Le fonctionnement de la *blockchain*

Par Gautier MARIN-DAGANNAUD
Élève-ingénieur à Télécom ParisTech – Institut Mines-Télécom et étudiant en master à l'École polytechnique, actuellement chez Ledgys

La *blockchain* est une technologie profondément disruptive. Pour en saisir le potentiel, il est indispensable de comprendre les bases de son fonctionnement à travers son cas d'usage originel, Bitcoin. Une *blockchain* est un registre distribué, c'est-à-dire partagé entre les acteurs d'un réseau. Comme dans tout registre, il y a des utilisateurs, qu'il faut pouvoir identifier, et des transactions, qui modifient l'état du registre. Cependant, à la différence de l'immense majorité des registres actuels, la *blockchain* fonctionne sans autorité centrale de contrôle. Cela implique de nombreux enjeux et problématiques techniques.

Les plateformes logicielles actuelles (Facebook, Amazon, Uber, banques en ligne) ont toutes un point commun, celui d'être organisées autour d'un acteur central chargé de maintenir leur intégrité et d'assurer leur développement. Cette centralisation a des avantages, notamment en termes de rapidité dans la gestion des conflits et de capacité à monter en charge, mais elle présente également de nombreux inconvénients, comme la censure, le monopole ou la vulnérabilité aux attaques.

La *blockchain* est une technologie permettant de partager une base de données de manière décentralisée, c'est-à-dire entre acteurs ne se faisant pas nécessairement confiance et sans entité centrale de contrôle. Elle rend possible la création d'un nouveau type de plateforme logicielle, les plateformes décentralisées. Pour bien saisir ce changement de paradigme, il est nécessaire de comprendre les bases du fonctionnement de cette technologie.

Comment fonctionne une *blockchain* ? L'exemple de Bitcoin

Les origines

À l'origine, la technologie *blockchain* a été inventée pour permettre la création de la première monnaie numérique décentralisée, le Bitcoin. Bitcoin est un système de paiement digital s'appuyant sur la crypto-monnaie du même nom. Comme dans tout système de paiement, il est nécessaire de tenir à jour un registre des comptes pour pouvoir connaître la balance financière de chaque utilisateur. Dans le monde « réel », ce sont les banques qui tiennent ce registre. Si l'on souhaite envoyer de l'argent à quelqu'un, il faut en faire la requête à la banque, puisque c'est elle qui tient les comptes. On parle d'organisme centralisé. Le principe fondamental de Bitcoin est relativement simple : au lieu que le registre soit maintenu par un seul organisme privé, il l'est de manière décentralisée. En clair, chaque ordinateur (appelé nœud) du réseau contient une copie du registre et aide à le maintenir à jour. Le registre est protégé par cette décentralisation. En effet, même si un ou plusieurs nœuds sont altérés ou détruits, le registre sera conservé tant que subsisteront des nœuds « honnêtes ».

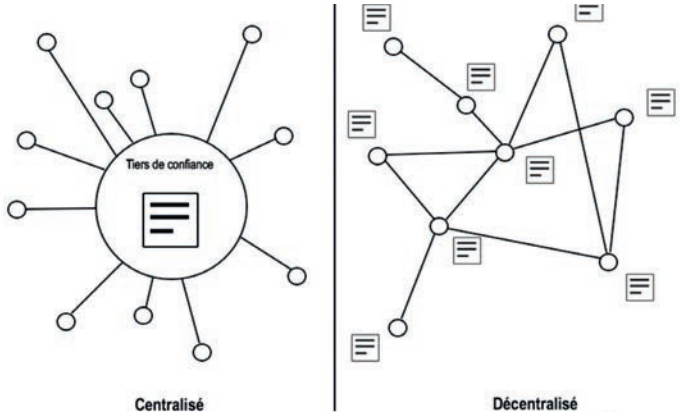

Figure 1 : Deux systèmes de maintien d'un registre : centralisé *vs* décentralisé.

Identifier les utilisateurs

Les utilisateurs du réseau sont identifiés par leur adresse, qui permet aux autres utilisateurs de leur envoyer des bitcoins. À chaque adresse est associée une clé privée. C'est elle qui permet de « débloquer » les fonds. L'adresse est générée en local par l'utilisateur à partir de sa clé privée, et ce, grâce à de complexes fonctions mathématiques, dont il suffit de retenir qu'elles fonctionnent à sens unique. S'il est quasiment impossible de trouver la clé privée associée à une adresse donnée, il est en revanche très facile de trouver l'adresse correspondant à une clé privée.

