La blockchain au-delà des crypto-monnaies

Veille Technologique

—

Fabien Le Bronnec
M2I IASI
2017-2018

INSTITUT INFORMATIQUE APPLIQUÉE

Table des matières

I. Introduction

La blockchain est presque unanimement reconnue comme une avancée majeure dans l'industrie de l'information. Certains observateurs prédisent même qu'elle modifiera notre société toute entière. Néanmoins, c'est un concept relativement jeune qui peine encore à trouver sa pleine application.

C'est surtout devenu ces dernières années un « buzz-word » apportant avec lui une plus-value marketing incontestable, propulsé par la folie spéculative autour des crypto-monnaies. Mais il semble bien qu'une majeure partie du grand public et même des professionnels ne sache pas vraiment ce qu'est une blockchain, comment elle fonctionne et ce qu'elle permet.

Après un bref historique de la technologie, nous tenterons d'en fournir un état de l'art technique et une description de son fonctionnement. Ensuite nous ferons un tour d'horizon des usages de la technologie avant de voir plus en détail quelques applications représentatives. Finalement, après une exploration des enjeux légaux autour de la blockchain, nous ferons un bilan de ce qui a été appris et des préconisations qui en découlent.

II. Présentation

1. Définition

Une blockchain est un registre de faits ou de transactions horodatés et triés chronologiquement. Ce registre est partagé sur de nombreux ordinateurs (nœuds) fonctionnant sur un réseau pair-à-pair et communiquant de manière cryptée. Lorsque l'un des nœuds soumet un nouveau fait au réseau, ce dernier forme un consensus pour horodater ce nouveau fait et l'intégrer à la blockchain. Cette dernière constitue donc une base de données distribuée et théoriquement infalsifiable.

La finalité de la blockchain est d'offrir un mécanisme de consensus concernant l'état d'une base de données partagée au sein d'un réseau d'opérateurs non fiables.

2. Présentation technique

En soit, la blockchain ne représente pas une évolution technique à proprement parler, il s'agit plutôt de l'articulation inédite de concepts pré-existants :

- Consensus distribué
- Cryptographie asymétrique
- Réseau peer-to-peer

A la base, la blockchain est une chaîne chronologique de bloc de données horodatées. La blockchain est dupliquée sur chacun des nœuds appartenant au réseau. Avec un nombre de nœuds suffisant et l'assurance qu'aucun opérateur unique ne possède la moitié des nœuds, il devient impossible pour un opérateur malveillant de falsifier les données, qui seraient immédiatement invalidées par tous les autres nœuds.

A un rythme régulier, les nouvelles données soumises au réseau sont horodatées et triées chronologiquement au sein d'un bloc qui sera intégré à la chaîne des blocs existants. Dès lors, comme on l'a vu, ces données et surtout leur ordre sont infalsifiables.

Les nœuds participant à la création de ces blocs sont dit mineurs. Chacun d'entre eux recevant les nouvelles données à des moments différents, chacun créera un bloc

potentiellement différent, mais un seul d'entre eux doit pouvoir avoir le dernier mot. Ils sont donc mis en concurrence les uns avec les autres via la résolution d'un défi mathématique.

Lorsqu'un nœud parvient à résoudre le défi permettant de valider son bloc en constitution, il envoi ce dernier à tous les autres nœuds, qui valident le nouveau nœud et l'intègre à leur copie de la chaîne.

Certaines blockchains permettent l'exécution de programmes qui opèrent donc sur des données et des conditions infalsifiables. Cela fonctionne exactement comme un contrat à la différence que son exécution n'a plus besoin d'être imposée de manière juridique, puisqu'elle l'est déjà de manière technique et automatisée. C'est ce que l'on nomme les contrats intelligents, ou smart-contracts.

3. Historique

L'historique du blockchain est intimement lié à celui de la crypto-monnaie puisque les deux concepts sont nés en même temps. Dès la fin des années 90, on voit émerger des propositions considérant la création de crypto-monnaies, mais aucune d'entre elle ne propose de modèle de confiance satisfaisant.

C'est en 2008 qu'un inconnu répondant au pseudonyme de Satoshi Nakamoto décrit dans un document d'une dizaine de pages seulement le concept de ce qui deviendra le Bitcoin. Il créé ensuite le premier bloc le 3 janvier 2009 puis un mois plus tard publie la première version du logiciel Bitcoin.

Suite à cela et de part la spéculation, tout s'enchaîne très vite. La parité dollar-bitcoin est atteinte dès février 2011 puis la valeur de la monnaie ne cesse d'augmenter de manière exponentielle, malgré quelques chutes. Des sociétés de minage se créent, de plus en plus d'opérateurs acceptent la monnaie. Profitant que le code de Bitcoin soit open-source les crypto-monnaies se multiplient.

Evolution du taux de change du bitcoin en dollar depuis sa création (source Wikipédia)

Dans le même temps, le concept de blockchain commence à se différencier de celui de la crypto-monnaie, tandis que de plus en plus d'acteurs commencent à réfléchir à de nouvelles applications, en particulier dans les domaines de gestion des transactions et des assurances. Les smart-contracts sont nés.

4. Enjeux

Les enjeux des blockchains sont nombreux et répartis dans de nombreux domaines.

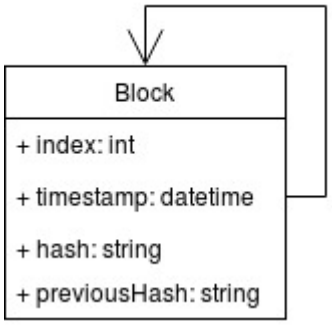
Une grande partie des acteurs des domaines financiers, d'assurances et légaux jouent le rôle d'intermédiaires de confiance. Comptables, assureurs, notaires sont chargés de certifier les informations que sont les contrats, les transactions, etc. Or comme on l'a vu, la blockchain rend la nécessité de tiers de confiance complètement obsolète, car l'information est auto-vérifiée. Même pour un sujet aussi trivial que les paris, il n'est plus nécessaire d'avoir recours à un bookmaker. Un tel impact se doit d'être anticipé avec une veille au long court.

III. Description Technique

Cette partie est dévolue à la description technique avancée du blockchain. La blockchain est un concept qui peut s'avérer techniquement difficile à appréhender. Or, comme nous l'avons vu plus haut, elle n'est pas innovante dans les technologies misent en jeu, mais dont la manière dont des technologies connues s'articulent entre elle.

1. Base de donnée distribuée

Avant tout autre chose, une blockchain est une base de données distribuée entre différents nœuds. Cette base de données, comme son nom l'indique, est une chaîne d'éléments appelée blocs. Dans sa plus simple expression, la chaîne est une liste chaînée (linked list en anglais), structure de donnée classique présente dans la plupart des langages de programmation. Chaque bloc maintient une référence au bloc le précédent dans la liste. Dans sa plus simple expression, un bloc peut être représenté de la manière suivante :



Données

index : Index du bloc dans la chaine
timestamp : Horodatage du bloc
hash : Résultat d'une fonction de hachage du contenu du bloc
previousHash : Résultat du hachage du bloc précédent dans la chaîne

Dans la réalité et pour que la blockchain ait une quelconque utilité, un bloc comprendra des données.

2. Contrôle et validation

La blockchain doit aussi proposer un mécanisme de validation de l'intégrité de chacun de ses blocs. Pour assurer sa validité, un bloc doit vérifier les assertions suivantes :

- L'index du bloc doit être supérieur de 1 au précédent
- Le previousHash du bloc correspond au hash du bloc précédent (index-1)

- Le hash du bloc lui même doit être valide

Le nœud est le programme qui maintient la chaîne. Il doit être capable de la maintenir à jour. A la réception d'une nouvelle chaîne, si cette dernière est plus longue que celle déjà maintenu et que tous ses blocs sont valides, elle viendra remplacer la chaîne déjà présente.

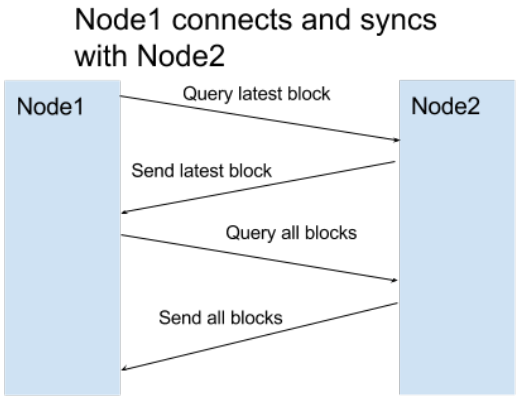
Notre cas d'étude fait abstraction pour des raisons de simplicité de la partie donnée elle-même. Mais il est évident que dans la réalité, ces données aussi sont vérifiées de la même manière que l'intégrité du bloc lui même. Par exemple, dans le cas des cryptomonnaie, chaque nœud dispose des informations nécessaires pour vérifier que les transactions sont valides.

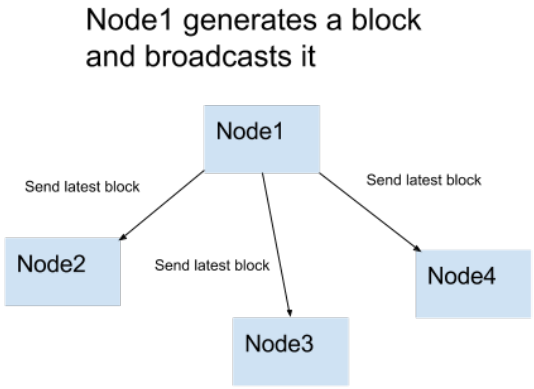
3. Communication entre les nœuds

Les différents nœuds du réseau doivent pouvoir communiquer entre eux pour émettre et recevoir les mises à jour de la chaîne et récupérer d'une éventuelle défaillance. Le réseau obéit à un principe d'horizontalité qui veut que chaque nœud est égal aux autre en privilèges et fonctionnalités, il n'y a pas de hiérarchie. Ils évoluent dont au sein d'un réseau pair-à-pair (peer-to-peer en anglais).

A sa connexion au réseau, un nœud requêtera les nœuds déjà présents sur le réseau au fur et à mesure qu'il les découvre et plus spécifiquement le bloc le plus récent (index le plus élevé) dont ils disposent. Si l'index du bloc reçu est supérieur à l'index maximal dont lui même dispose, le nœud se mettra à jour, soit différentiellement soit en requêtant la chaîne dans son ensemble. Il fera bien sûr en sorte de vérifier les nouvelles données reçues selon le mécanisme expliqué dans le point précédent. Puis il effectuera cette mise à jour de manière régulière.

