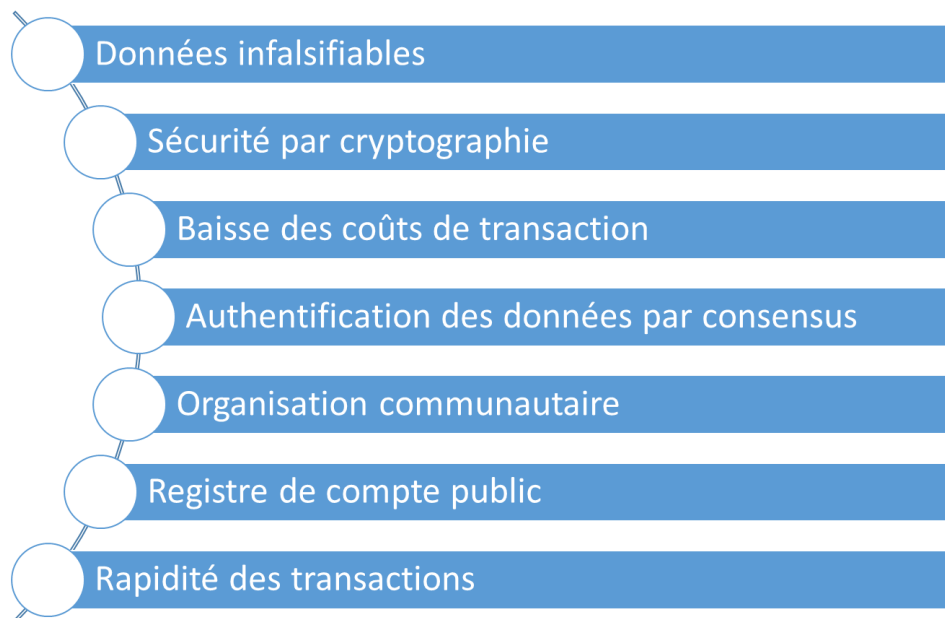


Figure 29 : Les 7 atouts de la technologie Blockchain

II.2.b Données infalsifiables

La technologie Blockchain repose sur le principe de preuve de travail (PoW, cf.I.2.d), qui garantit la génération d'un nouveau bloc de transactions, qui ne peut, en théorie, pas être modifié. C'est un des aspects les plus primordiaux de cette technologie, puisqu'elle permet de s'assurer d'avoir accès à des données dont la sécurité n'est pas compromise lorsqu'un bloc est inscrit sur une chaîne de blocs. L'intégrité des données est ainsi assurée et les utilisateurs de la blockchain n'émettent pas de doute concernant le niveau de fiabilité des données. A titre d'exemple, on peut imaginer une transaction de type « dépôt de brevet », lié à celui qui le

possède. L'action consistant à déposer son brevet sur la blockchain permet d'avoir une preuve non réfutable de l'appartenance du brevet à son propriétaire. De plus, le brevet n'aurait hypothétiquement plus à être déposé auprès d'un organisme ou d'une institution publique, ou du moins la preuve de propriété pourrait être justifié par la présence de cette transaction sur la blockchain.

On peut par ailleurs y voir un avantage supplémentaire : la prévention de la fraude. On pourrait imaginer également un comptable malintentionné voulant modifier les lignes de comptes de l'entreprise dans laquelle il travaille. Or, le fait de stocker les documents financiers d'une entreprise dans la blockchain assurerait des livres de compte non modifiables et visibles. Ainsi, l'utilisation de la blockchain en comptabilité pourrait pallier certains problèmes de fraude.

II.2.c Sécurité par cryptographie

La question de la sécurité et des données personnelles est une interrogation centrale pour un grand nombre de personnes. Afin de sécuriser la vie privée et les données de chaque utilisateur, les applications basées sur la blockchain peuvent permettre des services plus évolués que la plupart des applications traditionnelles.

