Le Bitcoin : motivations et fonctionnement

Lilian Pattier

1er octobre 2018

Résumé

De toutes les innovations technologiques que l'on a pu voir naître ces dernières années, il en est une qui sort particulièrement du lot : le Bitcoin. Cette cryptomonnaie, dont le nom est familier de tous mais dont le fonctionnement reste encore énigmatique pour la majorité, s'est imposée dans le domaine des monnaies non centralisées. Ce document a pour but de décrire les motivations et le fonctionnement du réseau Bitcoin pour enfin faire un tour d'horizon des enjeux qu'il soulève.

1 Motivations

De nos jours, les institutions bancaires sont fortement impliquées dans les transactions monétaires de toutes natures. Elles sont au centre des flux financiers et jouissent d'un certain pouvoir sur la circulation de l'argent. Un simple achat par carte de crédit auprès d'un commerce fait ainsi intervenir une tierce partie, à savoir une banque qui débite le montant sur le compte de l'acheteur et le crédite sur celui du vendeur. Il est a noté que le système monétaire actuel est déjà fortement électronique : Au Canada en 2013, le nombre de pièces et de billets ne représente que 23 % de la valeur de la masse monétaire.

Le recours à une instance tierce pour les transactions monétaires peut soulever plusieurs problèmes :

— Présence de frais de transaction / temps de transaction important.
— Nombre de transactions limité
— Difficultés inhérentes aux frontières géographiques des différents pays.
— Influence de la politique et de l'économie du pays sur la monnaie.
— Problèmes de liberté individuelle avec la présence d'une autorité centrale
— Nécessité de posséder un compte bancaire (difficile dans certains pays en voie de développement)

Ainsi, la création du Bitcoin est motivée par l'envie de pouvoir effectuer des transactions d'une partie à une autre, sans la présence d'une institution financière tierce.

2 La cryptomonnaie

Il nous faut dans un premier temps réussir à formuler le problème. Le fait de se passer d'une autorité financière qui régule les transactions doit être compenser par des solutions technologiques qui permettent de remplir cette tâche. Le modèle adopté est le réseau peer-to-peer. Tout comme une banque tient régulièrement un « livre des comptes » de façon à savoir si telle ou telle personne est en mesure d'effectuer une transaction, chaque ordinateur du réseau peer-to-peer héberge une copie d'un « livre de transactions ». Grossièrement, Bitcoin n'est ni plus ni moins qu'un grand fichier de transactions dont chaque nœud du réseau héberge une copie. Cependant, cela ne suffit pas à en faire un système complet. Il nous faut également :

— Un moyen d'authentifier et de sécuriser les transactions.
— Un moyen de gérer l'ordre chronologique des transactions.

Ces deux aspects étant naturellement solutionnés par l'institution bancaire dans le cadre d'une monnaie classique, nous devons trouver des solutions permettant de gérer ces cas dans le cadre de notre réseau peer-to-peer, tout en assurant la protection et la neutralité de ce réseau. Dans les prochains chapitres, nous décrivons les solutions apportées à ce problème, notamment à l'aide de 3 composantes majeures que sont le porte-monnaie, la chaîne de blocs et le minage.

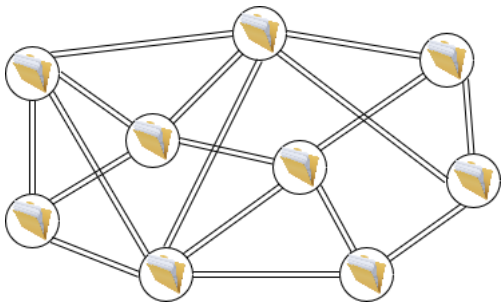

FIGURE 1 – Représentation simplifiée du réseau Bitcoin (les nœuds se partagent une copie du « livre des transactions »)

3 Les transactions

Envoyer de la monnaie à quelqu'un via Bitcoin revient à partager au réseau une transaction. Chaque nœud du réseau reçoit la transaction, l'applique à sa copie du « livre de transactions » que l'on a évoqué plus haut et l'envoie aux autres nœuds pour qu'ils fassent de même. La grande différence par rapport à un système bancaire réside dans la transparence des échanges : tous les utilisateurs du réseau y ont accès. Ainsi, les transactions sont sécurisées par des procédés cryptographiques de façon à respecter l'authenticité et l'intégrité des informations.

C'est ici qu'intervient le porte-monnaie (Wallet) : chaque utilisateur voulant effectuer une transaction dispose d'un porte-monnaie contenant plusieurs couples de clés privés - clés publiques (qui peuvent être générées autant de fois que nécessaire). Les transactions vont ainsi pouvoir être signées numériquement par un procédé de chiffrement asymétrique.