Lorsqu'il créé un nouveau bloc, un nœud le transmet à tous les autres nœuds auxquels il est connecté. Là encore, ces derniers valident le nouveau bloc comme vu précédemment et en cas de succès, l'ajoutent à leur propre chaîne.





Ainsi, tous les nœuds sont en permanence synchronisés les uns avec les autres, au delta de la latence mise en jeu par la communication et l'exécution des algorithmes. Bien sûr, cela fonctionne du fait que tous les nœuds partagent la même logique.

Néanmoins, si un nœud venait à utiliser une logique différente et ne pas suivre les règles communes, principalement pour des raisons malveillantes, les modifications qu'il apporterait à la chaîne seraient systématiquement refusées par tous les autres nœuds et ne pourraient donc pas se répandre dans le réseau. Le nœud malveillant ou défectueux lui même, ne disposant pas des informations faisant consensus, ne pourrait donc même pas opérer de manière viable sur le réseau qui est ainsi protégé.

Néanmoins, on découvre là l'un des premiers problème de la technologie en ce qu'elle est peut efficace. En effet, l'intégralité des données sont répliquées autant de fois qu'il y de nœuds, ce qui implique une forte empreinte mémoire proportionnelle au nombre d'acteurs. De même les échanges constants entre tous les nœuds du réseau créent un important trafic de données. Cette problématique d'efficacité est encore plus criante lorsque l'on aborde un point central de la blockchain : la méthode de consensus. Du fait de l'importance et de la complexité de cette notion, elle fait l'objet de sa propre partie ci-après.

IV. La Méthode de Consensus

1. Présentation du problème

Du fait que la blockchain existe au sein d'un réseau horizontale, son principe à la fois le plus critique et le plus complexe est certainement la nécessité de consensus entre les nœuds pour l'ajout de nouvelles données. En effet, il n'existe pas d'acteur ayant une autorité absolue qui pourrait arbitrairement ajouter des données automatiquement validées à la chaîne. Tous les nœuds « mineurs » pouvant potentiellement créer un nouveau bloc, il faut donc un mécanisme commun pour cette création qui permette la vérification et la validation par tous les autres nœuds. De plus, le réseau étant ouvert, chaque nœud ne peut pas accorder sa confiance aveuglément aux autres de manière à protéger l'ensemble du réseau contre des données fausses ou vérolées.

Cette situation est généralement assimilée au problème classique dit des « généraux byzantins ». Pour résumer cette métaphore, il faut imaginer un groupe de généraux éparpillés géographiquement ayant besoin de se mettre d'accord sur un plan de bataille. Avec le risque qu'il y ait un ou plusieurs traîtres parmi eux ou parmi leurs messagers.

2. Preuve de Travail

La méthode de consensus « historique » des blockchain est la Preuve de Travail (Proof of Work en anglais). Cette technique n'est pas nouvelle et a déjà été utilisée notamment comme mécanisme anti-spam avec Hashcash, qui a servit de base à l'algorithme du Bitcoin.

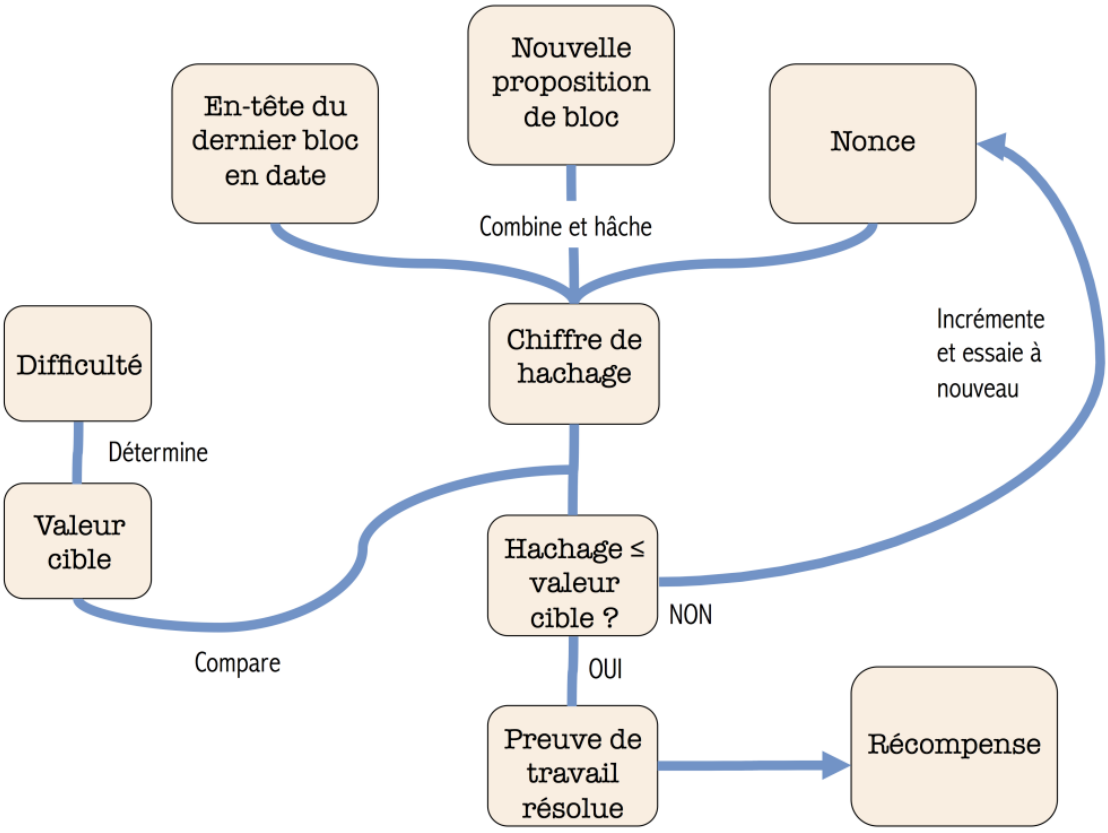
Description

Le principe est que pour ajouter un nouveau bloc de données à la chaîne, le nœud doit faire la preuve d'un « travail » au sens temps de calcul mis en jeu. Cette preuve de travail prend la forme du calcul d'un hachage, dont le résultat doit correspondre à un résultat attendu. Par exemple, dans le cas du Bitcoin, le hash obtenu doit se terminer par un nombre fixé de zéros successifs. Le nombre de zéros attendu constitue la « difficulté ». Plus elle est élevée, plus elle va ralentir la création de nouveau nœuds.

Pour résoudre le défi, le nœud va successivement calculer un hash des données du nouveau bloc auquel il adjoindra un nombre arbitraire, appelé « nonce », avec un algorithme

propre au réseau. Si le résultat coïncide à l'attendu, il a réussi, sinon il essaie de nouveau avec un autre « nonce ».

Chaque nœud du réseau est donc en compétition avec tous les autres pour l'ajout de nouveaux blocs. Quand un nœud parvient à résoudre le défi, il transmet le résultat à tous les autres nœuds via le réseau. Chaque nœud pourra vérifier que le défi a été correctement résolu en se contentant de recalculer le hash fournit. La preuve de travail est donc à la fois très complexe et gourmande en puissance de calcul afin d'être trouvée, mais très aisée à vérifier.



La régulation par la difficulté

Quand une blockchain devient populaire, le nombre de mineur tend à augmenter et donc la création de blocs à s'accélérer. Dans le cas des crypto-monnaie, à chaque bloc généré correspond pour une récompense en monnaie virtuelle, pour justement encourager le minage. Néanmoins, comme pour toute devise, une monnaie dont la masse augmente de manière incontrôlée risque un phénomène d'inflation quasi certain. Pour éviter cela, les

blockchains de crypto-monnaies ont mis en place des mécanismes pour artificiellement ralentir la production.

Le premier est l'abaissement régulier de la récompense octroyée à la création d'un bloc. Par exemple, dans le cas du BitCoin, le montant offert pour le calcul d'un bloc est divisé par 2 tous les 4 ans. Cela signifie que le nombre de BitCoins générable est fini et sera au maximum au alentours de 21 millions. Chiffre qui sera atteint au rythme actuel aux alentours de 2140. Mais pour que cela soit efficace en terme de régulation, il faut également que le temps de génération des nouveaux blocs soit connu et fixé. C'est là qu'entre en jeu la difficulté.

La blockchain a en effet la possibilité d'imposer le rythme auquel seront généré les blocs. On l'a vu plus haut, c'est essentiel à la constitution d'une crypto-monnaie viable. Généralement, ce rythme de production est fixé à la création d'une blockchain. Par exemple, pour le BitCoin, il s'agit d'un bloc toutes les 10 minutes. On l'a également vu, la difficulté est elle aussi fixée par la blockchain. Or, il existe une dernière variable, et qui elle n'est ni connue ni définie : le nombre de mineurs participant.

