efcse.eu

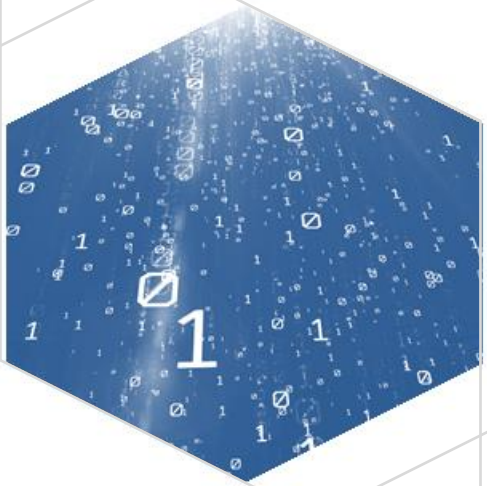
QU'EST-CE QUE LA BLOCKCHAIN ?

Par Marius LOMBARD-PLATET,
ENS, Be-studys, WG-4 EFCSE.

30/10/2019

La blockchain soulève les questions et attise les passions. Certains n'y voient qu'une bulle sur une technologie énergivore et peu sécurisée, d'autres ne cessent d'en chanter les louanges.

Faisons le point.



A propos de l'auteur

Marius LOMBARD-PLATET

Ingénieur diplômé de l'École Centrale Paris, il a également un Master II en recherche informatique de l'Université Paris-Saclay.

Actuellement doctorant en sécurité de l'information à l'ENS Paris, sous la direction de David Naccache et Pascal Lafourcade, il travaille sur les applications pratiques de la blockchain ainsi qu'à la sécurité des protocoles d'échange. Cette thèse est en partenariat avec la société Be-Studys, où il œuvre en tant qu'ingénieur de recherche.

Un nouveau mode de paiement

C'est en 2008 que fut publié Bitcoin, sous la plume d'un auteur inconnu au pseudonyme de Satoshi Nakamoto. Son implémentation se fit la même année, faisant de Bitcoin la première monnaie décentralisée. Pour créer cette monnaie non régulée par une banque centrale (traditionnellement responsable de l'émission de nouvelles liquidités et de la validité des transactions) Nakamoto s'est appuyé sur son invention : la blockchain.

Qu'est-ce que la blockchain ? Pour donner une réponse concise, la blockchain (ou chaîne de blocs en français) est un type de registre, qui cherche à être inaltérable et décentralisé. Continuons : un registre est un endroit où l'on stocke des données ; inaltérable car toute transaction inscrite dans le registre ne peut être modifiée à moins de fournir un effort considérable ; et décentralisé car ne dépendant d'aucune autorité : les utilisateurs sont tous égaux, il n'existe pas de banque centrale.

Un registre inaltérable, on en comprend l'intérêt contre les fraudes. Mais pourquoi décentralisé ? L'intérêt est simple. Une banque peut se faire cambrioler ; mais il est dur de cambrioler un système qui n'a pas de banque.

Dans un système centralisé, les banques sont garantes de la sécurité. Dans un système décentralisé, c'est l'ensemble des utilisateurs qui assurent cette garantie, obligeant l'attaquant à contrôler 33 % voire 50 % du système pour mener une offensive. Ce qui en théorie est improbable, et garantit donc la sécurité du système.

Sécuriser les transactions

Cependant, sans autorité centrale, il faut que les participants soient d'accord sur l'ordre et la validité des transactions au sein du réseau. Pour ajouter un bloc de transactions, on suit un algorithme de minage. Chaque participant qui souhaite proposer un nouveau bloc de transactions (ces participants sont également appelés mineurs) doit consacrer un investissement sur ce bloc (voir l'encadré). Un des blocs proposés par les mineurs

sera alors adopté, par un algorithme de consensus sur le réseau, comme prochain bloc de la blockchain. Puis on recommence avec un nouveau bloc.

Avec ces algorithmes, plus il y a de participants, et plus il est difficile pour un attaquant de modifier une donnée déjà enregistrée. Pour réécrire l'historique Bitcoin, un attaquant doit pouvoir réécrire l'historique plus rapidement que le reste du réseau ne rajoute des blocs. Autrement dit, un attaquant doit posséder au moins 50 % de la puissance du réseau pour mener son attaque. Pour cela, l'attaquant doit augmenter sa propre puissance de calcul, ce qui augmente la puissance totale du réseau, et augmente d'autant la difficulté pour un autre attaquant. Autrement dit, sur une blockchain, un attaquant améliore la sécurité du système contre d'autres attaquants.