Prenons le cas d'une application mobile. Généralement, lors de l'installation d'une application, les données personnelles sont au cœur du processus :

- Lorsqu'il faut accepter les termes d'installation : la propriété des données est transférée à l'éditeur de l'application, et les permissions qui permettent à l'éditeur d'utiliser les données sont accordées.
- Tout au long du cycle de vie de l'application, les données ne sont pas traçables par l'utilisateur.

Dans une application Blockchain, l'utilisation des données serait différente :

- Les utilisateurs peuvent contrôler toutes leurs données, et leur accès. Les utilisateurs peuvent en être les propriétaires.
- L'accès aux données est transparent, et l'utilisateur peut voir qui a demandé l'accès à ses données.
- L'utilisateur a la possibilité de donner ou de reprendre la permission d'accès à ses données personnelles.

L'identité des utilisateurs est protégée par le système de clé privée et de clé publique expliquée dans la première partie.

II.2.d Baisse des coûts de transaction

Un des principaux objectifs de la Blockchain du Bitcoin est d'obtenir une suppression d'intermédiaires acteurs de la transaction. Ainsi, cette suppression permet la réduction des coûts d'une transaction, et permet notamment les paiements « bon-marché » à l'international.

D'après un rapport 'The Fintech 2.0 paper : rebooting financial services', rédigé en collaboration entre Santander, InnoVentures, Oliver Wyman, et anthemis group, les économies dues à l'utilisation de la technologie Blockchain pourrait réduire les coûts liés aux paiements internationaux, à la sécurité et la mise en conformité de 15 à 20 milliard en 2022. Cela constitue donc un enjeu majeur pour les acteurs du secteur bancaire.

II.2.e Authentification des données par consensus

La désintermédiation requiert un système innovant sur lequel se baser afin d'avoir une confiance sûre des données présentes dans la blockchain. Cette confiance est établie par consensus entre les nœuds du réseau distribué. C'est ainsi qu'on parle de confiance distribuée.

Les DAO sont l'exemple le plus visible d'organisation reposant sur un système de consensus sur les données partagées. Ce type d'organisation permet d'avoir une chaîne de blocs persistante, un contrôle qui n'est dû qu'au code qui a été créé originellement, et une transparence de l'ensemble des transactions effectuées. The DAO est un projet mené par l'entreprise Slock.it, ayant pour but d'évaluer des projets qui lui sont soumis, de financer ces projets ou non, et de distribuer les risques et les récompenses associées, et ceci de manière collective. Cela ressemble à un système de crowdfunding ou d'investissement. Ce projet s'appuie sur la Blockchain Ethereum. The DAO possède tout de même une structure, composée de plusieurs développeurs renommés, qui sont susceptibles d'auditer les applications, ou projets, soumis à The DAO, afin de vérifier si le code correspond bien au service qui est rendu et présenter sur la plateforme. Cela pourrait paraître intrusif et ressembler à une autorité de contrôle, cependant, n'importe qui peut auditer n'importe quel projet. Cela permet de garantir la sécurité de l'application, sans pour autant promouvoir de centralisation.

Chaque projet sera ainsi soumis à quatre phases :

- La proposition (nombre d'Ether pour le prestataire, les produits / services proposés...)
- Les votes (chaque personne possédant des jetons pourra investir)
- Développement (une feuille de route est rédigée par smart contract, le prestataire devra respecter le rendu de livrables à certaines échéances)
- Déploiement (le service / produit est disponible et les avantages conclus originellement sont donnés)

En 2015, The DAO a cependant connu une situation problématique. Un smart contract a été validé par the DAO, et ce dernier était mal rédigé, en ce sens qu'il répétait un retrait de fond sans vérifier que les fonds étaient bien disponibles. Cela a permis au détenteur de ce contrat de récupérer 50 millions d'Ether. Ainsi, on peut en conclure que la technologie de la blockchain, et particulièrement les DAO, est une technologie qui n'est pas mature et qui connaît une croissance très rapide, qui demande un contrôle particulièrement intense pour

éviter une perte de confiance partielle ou totale en elle. Les détails de l'attaque sont disponibles sur internet sur le blog de slock.it (<https://blog.slock.it/a-dao-counter-attack-613548408dd7#.rdu0c49s4>).