A difficulté égale, plus le nombre de mineur est élevé, plus les blocs sont générés rapidement, ce qui pourrait être résumé par l'équation suivante :

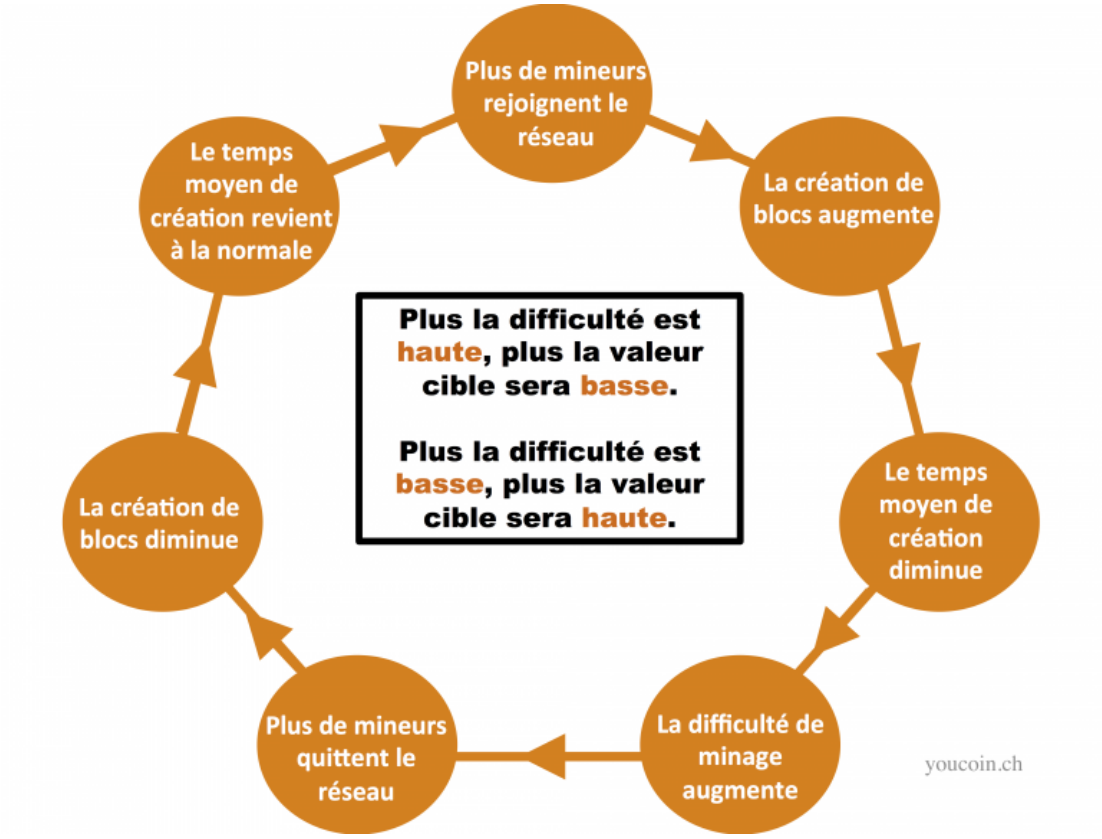
$$\frac{D}{N} = T$$

D : Difficulté
N : Nombre de mineurs
T : Temps nécessaire à la création d'un bloc

Il en découle que si l'on veut garder le temps de création de nouveau bloc fixe, il faut faire varier la difficulté en fonction du nombre de mineurs. En prenant encore le BitCoin en exemple, cela est géré via un algorithme implémenté depuis son origine et copié par la plupart des autres cryptomonnaies.

Tous les 2016 blocs générés (ce qui correspond normalement à un délai de 2 semaines), le temps total nécessaire à leur génération est comparé au temps prévu. Si le temps effectif est inférieur au temps désiré, la difficulté est augmentée et *vice versa*.

Le réseau connaît donc un régulation constante. En effet, si la difficulté est basse, de nombreux mineurs voudront rejoindre le réseau ce qui accélérera la création de bloc. La difficulté sera progressivement haussé jusqu'à un retour à un rythme normal. Une difficulté élevée découragera les mineurs les moins performants qui quitteront le réseau. Le rythme de création viendra donc se ralentir et la difficulté sera progressivement abaissée, recommençant ainsi le cycle.



Limites de la preuve de travail

Malgré son utilisation généralisée dans la blockchain, les limites de la preuve de travail ont déjà été identifiées.

i. Inefficacité

Comme on l'a vu, chaque nœud est en concurrence avec tous les autres pour résoudre le défi, donc la réalisation de la même tâche. Or, seul l'un d'entre eux sera gagnant. La puissance de calcul de tous les autres nœuds aura été en quelque sorte gaspillée.

ii. Coût

Le défi se voulant volontairement dur à résoudre, il est très gourmand en puissance de calcul, donc en énergie.

iii. Vulnérabilité

La Preuve de Travail est relativement sure. Elle n'est en théorie vulnérable qu'aux attaque de force brute, mais il s'avère tellement coûteux et peu probable de trouver un hash valide en le générant aléatoirement que ce n'est pas une réalité pratique. Reste que le réseau, de part son fonctionnement, ne peut plus assurer sa validité à partir d'un moment ou un acteur possède au moins 51 % des nœuds du réseau. En effet, si l'un de ses nœud injectait des données fallacieuses, ces dernières seraient validées par plus de la moitié du réseau et deviendraient valides « de fait ». Plus un réseau regroupe de nœuds, plus il est donc sûr. Le risque est néanmoins réel, puisqu'il y a déjà eut des attaques réussis sur certains réseaux.

3. Preuve de Participation

Du fait des limites énoncées plus haut de la Preuve de Travail, des développeurs ont cherché des alternatives à cette dernière. La solution la plus courante est celle de la Preuve de Participation ou Preuve d'Enjeu (Proof-of-stake en anglais), déjà implémentée par plusieurs chaînes, la première ayant été Peercoin.

Description

On l'a vu, dans une méthode par preuve de travail, tous les nœuds mineurs sont en concurrence les uns avec les autres et doivent rivaliser de puissance pour espérer miner le prochain bloc de la chaîne. Les cas de la preuve de participation est radicalement différent, car le nœud chargé de miner le prochain bloc est défini par la chaîne. C'est dans cette décision qu'intervient le mode de consensus.

En pratique, la sélection du prochain nœud validateur se fait selon de nombreuses modalités différentes, du complètement aléatoire au prédéfini. Néanmoins, on considère généralement que, pour qu'un nœud soit sélectionnable, il doit faire la preuve qu'il a un enjeu dans le fait de faire fonctionner normalement la chaîne. Il s'agit de la proof-of-stake (PoS).

Dans le cas d'une chaîne s'appuyant sur une crypto-monnaie, ce qui est encore généralement le cas, cette proof-of-stake se fait via l' « investissement » dans la crypto-monnaie. Afin d'être éligible, un nœud doit « déposer » un montant. Tant que ce montant sert de dépôt, il est bloqué et ne pourra pas changer de main. La sélection se fait alors de manière aléatoire parmi les nœud éligibles. Néanmoins, cette chance de sélection n'est pas homogène mais dépend du montant investi par chaque nœud. Un nœud ayant déposé 1000 unités aura 10 fois plus de chance d'être sélectionné qu'un nœud en ayant déposé 100.

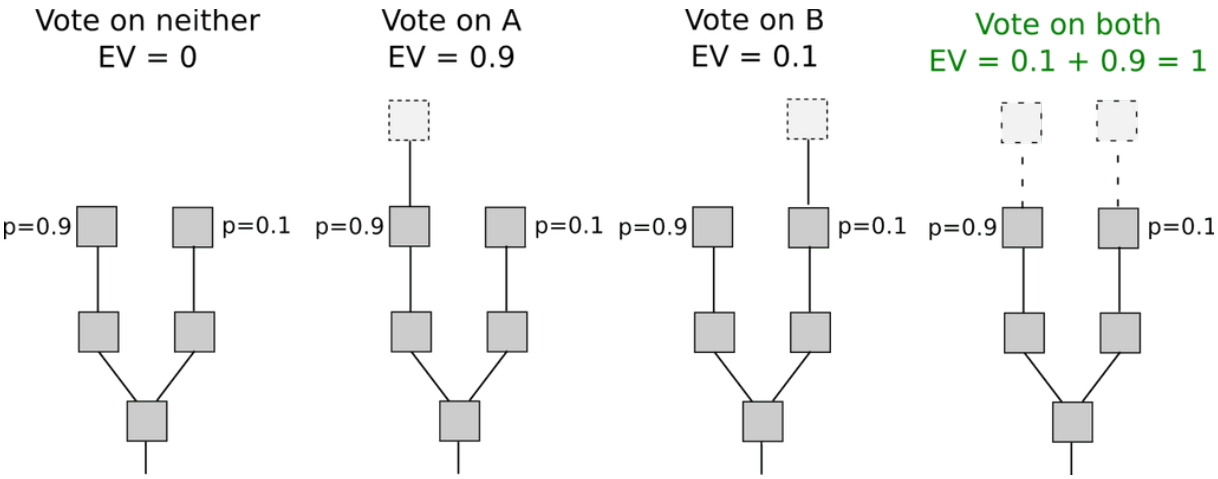
Cette méthode peut sembler au premier abord très déséquilibrée en faveur des nœuds les plus « riches », mais le problème ne devient manifeste que si un nœud possèdent

une proportion énorme du montant total déposé par tous les nœuds, ce qui dans la réalité n'est jamais le cas. D'ailleurs, la preuve de travail est elle aussi inégalitaire, puisqu'elle avantage les nœuds riches en matériel informatique et puissance de calcul.

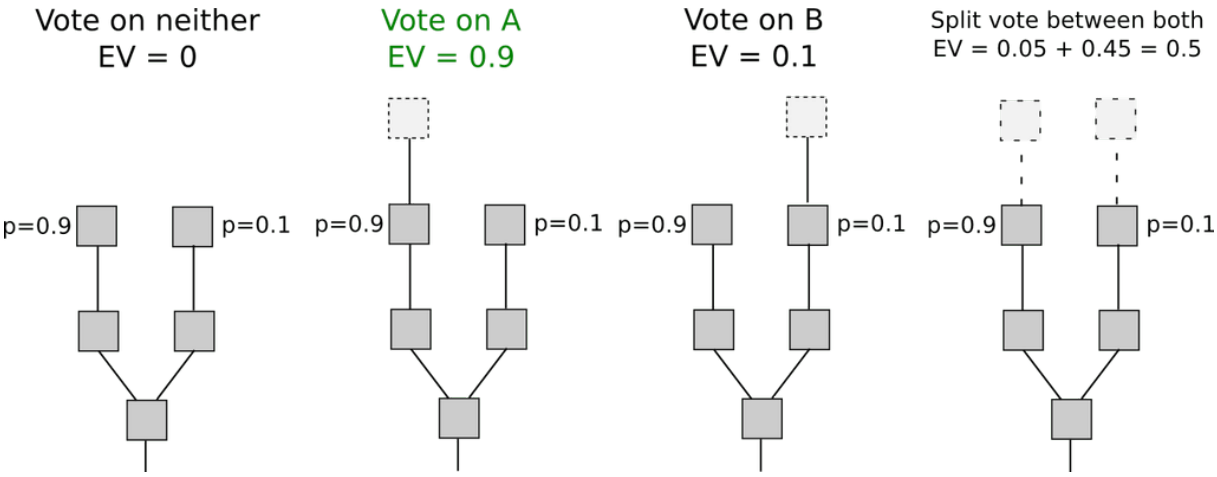
Du reste la génération du bloc est beaucoup plus économique en énergie et permet des cycles d'itération bien plu rapide. Néanmoins, cette méthode n'est pas dénué de défaut, et amènent de nouveaux risques absent de la méthode précédente.