Pour autant, la blockchain n'est pas inviolable. Des attaques plus subtiles existent, via des bugs logiciels ou une attaque sur le réseau Internet de la victime. Qui plus est, en 2018 et 2019, les blockchains Verge, Monacoin, Zencash, Bitcoin Gold, Bitcoin Cash et Ethereum Classic ont toutes été victimes d'une « attaque des 51 % », cumulant plus de 20 millions d'euros volés. Quant à Bitcoin, une telle attaque n'est jamais arrivée… pour l'instant. En 2018, 58 % de la puissance de calcul du réseau Bitcoin est contrôlée par quatre entreprises chinoises, et la Chine contrôle environ 80 % de la puissance de calcul totale. De façon similaire, en 2014, le groupe Gash.io a contrôlé plus de 51 % de la puissance totale avant de se scinder lui-même : pour une monnaie décentralisée, c'est un comble !

CONSENSUS ET INVESTISSEMENT

L'investissement peut être du temps de calcul, comme pour la *proof of work* de Bitcoin : l'ordinateur du mineur effectue de nombreux calculs (inversion partielle de SHA256) avant de pouvoir proposer un bloc. Citons également :

- *proof of stake* : investir une partie de ses ressources dans la cryptomonnaie pour parier sur quel sera le prochain bloc. C'est ce qui est utilisé pour la blockchain PeerCoin.
- *proof of space* : investir une partie de son espace de stockage sur disque dur (c'est le cas de Chia) ;
- *proof of elapsed time* : investir du temps de disponibilité de processeur (Hyperledger Sawtooth) ;
- etc.

Pour encouragement, un mineur gagne de l'argent à chaque bloc accepté qu'il a proposé. Sur Bitcoin, la récompense est actuellement de 12.5 bitcoins par bloc.

Il est à noter qu'à l'heure actuelle, la *proof of work* est l'algorithme le plus commun, même s'il est le plus énergivore : on estime qu'actuellement Bitcoin consomme 73 TWh d'électricité par an, soit un peu plus que l'Autriche. Seuls 38 pays consomment plus.

Une multitude d'applications

Mais trêve de questions sécuritaires. Jusqu'ici nous n'avons parlé que d'une blockchain, le Bitcoin, et que d'une application, la monnaie virtuelle. Le paysage est pourtant bien plus varié.

Une blockchain peut servir de support à toute application qui a besoin d'un registre inaltérable et décentralisé. Parmi ces applications, on compte le vote électronique, la gestion d'identité (passeports électroniques), le suivi de produits dans une supply chain, le contournement de censure (puisque la blockchain, inaltérable, ne peut pas être censurée) … Pour chacun de ces exemples, au moins une blockchain existe déjà. De plus, le potentiel des blockchains est immense : grâce aux smart contracts, des programmes qui s'exécutent sur une blockchain (qui sont donc inaltérables et décentralisés), on peut coder à peu près ce que l'on veut.

Par ailleurs, une blockchain peut être publique ou privée, et ouverte à tous (anonyme, ou permissionless en anglais) ou accessible aux membres authentifiés seulement[1] (permissioned). Chacun de ces modes correspond à un besoin précis : une cryptomonnaie sera publique et anonyme, un système d'échange monétaire entre banques sera authentifié et privé.

Bref, le monde des blockchains est riche et varié. Mais gare aux sirènes ! La blockchain n'est pas une panacée, n'en déplaise à ceux qui l'utilisent à tort et à travers. Ainsi, la blockchain est une technologie dure à implémenter. Dans de nombreux cas, une simple base de données sera plus simple, moins chère, et bien plus susceptible d'être un jour déployée sur le marché. En effet, une blockchain nécessite de mettre en place un réseau – avec son lot de contraintes organisationnelles – entre divers acteurs, sur des technologies encore jeunes. Dans la charte du DHS (Department of Homeland Security), reprise par le NIST (National Institute of Standards and Technology), sont présentées plusieurs alternatives (figure 1).

[1] Le sujet fait débat : une blockchain authentifiée dépend d'une autorité qui filtre les utilisateurs, mais pas les échanges. Peut-on toujours parler d'un système décentralisé ?