II.2.f Organisation communautaire

Compte tenu de sa structure, la Blockchain possède des applications communautaires, notamment grâce à sa caractéristique distribuée entre les nœuds du réseau. Ainsi, à l'instar d'un vote impliquant tous les citoyens d'un pays, la blockchain pourrait remplacer le système actuel (lourd et coûteux), par un système sécurisé, simple d'accès (via une plateforme dédiée par exemple) et auditable, tout en garantissant l'anonymat des personnes votant. Ces éléments font de la blockchain un système idéal sous-jacent à une application de vote.

De la même manière, les applications qui se baseraient sur les entreprises communautaires actuelles (type Uber, Blablacar) pourraient permettre à leurs utilisateurs de profiter de services similaires, en évitant un surcoût de la transaction (une commission).

II.2.g Registre de compte public

L'idée de concevoir un outil capable d'avoir un registre de données fiables et infalsifiables constitue un des principaux avantages caractérisant la blockchain. Ainsi, la principale utilité d'un registre de ce type est qu'il puisse être audité par n'importe quelle personne ayant accès aux blocs. Ainsi, toute erreur, toute tentative de fraude, ou tout comportement malveillant peuvent être tracés facilement.

Ainsi, plusieurs applications concrètes existent déjà. Nous en avons par ailleurs cité dans les précédents paragraphes, comme l'application de traçage des diamants Everledger. Ce concept existe également pour garantir la traçabilité de produits alimentaires (provenance.org), ou bien encore celle des médicaments.

Pour résumer, l'ensemble des applications qui peut mener à un contentieux (paiements détournés, contestation d'un résultat d'élection, paternité d'une propriété intellectuelle ou industrielle) peut aider à apporter des preuves permettant d'accuser ou de disculper un parti. Cependant, peu de réflexion sur la Blockchain émergent en ce moment, et cette technologie navigue dans un vide juridique. Ainsi, il serait possible qu'une preuve apportée par la Blockchain ne soit pas suffisante aux yeux de la justice.

II.2.h Rapidité des transactions

La caractéristique de rapidité des transactions constitue dans le même temps un levier et un frein au développement de la Blockchain. En effet, les transactions peuvent être de plusieurs

types. Nous pouvons notamment relever deux types de transactions : les transactions à l'international, et les transactions effectuées sur les marchés financiers. Lorsque des transactions internationales peuvent être effectuées en plusieurs jours, d'autres transactions (marchés financiers) peuvent être ordonnées en quelques microsecondes.

Ainsi, les caractéristiques de la Blockchain ne permettent pas de vitesse de transactions très élevées. Par exemple, la Blockchain du Bitcoin ne peut générer un bloc, et par conséquent les transactions qu'il contient, que toutes les 10 minutes, compte tenu de la méthode de Proof of Work adoptée. On peut donc en conclure, qu'il n'est aujourd'hui pas possible de faire du trading haute fréquence basé sur la Blockchain.

Cependant, lorsqu'il s'agit d'échanges internationaux, les transactions sur une Blockchain peuvent être effectuées beaucoup plus rapidement que ce que proposent les banques à l'heure actuel. Cette caractéristique peut donc être nuancée selon le type de transaction effectué.

Conclusion

Dans ce document, nous avons tout d'abord pu étudier le procédé technique sur lequel repose la Blockchain. Cette innovation informatique permet ainsi d'organiser les échanges de données sur un réseau distribué, assurant une sécurisation des données par chiffrement, et faisant participer les nœuds du réseau pour la création de nouveaux blocs de la chaîne.

Nous avons vu dans une seconde partie ce que cette innovation technologique induit, en termes de changements potentiels, dans différents secteurs d'activités différents, et nous avons essayé d'en retirer les éléments clés qui font de la blockchain une invention disruptive.