Le Nothing at stake

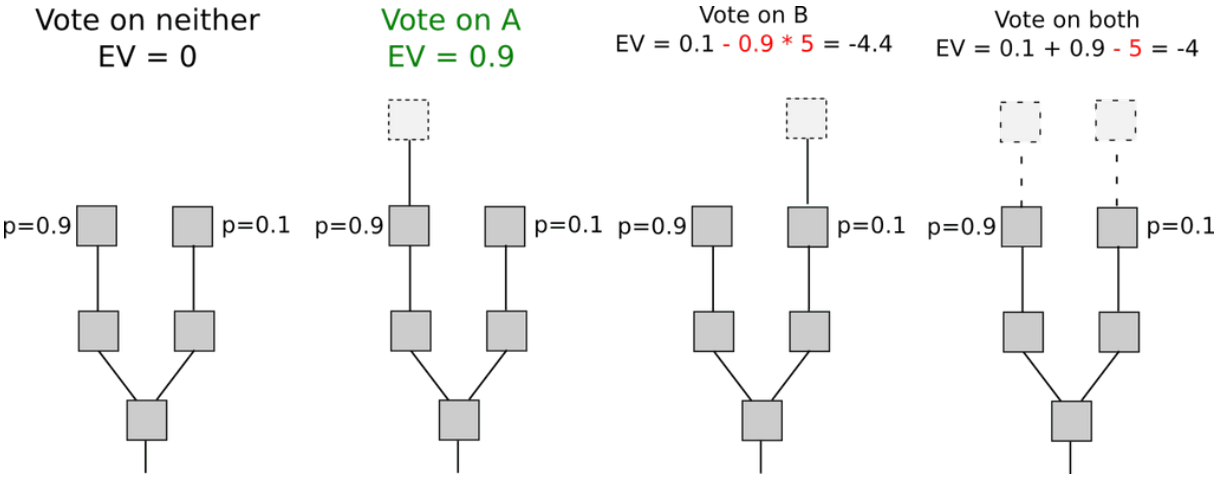
La problématique principale se présente lors de l'apparition d'un « fork » d'une blockchain qui désigne l'existence simultanée et contradictoire de deux états différents d'une même chaîne. Cette situation peut arriver aussi bien de manière accidentelle, du fait de la latence du réseau, qu'être une tentative de corruption malveillante. Un nœud mineur pourrait avoir tendance à créer le prochain nœud sur toutes les instances de la chaîne afin de s'assurer d'avoir participer à la bonne chaîne et ne pas risquer de perdre sa récompense. Au risque de ne jamais résorber le fork et de plonger la blockchain dans un état d'incohérence permanent.



La preuve de travail pallie facilement à se problème. En effet, le calcul d'un nouveau bloc étant une compétition particulièrement coûteuse, si un nœud calcul un bloc sur chaque chaîne, il a de forte chance de se faire devancer par un autre nœud se concentrant sur une seule occurrence de la chaîne. Tous les mineurs honnêtes se concentreront donc sur la chaîne la plus fiable, et le fork sera rapidement résorbé.



Par contre, sur système à preuve de participation, comme nous l'avons vu il n'y a pas de concurrence. Dans le cas d'un fork, le nœud élu pour la création du prochain bloc a tout le loisir de créer son nouveau bloc sur toutes les occurrences de la chaîne, car il n'a « rien à perdre » : « nothing at stake ». Comme on l'a vu plus haut, les mineurs en preuve de travail sont découragés de choisir ce comportement par une punition implicite. Il est donc nécessaire de mettre en place un mécanisme explicite de punition sur les blockchains en preuve de participation. Cela peut prendre plusieurs formes, mais revient grossièrement à infliger une « amende » à un nœud ayant produit un bloc sur la mauvaise chaîne. Cette amende restera normalement théorique, car son seul risque mènera toujours les nœuds honnêtes à choisir la bonne chaîne.



On peut le voir, le problème du nothing at stake peut se régler relativement facilement, au moins en théorie. Mais il faut garder à l'esprit que cette problématique ne se pose même pas en preuve de travail et que c'est aussi le cas de bien d'autres problèmes de sécurité nécessitant des réponses techniques particulièrement sophistiquées.

Limites de la preuve de participation

i. Vulnérabilité

La Preuve de participation est immunisée à la prise de contrôle d'un acteur possédant la majorité des nœuds. Sa validité est menacée seulement si un acteur possède 51 % de la masse monétaire totale, ce qui est jugé encore moins probable, sauf pour les blockchains les plus jeunes. Néanmoins elle propose de nombreux autres défis, que la preuve de travail élimine par son seul fonctionnement. Si la plupart des problèmes d'importance se sont vu apporter des réponses techniques, ces dernières sont généralement très complexes et ne garantissent pas toujours une absence de risque, seulement une probabilité extrêmement faible jugée acceptable.

ii. Valeur de la monnaie

Avec la preuve de travail, le coût élevé en temps et en énergie nécessaire à la création de nouveaux blocs et donc la création monétaire n'est pas qu'une affaire de sécurité et de simplicité. Elle vise à forcer la rareté de la cryptomonnaie afin d'en assurer la valeur, de la même manière que les banques centrales limitent l'émission de monnaie pour éviter l'inflation. Or, avec la preuve de participation, cette création monétaire est très peu coûteuse et sa monnaie étant créée en masse, sa valeur aura tendance a être très faible. C'est pourquoi elle n'aura de valeur réelle qu'au sein du réseau.

Bilan de la preuve de participation

Malgré ces défauts, la plupart des acteurs dans l'univers de la blockchain misent sur le développement de la preuve de participation. Il fait consensus que la seule contrainte de coût économique et écologique suffit pour se détourner de la preuve de travail. En effet, à lui seul, le réseau Bitcoin consomme plus d'énergie qu'un pays comme l'Irlande.

4. Conclusion technique

Toute technologie, et particulièrement dans les TIC, connaît un raffinement et une amélioration permanente. Mais il ressort de l'exploration technique approfondie que nous avons menée que la blockchain n'en est pas encore à ce stade, mais bel et bien en pleine constitution. C'est encore à l'heure de la réalisation de ce document un champ d'expérimentation en pleine ébullition qui n'a pas découvert toutes ses possibilités techniques.

De plus, il ne s'agit pas d'une technologie canonique ou même d'un protocole, mais d'un principe qui doit être adapté à chaque implémentation et utilisation réelle. Nous l'avons vu dans le cas principal de la méthode de consensus, mais c'est également vrai pour toutes les autres composantes, telles que la forme que prendront les données ou la méthode de communication entre les nœuds.

Cette double composante technique de l'expérimentation et de l'adaptation à son parallèle du côté des applications pratiques, qui nous allons le voir présentent les mêmes caractéristiques.

V. Utilisations

1. Les Crypto-monnaies

La première application de la blockchain qui vient a l'esprit est bien sûr la crypto-monnaie, puisque ces deux notions sont nées en même temps avec Bitcoin. Les crypto-monnaies sont des monnaies virtuelles et alternative, car non reconnues par des états ou banques centrales. Comme on l'a vu plus haut, la création de monnaie se fait par l'octroi d'un montant prédéfini lors d'un minage de bloc réussi, afin de récompenser le mineur et d'en encourager la participation. Mais une monnaie ne serait pas une monnaie sans la possibilité de s'en servir pour réaliser des transactions.

Fonctionnement des transactions

Le principe de fonctionnement des transactions est relativement simple et met en jeu la cryptographie asymétrique. Posséder des crypto-monnaie revient à posséder une « adresse » à laquelle est associé une quantité de « pièces ». Une adresse est constituée d'un couple de clés publique-privée.

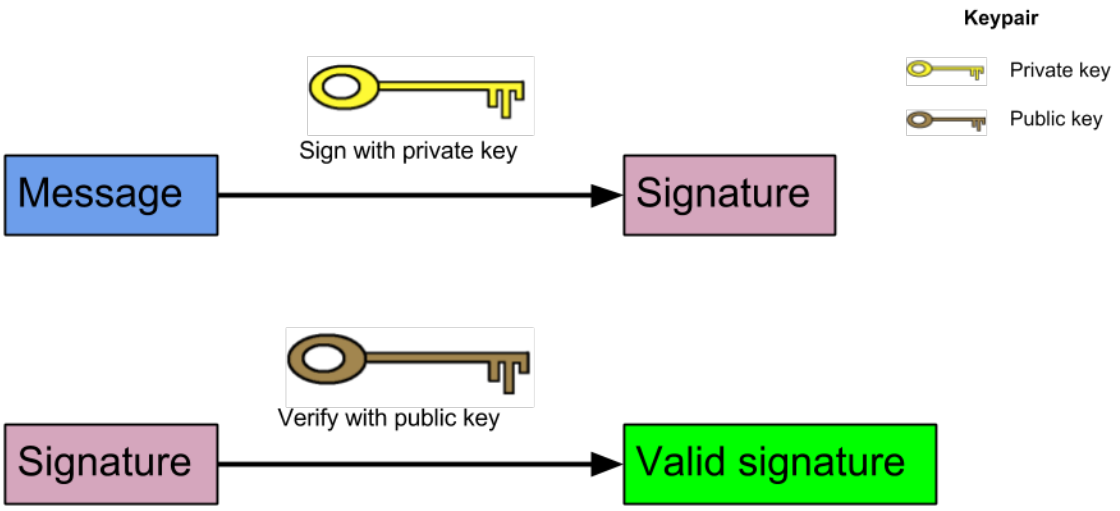
La partie publique est comme son nom l'indique la partie visible à tous. Elle permet à un tiers de transférer de l'argent vers l'adresse correspondant à cette clé et c'est cette dernière qui est utilisée pour journaliser, enregistrer et certifier les transactions au sein du réseau.

Le possesseur de la clé privée d'une adresse est donc le propriétaire des pièces qui y sont associées et cette clé est nécessaire à leur utilisation. Si l'acteur venait à perdre cette clé, il perdrait ses pièces. Si un tiers mettait la main sur une clé privée, il lui serait facile de trouver la clé publique et donc d'utiliser l'argent associé.

A la base, la génération de ce couple de clés se fait à l'aide d'algorithme de cryptographie connus et éprouvés, le plus populaire étant l'ECDSA. Les clés ainsi générées sont ensuite adaptées par la blockchain à son format spécifique selon un algorithme propre à chaque implémentation. Cette génération étant peu coûteuse car ne nécessitant pas la validation, hormis leur format, par le réseau lui-même, les acteurs sont fortement encouragés à utiliser plusieurs adresses, idéalement une par transaction dont ils sont le receveur.