Pour débloquer les fonds, l'utilisateur n'a pas à communiquer sa clé privée au réseau. S'il le faisait, n'importe quel nœud la recevant pourrait dépenser les fonds associés à l'adresse correspondante. Au lieu de cela, il produit – toujours en local – une signature électronique associée à la transaction qu'il souhaite effectuer. Cette signature électronique prouve que la personne possédant la clé privée

a bien approuvé la transaction. Elle est unique, ce qui signifie qu'elle ne peut pas être réutilisée pour une autre transaction. De plus, la fonction permettant la création de la signature est elle aussi à sens unique. Les nœuds du réseau ne peuvent donc pas deviner la clé privée associée à cette signature.

Le mécanisme de la signature électronique permet donc d'autoriser des transactions sans révéler la clé privée au réseau. Si la signature électronique est un outil indispensable au fonctionnement de Bitcoin, ce n'est toutefois pas l'innovation apportée par la technologie *blockchain*.

Les bases de la *blockchain*

L'innovation de la technologie *blockchain* porte sur le consensus. Plus précisément, il s'agit d'apporter une solution au problème de la double dépense, un problème prépondérant dans tout système décentralisé. Supposons qu'un utilisateur signe et envoie au même moment deux transactions prenant pour point d'entrée le même bitcoin, mais ayant deux destinataires distincts. Certains nœuds recevraient l'une des deux transactions en premier, ce qui invaliderait la seconde, tandis que d'autres effectueraient le processus inverse. À l'échelle du réseau, il y aurait donc un désaccord sur l'état du registre.

Pour pallier ce problème, Bitcoin propose d'enregistrer de manière ordonnée et horodatée les transactions dans une chaîne de blocs avec laquelle chacun des nœuds doit se synchroniser : c'est la *blockchain*. Cette chaîne est unique et permet à tous les nœuds de s'accorder sur l'état du registre. Les blocs contiennent une liste des transactions qui modifient l'état du registre. L'ajout de blocs s'effectue au niveau de chaque nœud. Ainsi, tous les nœuds possèdent une copie à l'identique de la *blockchain* (à quelques subtilités près). Chaque bloc référence le bloc précédent, ce qui forme une chaîne de blocs qui s'étend jusqu'au « *genesis block* », le tout premier bloc à avoir été créé. Pour connaître l'état du registre à un instant donné, il suffit de remonter la chaîne des blocs depuis son origine jusqu'au dernier bloc ajouté avant l'instant considéré.

Le fonctionnement simplifié de la *blockchain*

Après avoir été générée par un utilisateur, une transaction est transmise aux nœuds voisins, puis relayée de pair en pair à travers le réseau. Pour qu'une transaction émise soit valide, il faut que l'utilisateur dispose des fonds requis et que sa signature soit valide. Cependant, une transaction n'est pas finalisée tant qu'elle n'a pas été incluse dans un bloc. De plus, deux transactions concurrentes, c'est-à-dire qui tentent de dépenser les mêmes bitcoins, ne peuvent pas être incluses dans le même bloc. Dans ce système, il est donc impossible d'effectuer une double dépense.

Reste à savoir quel nœud a le droit de créer le prochain bloc. Les nœuds créateurs de blocs sont des nœuds spéciaux que l'on appelle « mineurs ». N'importe quel nœud peut devenir un « mineur », il suffit pour l'internaute de disposer du matériel et du logiciel adéquats. Lorsqu'un mineur reçoit une nouvelle transaction non validée, il la place dans ce que l'on appelle « l'ensemble des transactions non confirmées ». Cet ensemble est propre à