Malgré tout, la blockchain est en phase de pics d'espérances, et a commencé à connaître quelques désillusions. En effet, la blockchain Ethereum a été « attaquée » en juin 2016. La raison de cette faille a été un code non vérifié contenu dans un smart contract. Cependant, plusieurs fois par an depuis sa création, des articles présagent la fin du Bitcoin dans les mois à venir, et la blockchain du Bitcoin n'a, jusqu'à aujourd'hui pas connu de désillusion. Ainsi, on peut en conclure que la confiance en cette nouvelle technologie n'est pas entière, et qu'elle lui faut davantage d'expérience et d'initiatives afin de la rendre viable dans le monde de l'entreprise.

Cette technologie est ainsi confrontée à plusieurs enjeux :

- La connaissance du principe de la blockchain est essentielle. Cette notion est aujourd'hui largement utilisée comme « buzz word », et peu comprennent avec finesse les rouages techniques sur lesquels est basée la blockchain. Cet enjeu demande une vulgarisation de termes aujourd'hui trop techniques pour un public non initié à l'informatique.
- Un des principes de la blockchain repose sur un réseau suffisamment fourni pour pouvoir accorder une certaine confiance au réseau. Ainsi, la technologie blockchain doit être l'objet d'une adhésion suffisante pour assurer son bon fonctionnement
- Les initiatives blockchains sont très nombreuses et dispersées. Comme pour la plupart d'autres technologies informatiques, les blockchains doivent respecter des normes afin de garantir un fonctionnement considéré comme normal. Ces normes ne sont pas encore totalement établies et une standardisation est nécessaire.
- Certains cas d'usage particuliers entraînent des querelles d'experts soutenues. Cela peut mener à des divisions au sein des membres les plus connaisseurs de cette technologie. Ces querelles peuvent aller à l'encontre de l'adhésion de la blockchain auprès de décideurs éventuels.

Lexique

Arbre de Merkle : aussi appelé arbre de hachage, procédé informatique et cryptographique permettant la compression de données.

Bitcoin (btc) : monnaie cryptographique basée sur un système de transaction peer to peer (la blockchain).

Bloc : Ensemble de données (de transaction, de prédécesseur, d'empreinte...) adapté à la blockchain.

Blockchain de consortium : type de blockchain particulière dont la gouvernance est assurée par des nœuds prédéfinis.

Blockchain privée : type de blockchain particulière dont la gouvernance est assurée par un nœud unique.

Blockchain publique : type de blockchain particulière dont la gouvernance est assurée par l'ensemble des nœuds du réseau.

Branches (forks) : ensemble de blocs construits en parallèle, et non de manière linéaire.

Clé privée : clé possédée uniquement par un compte de tiers et qui permet la signature numérique d'une transaction.

Clé publique : adresse d'un compte.

Compte de contrat : compte particulier, qui est sécurisé par le code qui le caractérise uniquement.

Compte de tiers : compte particulier, sécurisé par une clé privée.

Compte séquestre : mise en suspend de l'objet d'une transaction tant que la transaction n'est pas validée.

Crypto monnaie : monnaie électronique inclut dans un réseau P2P ou décentralisé.

Cryptographie : discipline ayant pour objectif d'assurer une sécurisation ou une protection des données en transit.

DAO : Decentralized Autonomous Organization, organisation utilisant les smart contracts d'une blockchain afin de régir et d'assurer la gouvernance des participants.

Double dépense : action de payer deux fois avec le même actif. C'est donc une action frauduleuse.

En-tête de bloc : Ensemble de données (de taille 80o) contenues au début d'un bloc. Pour le Bitcoin, cet en-tête est constitué de :

- Version du bloc
- Le hash du précédent bloc
- La racine de Merkle du bloc

- Le temps
- La complexité (objectif de difficulté pour la preuve de travail par exemple)
- Nombre aléatoire de taille 32 bits

Ethereum : blockchain publique utilisant les smart contracts et dont la monnaie virtuelle est l'éther.