Une transaction est donc constituée d'une adresse à « débiter », d'un montant et d'une adresse à « créditer ». Selon le principe de la cryptographie asymétrique, les données

sont cryptées (signées) grâce à la clé privée et décodées grâce à la clé publique. Il revient donc au payeur de créer la transaction et de la signer avec sa clé privée. Cela se fait généralement au travers d'un client propre à la cryptomonnaie.



La transaction est alors placée dans le pool des demandes de transaction en attente d'intégration à la chaîne. Dans le cas des cryptomonnaies, c'est ici qu'intervient l'étape de minage. Les transactions en attente constituent les données du bloc en instance de création. Grâce aux clés publiques, les mineurs peuvent vérifier la validité de la transaction. Une fois le nouveau bloc terminé et intégré à la chaîne, la transaction est validée de manière irréversible et le transfert de monnaie est effectif. Le contenu des blocs et donc des transactions est librement consultable, y compris par des personnes extérieures au réseau. Seules les clés sont présentes, et donc anonymes.

Exemple de transactions dans un bloc Bitcoin

Les plateformes d'échanges

La nouveauté et l'inventivité des crypto-monnaies a provoqué la curiosité des investisseurs et un fort désir d'achat. Or, si les blockchains gèrent et garantissent les transactions mettant en jeu leur propre crypto-monnaie, elles ne vont pas plus loin, et ne gèrent donc pas l'échange de crypto-monnaie contre d'autre type de valeur. C'est pourquoi, comme toute valeur financière, telles que les actions ou les matières premières, on a vu apparaître des plateformes d'échange spécialisées.

La première plateforme phare fut Mt. Gox, une société japonaise qui fut pendant plusieurs années la plus importante plateforme d'échange de bitcoins. Victime d'un piratage massif se soldant par le vol de centaines de milliers de bitcoins en février 2014, la plateforme s'effondra et disparut. Depuis, de nombreuses nouvelles plateformes sont apparues. Elles ont généralement une ou plusieurs monnaies de référence, qu'elles permettent d'échanger contre des monnaies traditionnelles, dites « fiat ».

Car les monnaies fiat, outre leur caractère « officiel », sont garanties par les états. Très tôt après leur création, les crypto-monnaies ont commencé à s'échanger contre des devises plus traditionnelles. Comme toute valeur pouvant s'échanger ainsi, les plateformes en font varier la valeur en fonction de l'offre et de la demande.

Le Krach

Les achats augmentant, leur valeur d'échange en monnaie fiat a eut tendance à augmenter. Le mécanisme spéculatif s'est mit en branle et leur valeur a augmenté de manière exponentielle, comme nous l'avons vu plus haut. Beaucoups ont mit en garde contre

la naissance d'une bulle spéculative, mais il aura fallu en attendre l'explosion pour voir les choses se calmer.

Comme souvent s'agissant de bulle spéculative, c'est un événement externe qui en a provoqué l'effondrement. Le développement incontrôlé des crypto-monnaies a finit par inquiéter le gouvernement chinois qui a fait part de sa volonté de les réguler voire d'en interdire l'échange sur son territoire et à ses citoyens. Cela a créé un mouvement de panique et une prise massive de gain, dans un mouvement inverse au premier temps de spéculation de la part des investisseurs, entraînant une chute brutale des cours. Inquiétés par cette instabilité, d'autres états ont manifesté un désir de régulation, ce qui n'a fait qu'accélérer le cours de l'effondrement général.

Beaucoup ont comparé ce krach à l'éclatement de la bulle internet, qui avait fortement ralenti au début des années 2000 le développement du secteur des technologies de l'information et de la communication. Il avait fallut attendre l'émergence du web 2.0 et des réseaux sociaux pour que l'innovation retrouve un rythme de développement rapide. De fait, de nombreuses personnes estiment que les cryptomonnaies vont connaître une période de recul avant de se stabiliser et qu'il sera nécessaire d'attendre une plus grande maturité de la technologie et particulièrement de ses applications pour la voir recommencer à se développer notablement.

L'après-Krach (MàJ mai 2018)

Quelques mois après la grande chute des cours des monnaies électroniques, force est de constater que la plupart d'entre-elles sont reparties à la hausse. Dans l'exemple du Bitcoin, malgré de nombreuses chutes brutales (septembre 2017 -40%, décembre -30%, janvier 2018 -40 % et mars 2018 -40 %), depuis janvier 2017 la crypto-monnaie à tout de même multiplié plusieurs fois sa valeur d'un peu plus de 1,000$ à environ 7,000$, en moyenne.

Néanmoins, la plupart des acteurs mettent en garde contre l'avenir à court et moyen terme de ces monnaies. Ils pointent en effet la volatilité extrême de cet actif et sa sensibilité au contexte international. En effet, dans la continuité de ce qui s'est passé en chine (cf sous-partie précédente) et qui a déclenché le premier krach de septembre, à chaque annonce par un état ou une institution d'importance d'un désir de légiférer, les investisseurs paniquent et revendent en masse. Du fait de l'opacité relative des opérateurs de la plupart des crypto-monnaies, ce souhait d'encadrement étant important, comme nous le verrons dans la partie consacrée à l'aspect légal.

Nous voyons donc qu'il est trop tôt pour se prononcer sur la pérennité de la crypto-monnaie en tant qu'actif financier.

Evolution du cours du bitcoin depuis novembre 2017

2. Les smart-contracts

Définition

La notion de contrat-intelligent, smart-contract en anglais, est bien antérieure à celle de la blockchain. Depuis les années 80 des chercheurs travaillent sur la théorie de contrats dont la négociation serait simplifiée, l'exécution et la sécurisation automatisée. La citation suivante définit bien la notion :

« Concrètement, les smart contracts sont des programmes, accessibles et auditables par toutes les parties autorisées, dont l'exécution est donc contrôlée et vérifiable ; conçus pour exécuter les termes d'un contrat de façon automatique lorsque certaines conditions sont réunies. »[1]

1 Steve Snodgrass « Mais à quoi servent les smart contracts ? », sur le site du Think Tank « equationdelaconfiance », consulté le 25/03/2018 http://equationdelaconfiance.fr/decryptage/mais-quoi-servent-les-smart-contracts

Fonctionnement

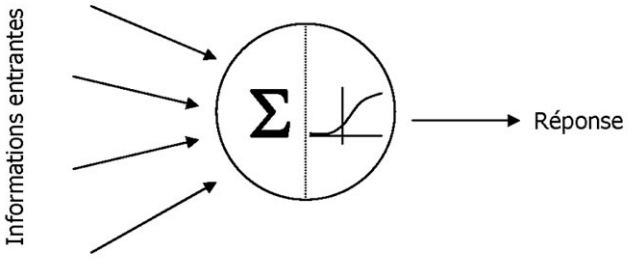
Un smart contract n'est ni plus ni moins qu'un programme écrit dans un langage informatique, généralement propre à la chaîne, et intégré à cette dernière comme n'importe quelle autre donnée. Ce programme est dans son essence composé de deux parties principales très classiques en programmation : des conditions et une exécution.

Conditions : Il s'agit simplement d'un ensemble de prédicats qui doivent être vérifiés. Par exemple, être un jour de la semaine donnée, trouver une écriture donnée dans une base, etc…

Exécution : C'est le « paiement » du contrat, les actions sur lesquelles se sont accordés les contractant.

Cela évoque tout de suite les neurones artificiels, leur faisceau d'informations entrantes (dendrites) et leur réponse unique (axone). On verra d'ailleurs plus loin que certaines utilisations des smarts contracts et la dépendance de ces derniers entre eux, revient à la création ad hoc de réseaux neuronaux simplifiés.

Figure 1 – Neurone artificiel (McCullogh et Pitts, 1943)



Limites et faiblesses

i. Conditions externes :

Dans le cas où les conditions sont internes à la blockchain (présence d'une certaine écriture ou transaction), ces dernières bénéficies des mêmes garanties que n'importe quelle donnée de la chaîne et cette dernière peut elle même les vérifier de manière absolument fiable. Mais le problème se pose dans le cas de conditions externes (résultat d'un match sportif, température extérieur, etc.) qui ne peuvent pas entre vérifiées par la chaîne. Cette dernière doit donc faire appel à l'un de ces tiers de confiance dont les smart contracts

voulaient justement s'abstraire. Il revient donc au contractants de désigner dans le contrat ces tiers connus et acceptés par les deux parties.

Il existe également des projets de services décentralisés de validation. Reprenant des principes de la blockchain, ces derniers reposent sur une grande quantité de participants qui vont chacun voter pour déterminer si ils valident la condition ou non, en cherchant à atteindre un consensus. Néanmoins, cela peut s'avérer trompeur car il faut garder à l'esprit qu'un tel système, dit Oracle, n'est pas plus garanti dans l'absolu d'avoir raison qu'un unique tiers de confiance. Tout au plus permet il de limiter le risque de malveillance.

ii. Contrats non modifiables :

Une des plus grandes forces du smart contract se révèle aussi être une de ses limites. Une fois intégré à la chaîne, un tel contrat est en effet très complexe à modifier. Le contrat original lui même est bien évidemment non modifiable, comme d'ailleurs un contrat « papier ».

Néanmoins, contrairement avec ce dernier, il apparaît difficile de produire un « avenant ». Au mieux peut on créer une nouvelle version du contrat qui viendra remplacer l'ancienne. Mais il reste impossible de « prévenir » le contrat original qu'il est obsolète, ce qui doit être vérifié dans les blocs plus récent de la chaîne. On voit bien que cela pourrait ralentir considérablement les traitements.

L'autre solution serait de mettre en place un contrat « inverse », avec les mêmes conditions mais une exécution « inversée ». Au delà du fait que cela ne soit pas toujours possible, cela double de fait les coûts d'exécution du contrat.

C'est pour ces raisons qu'aucune implémentation actuelle ne permet cette modification, et il est en pratique impossible de le faire sur les plateformes réelles de smart contract.

Usages possibles

Les usages des smart contracts en sont à leur balbutiement et il y a fort à parier que nombre d'entre eux n'ont pas encore été identifiés. C'est pourquoi nous avons choisi de sélectionner les quelques cas d'usages qui nous semblent les plus représentatifs, non dans leur objet ou leur finalité, mais dans leur manière d'utiliser les smart contracts.

i. Paiement d'une prestation

C'est le cas le plus simple et l'un des plus clairement utile. Dans le cas d'une prestation rémunérée, qu'il s'agisse d'un service ou de la vente d'une marchandise, l'une des

parties doit prendre des risques. Soit l'acheteur parie sur l'honnêteté du vendeur en le payant avant l'exécution de la prestation, soit le vendeur exécute la prestation sans garantie d'être payé. Le smart-contrat permet de s'abstraire totalement de ce risque.