Prenons l'exemple simplifié suivant : Bob veut envoyer 2 bitcoins à Alice. Il utilise un couple clé privée-clé publique issu de son porte-monnaie puis prépare la transaction (considérons ici qu'il s'agit du message « Bob envoie 2BTC à Alice »). Bob chiffre ce message avec sa clé privée et l'envoie au réseau. De cette façon, tous les nœuds du réseau peuvent s'assurer de l'origine de la transaction, simplement en déchiffrant le message avec la clé publique de Bob. (Notons que les adresses de l'émetteur et du destinataire dans les transactions sont en fait les clés publiques de ces derniers).

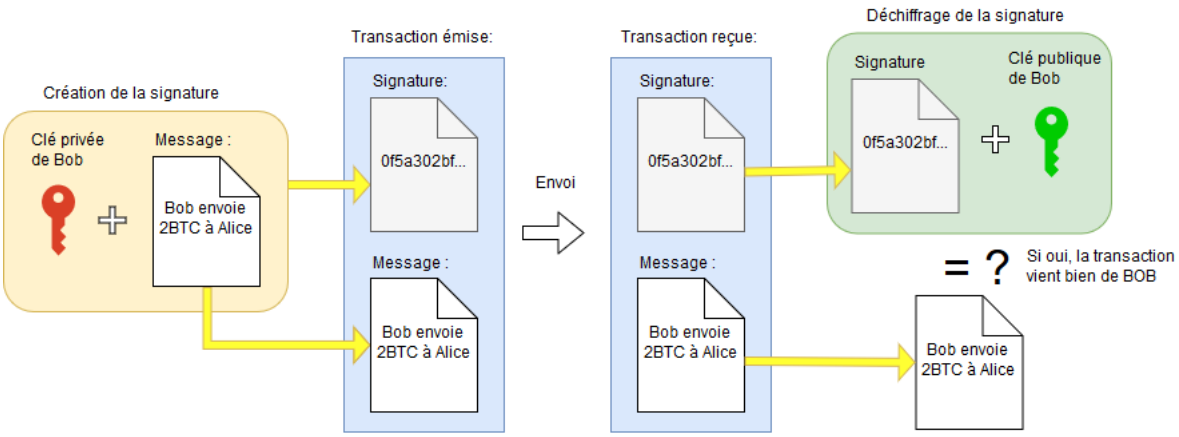

FIGURE 2 – Procédé de signature numérique par chiffrement asymétrique

Nous avons ainsi un moyen d'envoyer des transactions de manière sécurisée. Il reste cependant quelques problèmes à solutionner. Comme mentionné plus tôt, Bitcoin repose sur une sorte de « livre des transactions » partagé entre tous les pairs. Mais en aucun cas, le réseau ne garde une trace brute des soldes des différents comptes. Comment s'assurer alors que Bob dispose de suffisamment de bitcoins pour les envoyer à Alice ?

La réponse est simple : les transactions sont liées entre elles par des entrées/sorties : Pour que Bob puisse envoyer 2 BTC à Alice, il faut qu'il ait reçu au moins 2BTC lors de transactions antérieures. Ces précédentes transactions seront liées à la transaction actuelle par les entrées, tandis que la somme que Bob envoie à Alice constituera la sortie de la transaction courante.

La validité de chaque transaction est ainsi dépendante des précédentes transactions. Lors de la première installation d'un porte-monnaie Bitcoin, ce dernier télécharge l'historique des transactions effectuées sur le réseau en vérifiant ainsi leur validité, et ce jusqu'à la toute première. Chaque transaction qui a été utilisée en entrée d'une autre transaction devient ainsi désuète et ne pourra être réutilisée. Cela fait notamment part des vérifications que les nœuds du réseau effectuent pour s'assurer que la transaction en cours est valide et que l'émetteur dispose bien d'au moins la somme qu'il veut envoyer.