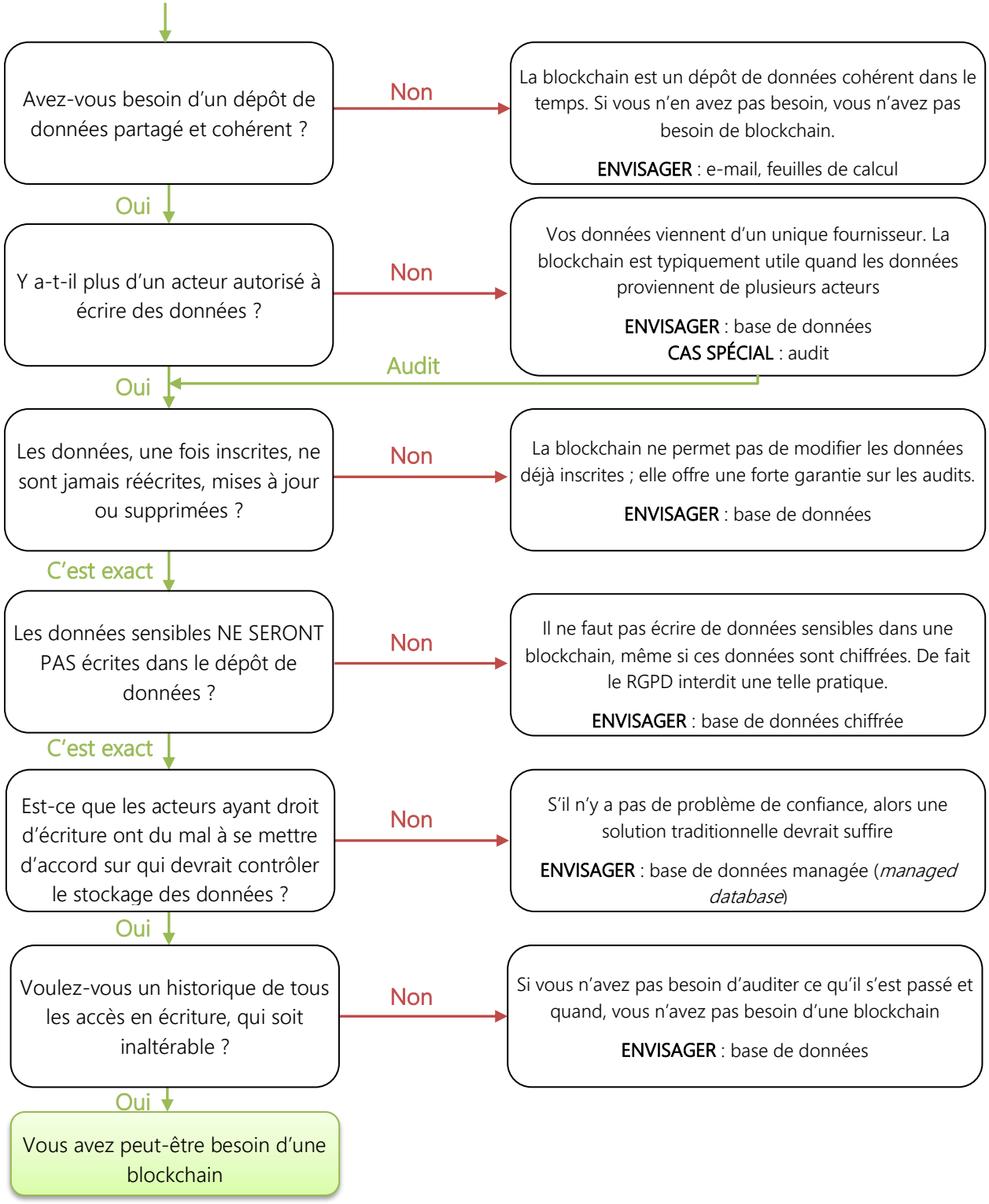


Figure 1 : Avez-vous besoin d'une blockchain ? (Traduction française du logigramme du DHS)

Par exemple : *My Health, My Data* est un projet européen H2020 qui permet aux hôpitaux de consigner les demandes d'accès à des données médicales. Les hôpitaux étant très soucieux de la confidentialité de ces données, aucun tiers de confiance n'est envisageable. Seules les entités accréditées peuvent accéder au système, ce qui implique l'utilisation d'une blockchain authentifiée privée.

À l'opposé, un système de suivi de *supply chain* à des fins internes (et donc pas d'audit) d'une seule entreprise n'a aucun intérêt à utiliser une blockchain : la blockchain est décentralisée, mais il n'y a qu'une seule entité dans le système. À quoi bon ?

En résumé, la blockchain est un nouvel outil de stockage de données (transactions financières, *smart contracts*, fiches de suivi…) qui offre de fortes garanties en termes de sécurité. Si ce n'est certainement pas l'outil miracle qui résoudra tous les problèmes de notre société, il n'en reste pas moins que c'est un outil extrêmement utile dans de nombreuses situations… à condition de savoir quand s'en servir.

EFCSE est organisée en groupe de travail dont l'un est dédié aux sujets de la BLOCKCHAIN

Contactez-nous via efcse.eu