Une personne A souhaite rémunérer une personne B pour la réalisation d'une prestation. Un smart-contrat est formalisé et enregistré sur la blockchain accompagné du montant du paiement de la prestation mis en gage par la personne A. Quand les conditions sont réuniees (la prestation a été effectuée par la personne B), le contrat est automatiquement exécuté et la personne B payée.

ii. Assurance

C'est un exemple beaucoup plus avancé de smart contract. Au delà de la sécurité et de la garantie détaillées dans la sous partie précédente, les smart contracts permettent ici des gains très importants dans la vérification et l'arbitrage. En effet un contrat d'assurance met potentiellement en interaction des acteurs dont le nombre et la diversité va bien au-delà des simples contractants. Il faut faire appel à des experts pour s'assurer des dommages et des causes, se référer à des décisions institutionnelles (pour la qualification d'une catastrophe), gérer les intérêts contradictoires ou les réclamations. Cela à pour effet que les prises en charges et remboursements sont généralement très complexes et très longs.

L'utilisation de smart contract permettrait d'automatiser, au moins en partie, les vérifications et d'accélérer les remboursements, voir les rendre totalement automatiques. Ces contrats pourraient se référer à des tiers de confiance ou des oracles pour ce qui est des données physiques (conditions météorologique par exemple). Les dégâts pourraient eux aussi être détectés et diagnostiqués de manière automatique grâce aux objets connectés, de même que les conditions de leur apparition.

3. Lutte contre la fraude

La fraude existe dans tous les domaines de l'économie, mais pour des raisons pratiques, on peut les regrouper dans deux formes principales. La première est la contrefaçon, pour ce qui concerne les objets physiques, qu'il s'agisse de violation de propriété intellectuelle, de non-respect des normes ou de mensonge sur les propriétés du produit. L'autre forme pourrait être assimilée à l'usage de faux et concerne la fraude financière, qu'il s'agisse par exemple d'usage de faux ou de fraude fiscale. Dans ces deux cas, la blockchain apporte des possibilités de sécurisation grâce à sa caractéristique phare, l'infalsifiabilité.

Avec le développement des échanges internationaux, la contrefaçon est une réalité plus présente que jamais. Même quand le consommateur souhaite et pense acheter des produits authentiques, il peut être victime de la contrefaçon. Et cette fraude peut concerner

des secteurs particulièrement sensibles tels que l'alimentaire ou les médicaments. Si les pays en voie de développement sont particulièrement concernés (scandales alimentaires à répétition en Chine, médicaments contrefaits en Afrique), les pays occidentaux ne sont pas épargnés, comme on a pu le voir avec le scandale de la viande de cheval dans des plats déclarés comme étant au bœuf.

La solution imaginée par plusieurs acteurs se place là encore dans la continuité des objets connectés et plus particulièrement de la traçabilité qu'ils permettent. Tous les échanges et les prestataires intervenant dans la vie du produit sont enregistrés dans la chaîne, permettant de tracer avec fiabilité.

Cette chaîne a ceci d'intéressant qu'elle est non seulement horizontale, tous les acteurs d'un même niveau pouvant s'assurer du respect des règles par les autres, mais également verticale, puisqu'elle lie entre eux producteurs et distributeurs.

4. KYC

Définition

Le KYC est l'acronyme de Know-Your-Customer, pour « Connais Ton Client ». Il s'agit du processus permettant de vérifier l'identité des clients d'une entreprise afin de lutter contre l'usurpation d'identité. Il s'avère critique dans le contexte de l'économie dématérialisée afin de s'assurer de l'identité des participants à une transaction. Pour les gouvernements, il s'agit également de lutter contre la fraude, le blanchiment ou le financement du terrorisme.

Contexte

Dans le contexte français, cette obligation visant particulièrement les entreprises de la *fintech*, « technologie financière », a été renforcée en 2016 par la loi dite Sapin 2. Il s'agit de la traduction dans le droit français d'une directive européenne imposant aux établissement financier une connaissance approfondie des participants à une transaction, aussi bien du donneur d'ordre que du bénéficiaire.

Les sanctions aux manquements étant particulièrement élevée, la nouvelle législation est tout de suite devenue une priorité dans de nombreuses entreprises. D'autant plus que si des solutions institutionnelles (Grand registre des bénéficiaires) sont en cours de démarrage, les obligations sont elle déjà effectives et les sociétés doivent s'y conformer.

Le KYC se fait au travers du stockage de documents officiels tels que des extraits Kbis fournis par le greffe du tribunal de commerce pour les entreprise ou la carte d'identité pour

les particuliers. Or la captation, la gestion et la validation de ces documents est complexe et coûteuse.

D'un autre côté, on assiste depuis le début de l'année 2018 à une préoccupation de plus en plus importante concernant le respect de la vie privée et le droit d'accès aux informations personnelles des utilisateurs du numérique. Un renforcement législatif au niveau français, européen voir international est d'ors et déjà en cours et les professionnels de l'information sont à la recherche de solutions d'avenir. Pour l'utilisateur, il faut transmettre toujours les mêmes documents à ses différents prestataires. On assiste donc à une redondance généralisée aux deux extrémités.

Apport de la blockchain

Plusieurs banques travaillent à l'utilisation de la blockchain pour la gestion du KYC. La blockchain permettrait de passer d'une gestion menée individuellement par chaque acteur à une gestion collective. L'aspect distribué des données permettrait un unique cycle de captation / validation par document.

Les différents documents et informations permettant l'identification d'une personne, morale ou physique, constituerait les données en formant les blocs. Grâce à la cryptographie asymétrique, les acteurs qui en ont la possibilité pourrait inscrire sur la blockchain avoir validé tel ou tel document appartenant à un portefeuille donné. Les mineurs ne seraient autre que les différents acteurs financiers (banques, market places, institutions telles que la Banque de France, etc...) assez nombreux pour garantir, comme nous l'avons vu plus haut, la non falsifiabilité des données.

La personne possédant le portefeuille aurait également son propre jeu de clé, qui lui permettrait de savoir et de gérer ce qui se rapporte à elle sur la chaîne ainsi que d'utiliser sa clé privée pour ouvrir ou fermer l'accès à un document à un autre acteur, lui offrant ainsi un contrôle total de ses informations personnelles.

VI. Exemples d'applications

1. Ethereum : le pionnier du smart contract

Si Bitcoin proposait déjà de créer des smart contracts, cette fonctionnalité reste néanmoins limitée et c'est Ethereum qui fut la première blockchain grand public à proposer une implémentation complète du smart contract.

Un vrai langage de programmation

Les smart contract n'étant rien d'autre que des programmes exécutés sur la chaîne, ils nécessitent un outil en permettant la programmation. Là où Bitcoin est limité par un langage de script ne connaissant qu'une centaine d'instructions préprogrammées, Ethereum a fait le choix d'un langage de programmation complet baptisé Solidity. Il s'agit d'un langage statiquement typé et interprété. C'est la blockchain elle-même qui va faire office de machine virtuelle pour exécuter le byte code compilé sur l'Ethereum Virtual Machine.

Un contrat pourrait être rapproché d'une classe dans la forme qu'il prend en Solidity. Il définit en effet des attributs et des fonctions. Il est également à noter que dans ce langage les contrats supportent l'héritage.

Une fois le contrat terminé il est nécessaire de le compiler en byte code. Le compilateur le plus courant pour Solidity est Solc. Il existe aussi un éditeur / compilateur en ligne nommé Remix.

Ce byte code devra ensuite être publié sur la blockchain. Cette étape nécessite du « gas » qui peut être acheté en Ethereum. Plus le byte code du contrat est important, plus le coût en gas sera élevé. De ce fait, il est nécessaire pour un développeur de penser à utiliser une blockchain privée pour pouvoir déboguer son application sans avoir à payer à chaque déploiement, par exemple avec une implémentation en mémoire d'Ethereum.

```
contract Mortal {
    /* Define variable owner of the type address */
    address owner;

    /* This function is executed at initialization and sets the owner of the contract */
    function Mortal() { owner = msg.sender; }

    /* Function to recover the funds on the contract */
    function kill() { if (msg.sender == owner) selfdestruct(owner); }
}

contract Greeter is Mortal {
    /* Define variable greeting of the type string */
    string greeting;

    /* This runs when the contract is executed */
    function Greeter(string _greeting) public {
        greeting = _greeting;
    }

    /* Main function */
    function greet() constant returns (string) {
        return greeting;
    }
}
```

Exemple d'un smart contract programmé en Solidity

Un contrat déployé disposera d'une adresse sur la chaîne qui permettra à n'importe qui en disposant de l'appeler. Ceci ce fait au travers du terminal proposé par Ethereum CLI. Un appel à un contrat « statique » qui ne modifie pas la chaîne pourra être gratuit, mais l'appel à une fonction qui modifie cet état nécessitera là encore de payer un montant de gas. Tous les montants en gas prélevés sont reversés aux mineurs de la chaîne afin d'inciter ces derniers à continuer de fonctionner malgré la baisse progressive de ce que rapporte le minage lui même.

Usages

Les usages de l'Ethereum sont exactement les mêmes que ceux présentés dans la partie consacrée au smart-contracts, principalement l'internet des objets, la traçabilité et la lutte contre la fraude. En janvier 2018, plus de 250 applications utilisant la chaîne Ethereum étaient répertoriées. La plupart des projets sont issues de start-ups, mais également de poids lourds de l'industrie numérique, tel que Microsoft ou IBM. Il est à noter que généralement, les grandes entreprises s'intéressant à l'Ethereum préfère travailler, au moins dans un premier temps, avec une instance privée de la chaîne, indépendante de la chaîne public. Elles ont en effet les ressources nécessaires au maintient de leur propre chaîne.

Limites et problèmes

Malgré les promesses de sécurité d'Ethereum, reste que les contrats sont programmés par des humains et il reste impossible de s'abstraire de la défaillance humaine. La blockchain a déjà connu deux attaques réussies d'envergure en 2016 et Novembre 2017 qui ont eut pour conséquence le vol cumulé de 200 millions de dollars. Après une analyse d'un million de contrats présents sur la chaîne, des chercheurs du MIT en ont identifié plus de 34,000 comme présentant des vulnérabilités.