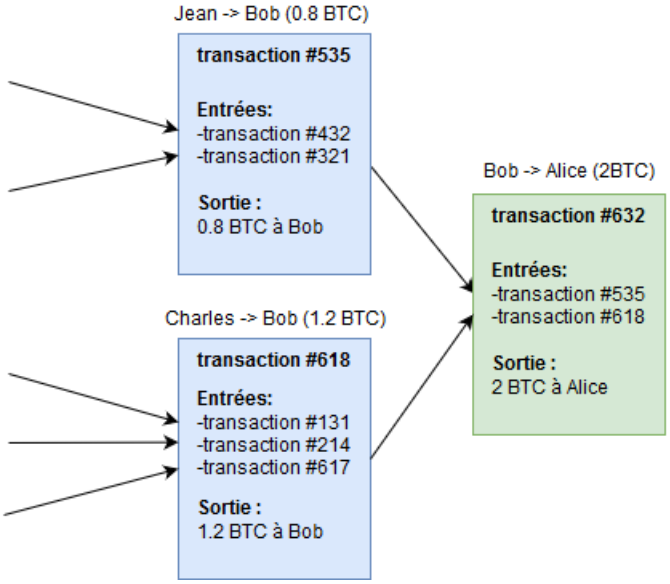

FIGURE 3 – Le système d'entrées/sorties des transactions

4 Ordre des transactions

Nous avons ainsi vu comment sont gérées les transactions dans le réseau Bitcoin : La signature numérique certifie de l'authenticité, de l'intégrité et de la non-répudiation de la transaction par son émetteur. Le réseau nous assure également que ce dernier dispose de suffisamment de bitcoins pour effectuer son paiement, par la validation de la chaîne de transaction. Il ne reste plus qu'à gérer l'ordre de traitement des transactions dans le réseau.

Dans un système classique, l'instance bancaire s'assure de l'ordre d'arrivée des transactions pour les traiter chronologiquement. Dans le réseau Bitcoin, elles sont transmises de nœuds en nœuds, et suivant la position des nœuds dans le réseau, il est possible de se retrouver avec des divergences dans l'ordre d'arrivée desdites transactions, ouvrant par ailleurs la possibilité à des utilisateurs malveillants de frauder. (Nous détaillerons ce point dans les prochaines parties).

Il nous faut donc un moyen pour chaque nœud du réseau de s'accorder sur l'ordre des transactions. Il est indispensable que cet ordre soit le même pour chaque nœud : les transactions courantes étant liées à des transactions antérieures (par le système d'entrées/sorties détaillé plus haut), nous pourrions nous retrouver dans des cas avec des transactions invalidées d'un côté du réseau et validées de l'autre côté, remettant tout le fonctionnement en question.

Nous allons voir que cet ordre est littéralement déterminé par une course entre tous les nœuds du réseau !

5 La chaîne de blocs (blockchain)

Le réseau Bitcoin solutionne le problème d'ordonnancement des transactions en les plaçant dans des blocs. Chaque bloc est relié à un bloc précédent, formant ainsi une chaîne qui grandit au fur et à mesure du temps. C'est ce qu'on appelle la blockchain. Les transactions qui ne sont pas encore placées dans un bloc sont « mises en attente ».

Ainsi chaque nœud du réseau reçoit les transactions en attente, (dans un ordre qui peut différer d'un nœud à l'autre), puis les place dans un bloc, et suggère au reste du réseau ce bloc comme étant le prochain de la chaîne. Mais encore une fois, suivant l'emplacement dans le réseau, deux blocs peuvent être suggérer dans des ordres différents. La solution à cela est d'obliger les nœuds à résoudre un problème de complexité importante pour pouvoir suggérer leur bloc comme successeur de la chaîne.

Chaque nœud va prendre le contenu du bloc sur lequel il travaille et y ajouter ce qu'on appelle un nonce (une chaîne de caractères aléatoire) puis passer l'ensemble à une fonction de hash. Le but est d'obtenir un résultat débutant par un nombre de 0 prédéfini. Par exemple, le résultat pourrait être de la forme :

$$000000000000000b5b497c2091b8ed0fa39847f8b79633981cc732afc78026$$

Si le résultat de la fonction de hash débute par au moins le nombre de 0 requis, le bloc est accepté comme étant le prochain de la chaîne, tous les nœuds s'accordent sur cette décision, et la course continue pour le prochain bloc. On dit alors que le nœud a fourni une « preuve de travail ». Si le résultat de la fonction de hash n'est pas de cette forme (c'est à dire dans la plupart des cas), le nœud change de nonce puis réeffectue l'opération jusqu'à ce qu'il obtienne un résultat de la forme requise ou qu'un autre nœud du réseau le fasse.

Plus le nombre de 0 imposé est grand, plus la complexité augmente. Le nombre de 0 est actualisé régulièrement de manière que l'ensemble de la puissance de calcul des ordinateurs du réseau qui cherchent une solution au problème permet d'ajouter un bloc à la chaîne toutes les 10 minutes. L'aspect aléatoire de la solution à ce problème rend rarissime l'ajout simultané de deux blocs distincts à la chaîne. Rarissime mais pas impossible. Si tel est le cas, la blockchain se divise en deux branches. On dit qu'il y a « bifurcation ». Chaque nœud continue alors la course en construisant à la suite du premier des blocs qu'il a reçu. Dès lors qu'une des branches devient plus grande que les autres, elle devient la branche à retenir. Les blocs des autres branches sont alors abandonnés, les transactions sont replacées en attentes et les nœuds continuent la course sur la branche principale.