Hash (empreinte) : fonction particulière qui permet de convertir une donnée en une suite de chiffre précise de manière unique. Ce chiffre représente donc l'identité de la donnée. L'information contenue dans la donnée est, quant à elle, impossible à connaître à partir de son empreinte uniquement.

Mineur : nœud du réseau dont la particularité est d'utiliser sa puissance de calcul afin d'ajouter un bloc à la blockchain, en calculant une fonction de hachage précise.

Oracle : entité permettant de récolter des données selon le besoin défini par les codes des smart contracts. Il existe plusieurs types d'oracles.

Preuve d'enjeu (Proof of Stake) : méthode de résolution d'une inégalité obligatoire permettant l'ajout d'un bloc par un mineur, qui repose sur la quantité de monnaie qu'un mineur possède par rapport aux autres.

Preuve de travail (Proof of Work) : méthode de résolution d'une inégalité obligatoire permettant l'ajout d'un bloc par un mineur, qui repose sur la puissance de calcul qu'un mineur possède par rapport aux autres.

SHA256 : fonction de hachage particulière. La double SHA256 est la fonction de hashage utilisée dans la blockchain du Bitcoin, pour vérifier l'inégalité de la preuve de travail.

Signature numérique : moyen de certification et de sécurisation de l'identité d'un compte.

Smart contract : programme informatique associé à un compte de contrat et qui s'exécute lorsqu'un autre compte (compte de contrat ou compte de tiers) envoie un message au compte de contrat auquel il est rattaché.

Tiers de confiance : organisme autorisé à utiliser des signatures électroniques. Cet organisme peut bénéficier de frais de transaction à chaque fois qu'il en certifie une.

Transaction : opération d'échange impliquant plusieurs parties. Dans le cadre de la blockchain, une transaction peut être définie comme l'ajout d'un objet dans un bloc.

Vérification de paiement simplifié : principe énoncé par Satoshi Nakamoto permettant de vérifier l'authenticité des blocs sans avoir besoin de l'intégralité des données contenues dans la blockchain.

Bibliographie

- Actance. (2015). *La blockchain : de nouveaux business models pour le secteur IT?* Récupéré sur actance.net: <http://www.actance.net/actualites/la-blockchain-de-nouveaux-business-models-pour-le-secteur-it.html>
- angel.co. (2016). *My powers*. Récupéré sur angel.co: <https://angel.co/mypowers-1>
- Bernard, P. (2016). *La blockchain au service de l'assurance*. Récupéré sur cestpasmonidee.blogspot.fr: <http://cestpasmonidee.blogspot.fr/2016/01/la-blockchain-au-service-de-lassurance.html>
- Bitcoin.fr. (2016). *Bitcoin expliqué par son inventeur*. Récupéré sur Bitcoin.fr: <https://bitcoin.fr/bitcoin-explique-par-son-inventeur/>
- Bitcoin.it. (2010). *Preuve de travail*. Récupéré sur Bitcoin.it: https://fr.bitcoin.it/wiki/Preuve_de_travail
- Bitcoin.it. (2013). *En-tête de bloc*. Récupéré sur bitcoin.it: https://fr.bitcoin.it/wiki/En-t%C3%AAt_de_bloc
- Blockchain France. (2015). *Focus sur la Zooz, le covoiturage version Blockchain*. Récupéré sur blockchainfrance.net: <https://blockchainfrance.net/2015/11/02/la-zooz-covoiturage-blockchain/>
- Blockchain France. (2016). *Blockchain : Honduras 1 - France 0*. Récupéré sur blockchainfrance.net: <https://blockchainfrance.net/2015/09/16/le-honduras-adopte-la-blockchain/>
- Blockchain France. (2016). *Des cadastres sur la Blockchain*. Récupéré sur blockchainfrance.net: <https://blockchainfrance.net/2016/03/03/des-cadastres-sur-la-blockchain/>
- Blockchain France. (2016). *Qu'est ce qu'une DAO?* Récupéré sur blockchainfrance.net: <https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/>
- Blockchain use cases II : non-financial and financial use cases*. (2015). Récupéré sur letstalkpayments.com: <https://letstalkpayments.com/blockchain-use-cases-part-ii-non-financial-and-financial-use-cases/>
- Blockverify. (2016). *Blockverify*. Récupéré sur blockverify.io: <http://www.blockverify.io/>
- Blogchain.fr/. (2015). *Blogchain*. Récupéré sur Blogchain.fr/: <http://blogchain.fr/>
- Bohic, C. (2016). *On a testé Onename : une identité sur la blockchain*. Récupéré sur itespresso.fr: <http://www.itespresso.fr/test-onename-identite-blockchain-120763.html>
- Catalini, C., & Gans, J. S. (2016). *Some Simple Economics of the blockchain*. MIT / NBER.
- Catalini, C., & Tucker, C. (2016). *Seeding the S-Curve ? The role of early adopters in diffusion*. MIT.
- Cavazza, F. (2016). *Définition, usages et enjeux des blockchains*. Récupéré sur Fred Cavazza: <https://fredcavazza.net/2016/01/07/definition-usages-et-enjeux-des-blockchains/>
- crowdlending.fr. (2015). *La blockchain va révolutionner le crowdfunding (déjà!)*. Récupéré sur Crowdlending.fr: <http://www.crowdlending.fr/la-blockchain-va-revolutionner-le-crowdfunding-deja/>
- Debune. (2016). *What is Debune?* Récupéré sur debune.org: <http://debune.org/what-is-debune/>