2. Lutte contre la fraude alimentaire

En Chine les scandales alimentaires dus à la fraude sont courants et coûtent la vie à plusieurs dizaines de personnes par an. La lutte contre la fraude alimentaire est donc une priorité. Ce pays immense très en retard concernant les instances de contrôle, contrairement par exemple à l'Europe de l'Ouest, mise donc beaucoup sur la blockchain.

L'entreprise pionnière dans la lutte contre la fraude alimentaire est sans conteste Walimai, fondée en 2015. Elle utilise à plein la puissance conjuguée de la blockchain et de l'internet des objets. En effet, la solution qu'elle propose se base sur une puce propre à chaque produit qui permet de l'identifier sur la blockchain. Chaque échange est enregistré au

sein de la blockchain. Cette traçabilité peut être consultée grâce à une application mobile en scannant simplement la puce.

Le géant chinois de la vente en ligne Alibaba, qui subit de nombreuses accusations en terme de contrefaçon, a lui aussi opté pour la blockchain. Il a fondé un ambitieux « Food Trust Framework », particulièrement tourné vers l'Australie et la Nouvelle-Zélande, deux gros exportateurs alimentaires réputés pour la fiabilité de leur contrôle.

VII. Contexte Légal

Il est devenu coutumier de constater que les différents cadres juridiques sont souvent en retard sur les différentes évolutions technologiques. Les technologies évoluent plus vite que le droit et on peut difficilement attendre du législateur qu'il légifère *à l'avance* sur des concepts qui n'existent pas encore.

Les blockchains évoluent donc encore pour une grande part dans un angle aveugle de la loi. Néanmoins, il semble que les institutions ont prit conscience de la nécessité d'encadrer les innovations, ne serait ce que pour poser des gardes fous le temps qu'elles atteignent leur maturité. De nombreux pays et institutions montrent déjà une volonté de prendre contrôle de la blockchain.

1. Enjeux légaux

Le premier enjeu est celui de la responsabilité, particulièrement en cas de défaillance ou de bug. En effet, la blockchain s'appuie sur des algorithmes écrits par des humains, et l'erreur reste possible. Hors en cas de conséquences dommageables, se pose la question de trouver qui est responsable. Les blockchains étant développées et maintenues par de nombreux développeurs, souvent anonymes, il devient compliqué de trouver un acteur défini contre lequel se retourner. Si les principaux acteurs (développeurs, mineurs) refusent de se laisser saisir par le droit, il reste nécessaire de statuer sur une résolution des éventuels conflits ou risquer de laisser se constituer une jurisprudence par à-coup et basée sur des lois non pertinentes pour ce cas précis.

De même, les différentes législations nationales et internationales fixent ce qui constitue un contrat et son caractère obligatoire. Bien que par nature un contrat de soit pas soumis à une exigence de forme, en pratique il existe des attendus quand aux informations nécessaires pour la reconnaissance du contrat. Dans bien des cas, il est même nécessaire, en plus de deux parties signataires, de faire appel à un acteur externe, investi d'une certaine légitimité, qui viendra acter le contrat (avocat, huissier, administration). Or il est évident que le *smart contract* sort complètement de ce qui est prévu et attendu. Et malgré son exécution automatique, il se posera très vite en cas de conflit la question des conditions juridiques de validité d'un tel contrat.

Nous verrons donc ci-après le contexte juridique actuel en France et dans le monde.

2. En France

La France a très vite compris la nécessité de se saisir du sujet. La « Loi pour la croissance, l'activité et l'égalité des chances économiques » du 6 août 2015, dite « Loi Macron » consacre une partie à la question des blockchains qui est rentrée en application avec l'ordonnance n°2016-520 du 28 avril 2016.

Selon les législateurs, cette loi poursuit deux objectifs : donner une définition juridique à la blockchain afin de combler un vide juridique et expérimenter l'application de la technologie au domaine financier sur un périmètre volontairement restreint.

La loi définit donc la blockchain comme un « dispositif d'enregistrement électronique partagé permettant l'authentification [d'] opérations »[2]. D'autre part elle acte que « le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L. 223-12, qui tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du Code civil »[3]. C'est donc en d'autres termes une reconnaissance de l'existence et de la force obligatoire du smart contract.

L'application est aujourd'hui limitée aux nouvellement créés « Minibons », des bons de caisse spécifiquement conçus pour le financement participatif. Le financement participatif, qui connaît une très forte évolution due en particulier aux plateformes numériques constitue en effet aux yeux du gouvernement français un champ d'expérimentation idéal pour la blockchain. En pratique, les minibons constituent des prêts à des sociétés commerciales qui peuvent être souscrits par des particuliers ou des acteurs institutionnels. Il est défini que « l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'Etat. »[4]

Dans la continuité, une ordonnance dont l'entrée en vigueur est prévue au plus tard pour juillet 2018 visera à étendre la caractère légal des transactions enregistrées dans une blockchain aux titres financiers non côtés.

Néanmoins, en pratique il apparaît que le Conseil d'État n'a pas encore fixé les « conditions » susmentionnées, l'application réelle reste donc bloquée.

Finalement, le gouvernement réfléchit à une expérimentation dans le cadre des collectivités territoriales, notamment dans la traçabilité des documents et pour les commandes publiques.

2 article L.223-12 du Code monétaire et financier français
3 idem
4 article L.223-12 du Code monétaire et financier français

3. Dans l'Union Européenne

Si l'Allemagne reconnaît le statut de monnaie au Bitcoin depuis 2013, pour ce qui est de la blockchain elle-même la France, avec les actions décrites plus haut, fait figure de précurseur en Europe. Si l'Union Européenne compte réguler la blockchain à l'avenir, elle refuse de mettre en place une réglementation avant l'avènement de réels modèles d'exploitation. Elle compte mettre en place une commission de surveillance mais se laisse un délai de 5 à 10 ans avant toute réelle législation.

4. A l'international

Légalisation japonaise

Une loi entrée en vigueur le 1er avril 2017 au Japon reconnaît officiellement les monnaies numériques comme légalement utilisables dans les échanges. Cela a participé à l'envol du cours des diverses crypto-monnaies au cours de cette année et s'ancre dans une adoption précoce des crypto-monnaies en Asie du sud est (en particulier Japon et Corée du sud). Plusieurs milliers d'entreprises acceptent désormais les paiements en crypto-monnaie, que ce soit dans l'hôtellerie, l'électronique ou les transports.

Pionnière dans la législation, son étude est particulièrement intéressante car elle préfigure certainement des conditions d'adoption des crypto-monnaies dans d'autres pays. Car au-delà de cette légalisation, la loi fixe aussi un cadre légal aux nombreuses plateformes japonaises. Elle impose une ouverture de compte beaucoup plus réglementée sur son territoire, imposant des processus plus stricts de KYC. Elle oblige également ces mêmes plateformes à faire preuve de plus de transparence dans les informations qu'elles communiquent à leurs clients à leur sujet. Ces dernières doivent également prouver que leur infrastructure est suffisamment sécurisée et qu'elles disposent d'un capital suffisant.

Finalement, le dernier point d'intérêt de cette loi est la distinction qu'elle fait entre les monnaies numériques, qui correspondent aux crypto-monnaies, et les monnaies électroniques, utilisées notamment par certaines market places et à l'usage beaucoup plus restreint.

Interdiction chinoise

A l'inverse, la Chine, où les crypto-monnaies connaissaient également le succès, a préféré interdire leur usage. Comme on l'a vu, cette interdiction effective au 1er novembre 2017 a déclenché la première d'une longue série de chute du cours des crypto-monnaies.

Elle vise tout échange en crypto-monnaie et en particulier les plateformes, qui ont soit disparu soit se sont délocalisées.

Dans les faits, de nombreux investisseurs se sont donc tournés vers l'étranger grâce à internet. A-t-elle point qu'en février 2018, le pays à lancer une campagne visant à empêcher l'accès aux plateformes étrangères à l'intérieur de ces frontières.

VIII. Bilan et préconisation

1. La blockchain n'est pas une fin en soi

Cette préconisation est sûrement valable pour la plupart des choix techniques, néanmoins il semble très important de souligner que l'usage de la blockchain ne devrait se faire que si le besoin le justifie vraiment. En effet, l'impact marketing non-négligeable des « buzz-words » cryptomonnaies, blockchains et smart-contract ne doit pas faire perdre de vue les limites et les inconvénients de la technologie. Elle souffre de problèmes inhérents, principalement dus à sa relative nouveauté, que nous avons explorés tout au long de ce dossier.

Au delà, il faut bien garder à l'esprit qu'engager une application sur la blockchain est certainement un choix définitif et qu'il sera très difficile, si c'est seulement possible, de revenir en arrière.

Mais dans son principe, la blockchain fonctionne. Ses objectifs d'infalsifiabilité et de distribution sont remplis. Pour vraiment juger de l'utilisabilité de ce concept dans un environnement industriel, il est nécessaire de faire abstraction de l'actualité autour des crypto-monnaies.

2. Blockchain privée ou public ?

Une grande partie des risques et des ressources qui seront mis en jeu par une application blockchain dépend de ce choix majeure : faut il utiliser une blockchain publique existante ou créer sa propre instance ?

Blockchain publique

C'est le moyen le plus simple et le plus rapide de créer une application utilisant la blockchain, beaucoup d'entre-elles ayant été créée avec cette finalité. En échange d'un coût d'utilisation, en général via l'achat et la dépense de crypto-monnaie, il est possible de s'intégrer à la blockchain et d'utiliser ses possibilité : stockage de données, transactions, smart-contracts. La blockchain choisie doit donc proposer une API complète et efficace pour interagir avec elle.

Cela permet de réduire drastiquement les coûts de développement et de maintenance, mais lie de manière forte l'application à la blockchain choisie. En effet, si une migration reste possible, elle peut s'avérer complexe et les données déjà enregistrées sur la chaîne ne pourront pas en être effacé. De plus, pour ce qui est d'éléments « vivants », tels que les smart-contracts, une migration sera pour le moins aventureuse, si elle n'est pas complètement impossible.

C'est donc certainement un choix à réserver aux start-ups ou aux projets de type « proof of concept » visant à prouver la faisabilité et la viabilité d'un concept.

Blockchain privée

C'est le choix qui est d'ors et déjà fait par les entreprises et institutions déjà bien installées parmi lesquelles : IBM et Microsoft pour l'informatique ou Barclays et UBS pour les banques. Généralement, il ne s'agit pas de recréer une blockchain depuis le début, mais plutôt de récupérer des programmes existants pour en mettre en place une instance indépendante et adaptée au besoin. Ethereum est d'ailleurs souvent prise pour base.