Il est a noté qu'il est fortement improbable que deux blocs soit validés en même temps plusieurs fois à la suite.

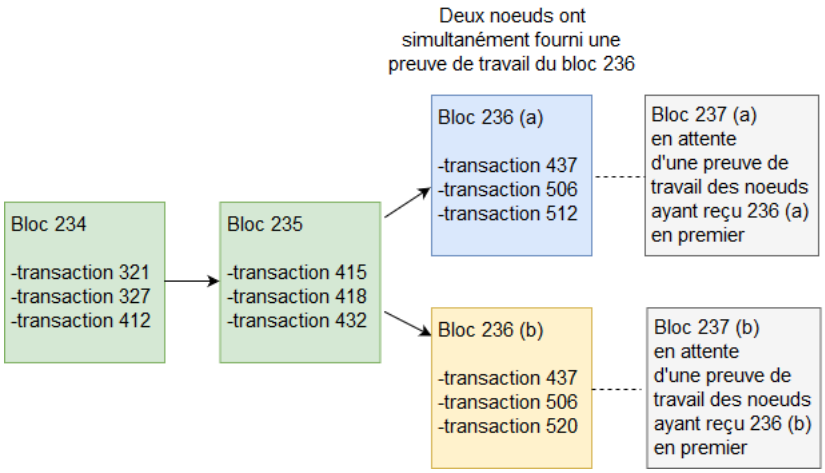

FIGURE 4 – Illustration d'un cas de bifurcation. Si un nœud fourni une preuve de travail pour le bloc 237 (a) en premier, la branche (b) est abandonnée : les transactions de ses blocs, non validées dans la branche (a) (ici, la transaction 520) sont replacées en attente.

6 Problème de la double dépense

Considérons le cas de figure suivant : Bob veut acheter un ordinateur à Alice. Il commence par envoyer une transaction pour le paiement : la transaction est acceptée dans un bloc qui est ajouté à la fin de la blockchain. Alice envoie alors l'ordinateur à Bob par la poste. Aussitôt le colis envoyé, Bob réeffectue le même virement mais en s'indiquant comme destinataire. On peut alors imaginer que Bob ait précalculé plusieurs blocs qu'il rajoute au fur et à mesure à sa chaîne, en y incluant sa transaction vers lui-même. Si la branche de Bob devient plus grande, elle devient la suite de la blockchain. La transaction vers Alice est alors remise en attente mais ne pourra plus être validée dans un bloc ultérieur car les entrées de cette transaction ont déjà été utilisées pour le virement de Bob vers lui-même. Résultat, Bob n'a rien dépensé mais recevra quand même l'ordinateur qu'Alice lui a envoyé.

En réalité, ce problème a également été pris en compte : par construction de la blockchain, il est totalement impossible de précalculer des blocs. En effet, chaque nouveau bloc de la chaine contient :

— Une référence au bloc précédent (en outre, le hash qui lui a permis d'être validé : sa preuve de travail)
— La liste des transactions courantes
— Le nonce

Ainsi, il est impossible de valider un bloc sans détenir l'information de la référence du bloc précédent, de même qu'il est impossible pour un utilisateur d'altérer un bloc en milieu de chaîne, car dans ce cas, la référence de ce bloc serait changée impliquant le changement de tous les blocs suivants. En somme, la référence du bloc précédent fait partie intégrante des informations passées à la fonction de hash du bloc courant pour sa validation.

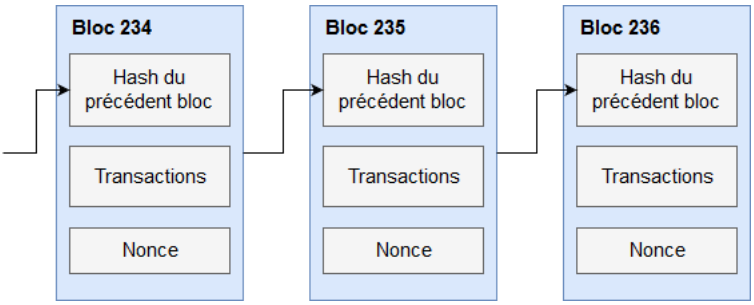

FIGURE 5 – Chaque bloc est lié au bloc précédent par la preuve de travail de ce dernier

La seule façon pour Bob de mettre à profit cette situation serait une course entre lui et le reste du réseau Bitcoin pour la création des nouveaux blocs. Il faudrait dès lors qu'il possède plus de la moitié de la puissance de calcul du réseau pour rivaliser avec les autres nœuds. Cependant, nous allons voir dans la partie suivante que même s'il possédait une telle puissance de calcul, il aurait tout intérêt à travailler à la validation des blocs de manière honnête, plutôt que de compromettre l'intégrité du système.