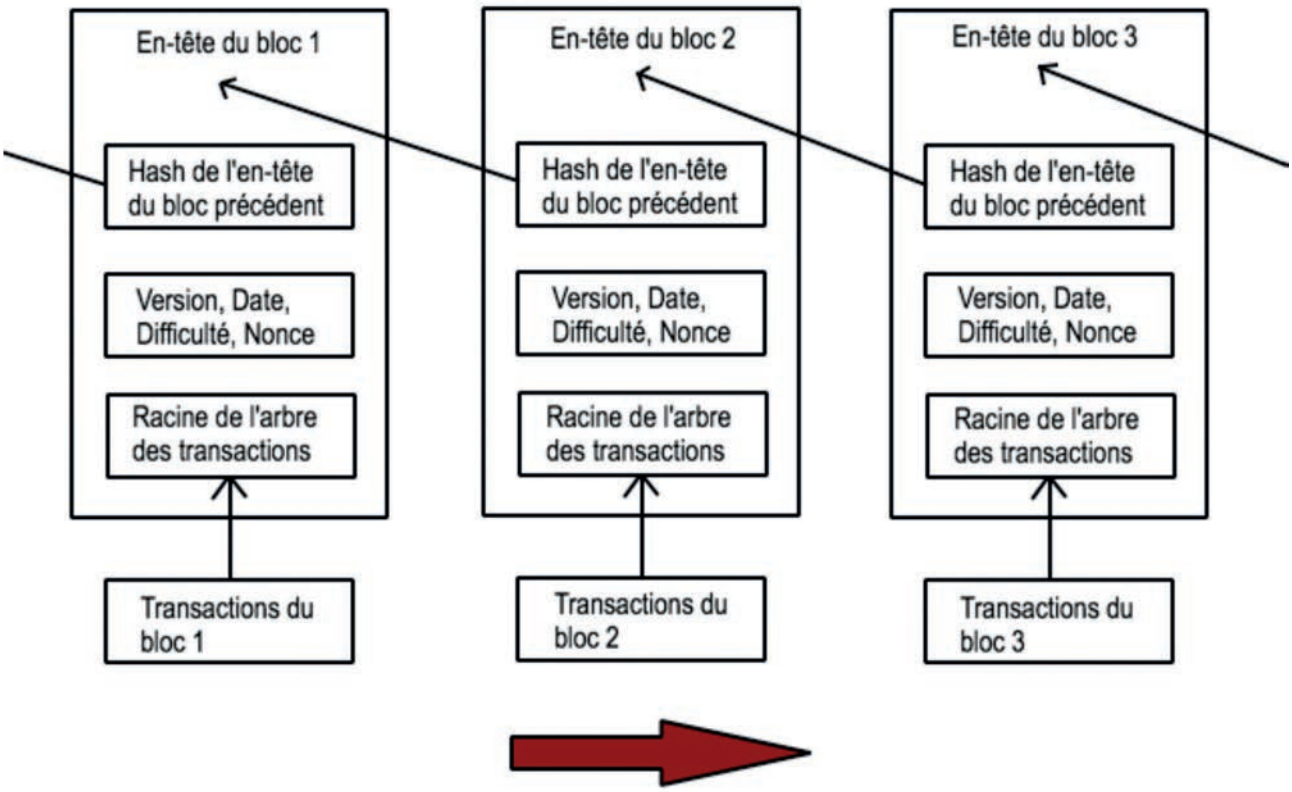

Figure 2 : Fonctionnement simplifié de la *blockchain*.

chaque mineur, il peut différer d'un mineur à l'autre du fait du temps de propagation des transactions sur le réseau. C'est une sorte de liste d'attente pour transactions, celles-ci en sortant une fois qu'elles ont été incluses dans un bloc.

Créer un bloc : la « preuve de travail »

N'importe quel mineur peut collecter un certain nombre de transactions dans sa liste, vérifier leur validité et former un bloc. Cependant, ce bloc ne sera pas validé tant que le mineur n'aura pas produit la « preuve de travail » (*Proof of Work*) associée au bloc considéré. Cette preuve de travail est une donnée difficile à produire, mais facile à vérifier. Sans cette donnée, le bloc ne peut pas être validé par les nœuds du réseau, même si les transactions qui le composent sont valides. Le fait qu'il soit difficile de créer cette donnée permet de décider lequel des blocs créés par les mineurs sera ajouté à la chaîne.