- Everledger. (2016). *Smart contracts*. Récupéré sur everledger.io:
http://www.everledger.io/smart_contracts
- Fischer, J.-B. (2016). *Blockchain et IoT : le plaidoyer d'IBM*. Récupéré sur bitcoin-france.org:
<https://bitcoin-france.org/2016/05/02/blockchain-et-iot-le-plaidoyer-dibm/>
- Fredouelle, A. (2016). *Ripple, la blockchain qui secoue la finance mondiale*. Récupéré sur journaldunet.com: <http://www.journaldunet.com/economie/finance/1184734-ripple/>
- Hottot, K. (2016). *The DAO : un pirate dérobe 50 millions de dollars, la contre-attaque se prépare*. Récupéré sur nextinpact.com: <http://www.nextinpact.com/news/100336-the-dao-pirate-derobe-50-millions-dollars-contre-attaque-se-prepare.htm>
- IBM. (2016). *Explore Watson IoT with blockchain*. Récupéré sur ibm.com:
<http://www.ibm.com/internet-of-things/iot-news/announcements/private-blockchain/>
- Ilén, I. (2016). *Is Blockchain the future of Cloud Storage?* Récupéré sur nxfab.com:
<http://www.nxfab.com/blog/2016/5/27/the-age-of-autonomic-intelligence>
- Jeux Bitcoin. (2016). *jeux-bitcoin*. Récupéré sur jeux-bitcoin.com: <https://jeux-bitcoin.com/>
- jurispedia.org. (2009). *Institutions de régulation du commerce électronique*. Récupéré sur fr.jurispedia.org:
[http://fr.jurispedia.org/index.php/Institutions_de_r%C3%A9gulation_du_commerce_%C3%A9lectronique_\(fr\)](http://fr.jurispedia.org/index.php/Institutions_de_r%C3%A9gulation_du_commerce_%C3%A9lectronique_(fr))
- Lahalle, E. (2016). *[DOSSIER] LA BLOCKCHAIN : FUTUR TIERS DE CONFIANCE ? – LES UTILISATIONS POSSIBLES DE LA BLOCKCHAIN EN ASSURANCE*. Récupéré sur insurancespeaker-wavestone.com: <https://www.insurancespeaker-wavestone.com/2016/03/dossier-blockchain-futur-tiers-de-confiance-utilisations-possibles-de-blockchain-assurance/>
- Ledgys. (2016). *Home*. Récupéré sur ledgys.io: <http://ledgys.io/>
- Linuxfr.org. (2013). *Journal : Comment fonctionne Bitcoin*. Récupéré sur linuxfr.org:
<http://linuxfr.org/users/gof/journaux/comment-fonctionne-bitcoin>
- LTP. (2015). *Blockchain use cases : Comprehensive analysis & startups involved*. Récupéré sur letstalkpayments.com: <https://letstalkpayments.com/blockchain-use-cases-comprehensive-analysis-startups-involved/>
- LTP Team. (2015). *An interview with the Founder of Blockchain Company Otonomos*. Récupéré sur letstalkpayments.com: <https://letstalkpayments.com/an-interview-with-the-founder-of-blockchain-company-otonomos/>
- Madore, P. (2015). *Assembly uses the bitcoin blockchain to monetize development*. Récupéré sur cryptocoinsnews.com: <https://www.cryptocoinsnews.com/assembly-uses-bitcoin-block-chain-monetize-development/>
- Noizat, P. (2014). *Bitcoin et les arbres de Merkle*. Récupéré sur e-ducat.fr: <http://e-ducat.fr/2014-02-09-bitcoin-et-les-arbres-de-merkle/>
- Octo. (2016). *Bitcoin : un système de paiement électronique pair-à-pair (traduction du papier de Satoshi Nakamoto par Arnaud-François Fausse)*. Récupéré sur Blog.octo.com:
http://blog.octo.com/wp-content/uploads/2016/01/bitcoin_fr.pdf