Elle nécessite évidemment que des ressources conséquentes soient affectées au projet, pour sa création puis pour sa maintenance qui peut s'avérer coûteuse. De plus, elle nécessite de la part de l'initiateur du projet de disposer d'un capital confiance et/ou d'une certaine autorité (ou d'adopter une philosophie open-source) pour inciter les autres acteurs à utiliser la chaîne.

C'est faire le choix du contrôle, justifié pour des projets visant la pérennité et la stabilité par des initiateurs aux épaules solides.

3. Dans quels cas utiliser une blockchain ?

Ces clarifications faites, il se dégage un type d'application pour laquelle le .

Base de donnée distribuée entre de nombreux acteurs

C'est sûrement ici que se trouve les vraies possibilités offerte par la blockchain, car il est fait usage à plein des possibilités offertes par la technologie. L'idée de ce type d'application est d'offrir un outil commun à des acteurs qui travaillent ou veulent travailler ensemble. C'est particulièrement intéressant dans un contexte qui présente les caractéristiques suivantes :

- Nombreux acteurs

- Nombreuses transactions entre les acteurs
- Données publiques

En pratique, les applications « réelles » qui semblent les plus intéressantes sont les suivantes :

- Sécurisation d'une chaîne d'approvisionnement
- Décentralisation des transactions d'une market place
- Gestion personnalisée de l'utilisation de ses données (notamment personnelles)

Cela se recoupe notamment avec bon nombre des projets déjà lancés par les acteurs d'importance et qui ont déjà été évoqués.

IX. Conclusion

Les applications réelles des blockchains en sont à leur balbutiement et il ne s'agit encore bien souvent que de promesses. Mais c'est un domaine en pleine effervescence ou les expériences se succèdent les unes aux autres.

De plus, si la blockchain est avant tout une articulation de concepts pré-existants, elle doit elle même s'articuler avec d'autres concepts émergeant pour réaliser son plein potentiel. Il dépend notamment des avancés concernant l'Internet des Objets pour ce qui est de s'« interfacer » avec le monde physique.

Finalement, outre son manque de maturité, de nombreux défis se présentent à la blockchain. Les réseaux les plus anciens, Bitcoin en tête, souffrent d'une crise de croissance qui voit l'intégration de nouvelles données au réseau demander de plus en plus de temps. Et de nombreux observateurs s'inquiètent des impacts environnementaux potentiels d'une technologie très gourmande en énergie.

X. Glossaire

Blockchain : Registre de faits ou de transactions horodatés et triés chronologiquement et partagé sur de nombreux serveurs.

Bloc : Élément constitutif d'une blockchain, maillon de la chaîne.

Cryptographie asymétrique : Principe de cryptographie basé sur un couple de clés publiques / privées. La clé publique permettant d'encrypter des données qui ne pourront être décryptées que par le possesseur de la clé privée.

Know-Your-Customer (KYC) : Obligation et par extension processus permettant de vérifier l'identité des clients d'une entreprise

Mineur : Nœud de la chaîne participant à la création de nouveau blocs.

Nœud : Instance de la chaîne sur le réseau.

Réseau pair-à-pair : Réseau horizontal dont chaque membre est à la fois client et serveur,

Smart-contract : Programme qui s'exécute sur la chaîne lorsque les préconditions sont remplies.

XI. Webographie

Description Technique

Article wiki par la Peer-to-peer Foundation « Blockchain » dans sa version du 08/01/2018 consultée le 19/01/2018
http://wiki.p2pfoundation.net/Blockchain

HARTIKKA Lauri « Naivecoin: a tutorial for building a cryptocurrency » consulté le 19/01/2018
https://lhartikk.github.io/

Article Wikipedia « Proof-of-work system » dans sa version du 09/01/2018 consultée le 22/01/2018
https://en.wikipedia.org/wiki/Proof-of-work_system

Article Wikipedia « Hashcash » dans sa version du 02/01/2018 consultée le 22/01/2018
https://en.wikipedia.org/wiki/Hashcash

ACHESON Noelle (06/06/2016), « How does Proof of Work, um, work ? », sur le site Decentralize Today, consulté le 22/01/2018
https://decentralize.today/how-does-proof-of-work-um-work-f44642b24215

Article YouCoin.ch « Que signifie la « difficulté » ? » consulté le 28/02/2018
http://youcoin.ch/questions-reponses-faq/que-signifie-la-difficulte/

Article BitCoinWiki « Technical background of version 1 Bitcoin addresses » dans sa version du 28/10/2017 consultée le 01/03/2018
https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

TERUZZI David (14/036/2016) « Les consensus: Proof of work vs Proof of stake », sur le site BlockchainCafé, consulté le 07/03/2018
http://blogchaincafe.com/les-consensus-proof-of-work-vs-proof-of-stake

« The Greeter » : getting started tutorial sur le site Ethereum.com, consulté le 10/05/2018
https://www.ethereum.org/greeter

Usages et actualité

LESAGE Nelly (16/01/2018), « La Chine met la pression sur les échanges de crypto-monnaies », sur le site Numérama, consulté le 02/03/2018

https://www.numerama.com/business/321916-la-chine-met-la-pression-sur-les-echanges-de-crypto-monnaies.html

Article Wikipedia «Contrat intelligent» dans sa version du 25/12/2017 consultée le 25/03/2018
https://fr.wikipedia.org/wiki/Contrat_intelligent

SNODGRAS Steve « Mais à quoi servent les smart contracts ? », sur le site du Think Tank Equation de la Confiance, consulté le 25/03/2018
http://equationdelaconfiance.fr/decryptage/mais-quoi-servent-les-smart-contracts

Article Wikipedia «Know your customer» dans sa version du 16/04/2018 consultée le 17/04/2018
https://fr.wikipedia.org/wiki/Know_your_customer

FREDOUELLE Aude (20/05/2016), «Banques : comment la blockchain va révolutionner la connaissance client», sur le site Journal du Net, consulté le 17/04/2018
https://www.journaldunet.com/economie/finance/1178642-5-manieres-dont-la-blockchain-va-revolutionner-la-finance-kyc/

ORIOT Linda (30/01/2018), «BBlockchain et KYC : premier pas vers l'identité numérique ?», sur le site La ChainTech, consulté le 17/04/2018
https://www.chaintech.fr/blog/blockchain-kyc-identite-numerique/

POLROT Simon (20/03/2016), «Smart contract, où le contrat auto-exécutant », sur le site Ethereum France, consulté le 21/04/2018
https://www.ethereum-france.com/smart-contract-ou-le-contrat-auto-executant/

LEPLATRE Simon (27/03/2017), «Alibaba fait appel à la blockchain pour lutter contre les faux produits alimentaires », sur le site Le Monde, consulté le 10/05/2018
http://www.lemonde.fr/economie/article/2017/03/27/alibaba-fait-appel-a-la-blockchain-pour-lutter-contre-les-faux-produits-alimentaires_5101397_3234.html

ORCUTT Mike (01/03/2018), « Ethereum's smart contracts are full of holes », sur le site MIT Technology Review, consulté le 10/05/2018
https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/

THAUREAUX Thierry (25/01/2018), « Solidity, langage des smart contracts », sur le site L'informaticien, consulté le 10/05/2018
https://www.linformaticien.com/dossiers/solidity-langage-des-smart-contracts.aspx#suite

Article Wikipedia « Ethereum » dans sa version du 03/05/2018 consultée le 10/05/2018
https://en.wikipedia.org/wiki/Ethereum

Article Wikipedia « Solidity » dans sa version du 04/05/2018 consultée le 10/05/2018
https://en.wikipedia.org/wiki/Solidity

Juridique et légal

Article Wikipedia « Loi pour la croissance, l'activité et l'égalité des chances économiques » dans sa version du 06/01/2018 consultée le 19/01/2018
https://fr.wikipedia.org/wiki/Loi_pour_la_croissance,_l%27activit%C3%A9_et_l%27%C3%A9galit%C3%A9_des_chances_%C3%A9conomiques

DE CHARENTENAY Simon (19/09/2017), « Blockchain et Droit: Code is deeply Law », sur le site BlockChain France, consulté le 19/01/2018
https://blockchainfrance.net/2017/09/19/blockchain-et-droit/

MARGNOUX Pierre-Yves, TESSONNEAU Alexandre (09/2016), « La France confère une valeur légale à la blockchain », sur le site Global Security Mag, consulté le 19/01/2018
http://www.globalsecuritymag.fr/La-France-confere-une-valeur,20160924,65548.html

LAUSSON Julien (12/12/2017), « Le gouvernement ouvre l'usage de la blockchain pour l'échange de titres financiers », sur le site Numerama, consulté le 19/01/2018
https://www.numerama.com/politique/313870-le-gouvernement-ouvre-lusage-de-la-blockchain-pour-lechange-de-titres-financiers.html

ZIGNANI Gabriel (31/10/2017), « Expérimentation de la blockchain dans les collectivités : quelles possibilités ? », sur le site La Gazette des Communes, consulté le 19/01/2018
http://www.lagazettedescommunes.com/532710/experimentation-de-la-blockchain-dans-les-collectivites-quelles-possibilites/

LUCCHESE Vincent (28/09/2017), « Le Japon se lance dans la monnaie virtuelle », sur le site Usbek et Rica, consulté le 10/05/2018
https://usbeketrica.com/article/le-japon-se-lance-dans-la-monnaie-virtuelle

TIANA (psudonyme) (10/11/2017), « La Chine officialise l'interdiction des échanges de crypto-monnaies », sur le site Coin24, consulté le 10/05/2018
https://coin24.fr/2017/11/10/chine-officialise-linterdiction-echanges-de-crypto-monnaies/

YU Xie (07/02/2018), « China to stamp out cryptocurrency trading completely with ban on foreign platforms », sur le site South China Morning Post, consulté le 10/05/2018
http://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-cryptocurrency-trading-completely-ban

Bilan et préconisations

HOCHSTEIN Marc (14/01/2018), « Don't Use a Blockchain Unless You Really Need One », sur le site CoinDesk, consulté le 21/05/2018
https://www.coindesk.com/dont-use-blockchain-unless-really-need-one/

CARDIANL David (15/03/2018), « How to Tell if You Should Use Blockchain in Your Application », sur le site ExtremTech, consulté le 21/05/2018
https://www.extremetech.com/extreme/265480-tell-use-blockchain-application