Pour conclure cette partie, il faut garder à l'esprit que les blocs situés en fin de chaîne sont plus susceptibles d'être abandonnés au profit d'une nouvelle branche, et même sans parler d'utilisateur malveillant, il est possible qu'une transaction se retrouve dans un bloc et soit abandonnée par la suite. Il est donc recommandé d'attendre la création de quelques blocs avant de considérer que la transaction a réellement été validée.

7 Le minage

Jusqu'à maintenant, nous avons beaucoup parlé du fonctionnement de la blockchain mais nous avons omis un détail : qu'est-ce qui pousse les nœuds à travailler pour valider les blocs ? Quel intérêt ont-ils à faire cela ? La résolution d'un bloc entraîne une récompense : une certaine somme de bitcoins est offerte au groupe d'ordinateurs ayant fourni la preuve de travail. C'est ce qu'on appelle le minage. C'est d'ailleurs la seule façon de créer de la monnaie dans le réseau Bitcoin. Il est a noté que tous les 4 ans, la récompense pour la résolution d'un bloc diminue pour que la masse monétaire du réseau converge d'ici quelques années, dans un but d'équilibre de l'offre et de la demande.

Comme nous l'avons mentionné précédemment, il y a une chance infime pour qu'un ordinateur isolé fournisse une preuve de travail, du fait de l'insignifiance de sa puissance de calcul face au reste du réseau. Les ordinateurs

qui veulent miner se regroupent ainsi, formant des « mining pools » et partagent la récompense entre eux, en fonction de la puissance de calcul mis à profit par chacun des individus à la résolution du problème.

Finalement, pour en revenir à la question soulevée dans la partie précédente : En imaginant qu'un groupe de mineurs détienne la majorité de la puissance de calcul du réseau, pouvons-nous être assuré qu'il se comportera de façon honnête, sans essayer de mettre sa puissance de calcul au profit de problèmes comme celui de la double dépense ? Une courte réflexion nous permet de répondre à cela : Est-il préférable d'agir de façon honnête et de résoudre le maximum de blocs de façon à générer le plus de profit possible ou bien d'essayer de compromettre le système de manière beaucoup moins lucrative, rendant le système non sûr aux yeux des utilisateurs et risquant de les pousser à l'abandonner ?

Conclusion

Nous avons ainsi décrit le fonctionnement et les enjeux du Bitcoin. Cette cryptomonnaie permet la réalisation de transactions de pair à pair, sans instance intermédiaire et de façon sécurisée via la mise en place de protocoles robustes. Le Bitcoin a de nombreux avantages : facilité et rapidité des transferts, absence de limite géographique, accessibilité... mais souffre également de beaucoup de faiblesses : reconnaissance juridique, instabilité financière, complexité de fonctionnement, méconnaissance du grand public...

Même s'il ne s'est pas encore imposé comme une révolution aux yeux du grand public, le Bitcoin n'en reste pas moins un innovateur majeur dans le domaine des cryptomonnaies et on peut aisément imaginer que dans un futur proche, ces dernières jouent un rôle important dans l'économie mondiale.

Références

[1] Scott Driscoll. How bitcoin works under the hood, juillet 2013. `www.youtube.com/watch?v=Lx9zgZCMqXE`.

[2] Forex. Les avantages et inconvénients du bitcoin. *La Tribune*, 2014.

[3] Ben Fung, Kim P. Huynh, and Gerald Stuber. L'usage de l'argent comptant au Canada. *Revue de la banque du Canada*, page 54, 2015.

[4] David Louapre. Le Bitcoin et la Blockchain (avec Heu ?Reka) - Science étonnante n31, juin 2016. `www.youtube.com/watch?v=du34gPopY5Y`.

[5] Satoshi Nakamoto. Bitcoin : a peer-to-peer electronic cash system. 2008. `https://bitcoin.org/bitcoin.pdf`.

[6] Mathieu Nebra. Comprendre le bitcoin et la blockchain, décembre 2017. `www.openclassrooms.com/fr/courses/3925766-comprendre-le-bitcoin-et-la-blockchain`.