Pour produire cette donnée, les mineurs doivent calculer la valeur d'une fonction prenant pour entrées l'empreinte [1] (également appelée « *hash* ») du bloc précédent, l'empreinte des éléments du bloc actuel et un nombre variable, appelé « nonce ». Les mineurs font varier ce nonce jusqu'à ce que le résultat de la fonction réponde à des conditions prédéfinies par le protocole, notamment à un paramètre nommé « difficulté », qui permet de définir l'étendue des résultats valides. Plus la difficulté est élevée, et plus l'étendue est restreinte, ce qui rend la découverte d'un nonce valide plus compliquée. Il est également important de noter que, là encore, la fonction est à sens unique. Il est donc impossible de prédire à l'avance un nonce qui satisfasse aux conditions du protocole. Ainsi, le seul moyen de trouver un nonce valide est de faire calculer à sa propre machine un très grand nombre de nonces, d'évaluer pour chacun d'entre eux la valeur de la fonction et d'en vérifier la validité. Pour un seul nœud, il faudrait en moyenne plusieurs années pour trouver un bloc valide. À l'échelle du réseau, la difficulté est établie de telle sorte qu'en moyenne 10 minutes sont nécessaires pour qu'un nœud trouve un bloc valide. Si la preuve de travail est difficile à produire, elle est en revanche très facile à vérifier. Pour vérifier si une preuve est valide, il suffit d'évaluer la valeur de la fonction pour le nonce donné. On peut faire une analogie avec la combinaison d'un cadenas : trouver la combinaison par itérations est un processus très long, mais il est en revanche très facile de vérifier si une combinaison ouvre le cadenas – dans notre cas, si elle est valide.

La propagation des blocs

Une fois la preuve trouvée, le nœud « gagnant » ajoute son bloc à la chaîne. On dit qu'il a « miné » le bloc. Il reçoit en compensation une somme fixe déterminée par le réseau (12,5 bitcoins, aujourd'hui), ainsi que les éventuels frais de transaction. Bitcoin encourage donc les mineurs à entretenir le réseau en les récompensant par une rémunération. C'est par ailleurs de cette manière que des bitcoins sont introduits dans l'écosystème.

Ensuite, le mineur transmet le bloc au reste du réseau. Tous les nœuds qui le reçoivent vérifient la validité des transactions du bloc, ainsi que la preuve de travail, puis ajoutent le bloc à la chaîne. Si le nœud est un mineur en train de chercher un bloc valide, il doit reprendre le processus de création de bloc à partir de ce nouveau bloc créé (rappelons que tout bloc pointe sur le précédent). Il est possible qu'un nœud du réseau reçoive des blocs – ou des successions de blocs – valides concurrents. Dans ce cas, la règle est de toujours prendre la chaîne la plus longue comme référence.

Cette règle implique que pour qu'un attaquant fasse accepter aux nœuds du réseau sa version de la chaîne, il doit être en mesure de produire une chaîne de blocs valides plus longue que celle sur laquelle travaillent tous les autres mineurs « honnêtes ». En d'autres termes, il doit posséder plus de 50 % de la capacité de calcul du réseau. C'est ce que l'on appelle une « attaque 51 % ». Le réseau est donc d'autant plus sécurisé que la puissance de calcul combinée des mineurs est élevée. Notons tout de même qu'une telle attaque ne permettrait pas aux attaquants de voler des bitcoins, puisque ces derniers sont protégés par le mécanisme de signature digitale. Ils ne pourraient effectuer, tout au plus, que des doubles dépenses ou des dénis de service.

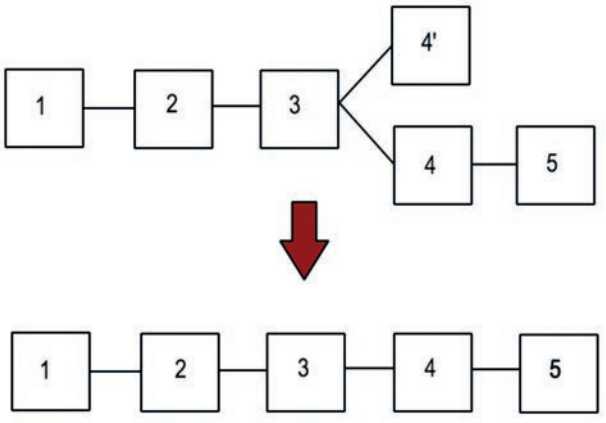

Figure 3 : Le basculement vers la chaîne de blocs la plus longue.