- Oname. (2016). *Oname*. Récupéré sur oname.com: <https://oname.com/>
- Otonomos. (2016). *Otonomos*. Récupéré sur otonomos.com: <https://www.otonomos.com/about-us/>
- Palop, K. (2016). *Dossier Blockchain - Partie 2 : les défis de la blockchain dans le monde réel (1/3)*. Récupéré sur arsiemons.fr: http://www.arsiamons.fr/defis_blockchain_monde_reel_1_3/
- Porlot, S. (2016). *Les Oracles, lien entre la blockchain et le monde*. Récupéré sur ethereum-france.com: <https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/>
- Santander InnoVenture, Oliver Wyman, Anthemis group. (2015). *The Finetech 2.0 Paper : Rebooting financial services*.
- Simonin, X. (2016). *Pour comprendre la technologie blockchain*. Récupéré sur revue-banque.fr: <http://www.revue-banque.fr/management-fonctions-supports/article/pour-comprendre-technologie-blockchain>
- Teruzzi, D. (2016). *La programmation de smart contracts: une opération hautement délicate*. Récupéré sur blockchaincafe.com: <http://blockchaincafe.com/la-programmation-de-smart-contract-une-operation-hautement-delicate>
- Teruzzi, D. (2016). *Les consensus : Proof of Work vs Proof of Stake*. Récupéré sur finyear.com: http://www.finyear.com/Les-consensus-Proof-of-Work-vs-Proof-of-Stake_a35663.html
- Teruzzi, D. (2016). *Les protocoles de consensus distribués*. Récupéré sur blockchaincafe.com: <http://blockchaincafe.com/264-2>
- Wikipedia. (2016). *Arbre de Merkle*. Récupéré sur Wikipedia: https://fr.wikipedia.org/wiki/Arbre_de_Merkle
- Wikipedia. (2016). *SHA-2*. Récupéré sur Wikipedia: <https://fr.wikipedia.org/wiki/SHA-2>
- Yermack, D. (2015). *Corporate Governance and Blockchain*. NBER Working Paper.
- Zaninotto, F. (2016). *La blockchain expliquée aux développeurs web*. Récupéré sur marmelab.com: <http://marmelab.com/blog/2016/05/12/blockchain-expliquee-aux-developpeurs-web-la-theorie.html>