Au-delà de la monnaie

L'Internet de la valeur

Au départ, l'innovation technologique de la chaîne de blocs avait été éclipsée par son application première, la monnaie bitcoin. Cependant, il n'a pas fallu longtemps pour que l'on prenne conscience de son potentiel. Les bitcoins ne sont qu'une suite de 0 et de 1, ils peuvent être dupliqués sans effort. Comment s'assurer de la va-

(1) Une empreinte, ou hash, *est le résultat d'une fonction de hachage appliquée à une donnée initiale. La fonction de hachage est une fonction à sens unique. Son résultat est généralement un nombre hexadécimal (= de base 16) de taille fixe (256 bits, par exemple). Pour une même donnée initiale, on obtiendra toujours la même empreinte. En revanche, il est quasiment impossible de déterminer la donnée initiale à partir de son empreinte.*

leur d'un actif que l'on peut dupliquer indéfiniment ? Dans le cas de la monnaie fiduciaire, on a recours à des autorités centrales qui maintiennent l'intégrité du registre. Dans le cas de Bitcoin, c'est la *blockchain* qui assure la non-multiplication de la monnaie. Le principal intérêt de la *blockchain* est sa capacité à donner de la valeur à des actifs numériques, et ce, sans avoir recours à une autorité centrale.

Colored Coins et *Smart Contracts*

Les actifs numériques s'étendent au-delà de la monnaie. Par exemple, le protocole *Colored Coins* permet de représenter des actifs réels (actes de propriété, actions, obligations) *via* la *blockchain* Bitcoin. D'autres *blockchains* ont été créées pour faciliter la création de *tokens* (des jetons). Par exemple, Ethereum est une *blockchain* permettant le déploiement des contrats intelligents (*smart contracts*). Ces contrats sont des programmes dont l'exécution est assurée par les nœuds du réseau. Ils permettent d'automatiser la logique contractuelle et de la transposer aux actifs numériques. Avec Ethereum, il est possible de déployer une infinité d'actifs numériques valorisés par la *blockchain* et d'en automatiser la gestion grâce à des contrats intelligents. Une fois un tel contrat déployé sur le réseau, il est impossible d'en censurer l'exécution lorsqu'il est appelé, ni de l'annuler. Seul un consensus mondial de l'ensemble des acteurs du réseau – mineurs, développeurs, échanges et utilisateurs – peut permettre de revenir sur l'exécution d'un contrat. Cela fait de la *blockchain* le système le plus résistant à l'intervention d'un tiers parti que nous ayons jamais eu.

À nouvelles plateformes, nouveaux enjeux

Aujourd'hui, il existe des centaines de *blockchains* pour des centaines d'usages différents. De nombreuses plateformes décentralisées sont en train de voir le jour. Elles sont non propriétaires et *open source*, ce qui implique de nombreux changements en matière de répartition de la valeur. Les crypto-monnaies jouent un rôle très important dans cette répartition. En général, une crypto-monnaie spécifique à une plateforme est créée lors de son lancement. Elle est répartie selon les règles programmatiques qui régissent la plateforme, règles qui peuvent elles-mêmes évoluer conformément aux mécanismes de gouvernance spécifiques à la plateforme, de sorte que la répartition de la monnaie tende vers un optimum. Dès lors, chaque acteur de la plateforme est récompensé en fonction de son apport à l'écosystème, dans une logique de libre marché. Cela contraste avec les plateformes existantes, dans lesquelles l'autorité centrale est chargée de répartir la valeur et les responsabilités.

Des points de centralisation existent encore à l'heure actuelle. Notamment les plateformes d'échange de crypto-monnaies sont, dans leur immense majorité, opérées par des organisations centralisées. Cependant, des échanges décentralisés sont en cours de développement. Il existe même des projets visant à connecter les *blockchains* entre elles, et ce, de manière décentralisée. Ce serait là entrer dans un monde de plateformes interopérables sans friction.

Cependant, de nombreux défis d'ordres technique, légal et organisationnel restent à relever – avant de pouvoir y arriver.

Références sur la Toile

http://bitcoin.stackexchange.com/questions/22/is-it-possible-to-brute-force-bitcoin-address-creation-in-order-to-steal-money

https://www.reddit.com/r/BitcoinBeginners/comments/3eq3y7/full_node_question/ctk4lnd

https://bitcoin.org/en/developer-guide#block-chain

http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

https://github.com/ethereum/wiki/wiki/White-Paper

https://en.bitcoin.it/wiki/Main_Page

http://bitcoin.stackexchange.com/questions/11054/understanding-spv-simple-payment-verification