Tout savoir sur la monnaie Bitcoin

Comprendre et utiliser le Bitcoin

Le minage des Bitcoins

Bien que parfaitement invisible aux yeux des utilisateurs, le minage est essentiel au fonctionnement du réseau Bitcoin, car il permet de sauvegarder et de confirmer chaque transaction.

En l'absence d'une entité régulatrice, le minage permet de s'assurer que personne ne peut dépenser deux fois ses Bitcoins. Comment fonctionne le minage et qu'est-ce vraiment que la chaîne de bloc ?

Une activité nécessaire au fonctionnement du Bitcoin

Le minage, c'est l'utilisation de matériel informatique pour exécuter des algorithmes issus de la cryptographie afin de confirmer les transactions et de garantir la sécurité du réseau. C'est pour cela que l'on dit que le Bitcoin est une cryptomonnaie.

Comme rémunération pour leurs services, les mineurs reçoivent des Bitcoins spécialement créés à cet effet par le réseau. Ils peuvent également percevoir des commissions sur les transactions qu'ils confirment. Le minage est une activité très concurrentielle et coûteuse en matériel et en énergie.

L'objectif des mineurs est de rassembler les transactions qu'ils reçoivent du réseau au sein d'un groupe de transactions, appelé un bloc, qui va être rattaché à la chaîne de bloc. Un bloc contient actuellement environ 300 transactions. Chaque bloc possède un identifiant unique (son nom en quelque sorte) déterminé automatiquement par un algorithme en fonction des transactions qu'il contient.

Afin d'être rémunéré, un mineur doit exécuter un algorithme de cryptographie à de nombreuses reprises, en général plusieurs milliards de fois par seconde pendant plusieurs minutes. Cet algorithme, le SHA-256, est extrêmement gourmand en ressources informatiques. Comme le minage est une activité concurrentielle, les mineurs sont obligés de s'équiper avec du matériel le plus puissant possible s'ils veulent continuer à être compétitifs par rapport aux autres mineurs. De ce fait, la puissance informatique dédiée au réseau Bitcoin augmente en permanence. Elle culmine aujourd'hui à presque 2 millions de GigaHash par seconde (ou GH/s) ce qui signifie que chaque seconde, le réseau Bitcoin exécute l'algorithme SHA-256 environ 2 millions de milliards de fois.

Cette puissance du réseau est un gage de sécurité. En effet, pour prendre de vitesse les autres mineurs et pouvoir inscrire des transactions frauduleuses dans la chaîne de bloc, il faudrait qu'un pirate puisse rassembler plus de la moitié de la puissance totale du réseau. C'est la fameuse règle du 51 %. Il faudrait disposer de 51 % de la puissance totale du réseau pour y inscrire des transactions frauduleuses. Ce qui est aujourd'hui impossible en pratique. L'investissement nécessaire pour disposer de cette puissance serait actuellement de deux milliards de dollars.

Et d'ailleurs, même si cela était possible, il ne serait pas forcément avantageux de pirater le réseau ! En effet, et l'inventeur du Bitcoin le dit lui-même, quelqu'un disposant d'autant de puissance aurait plutôt intérêt à miner légalement, car ce serait bien plus rentable que de dépenser doublement une transaction qui, de toute façon, finirait par être purgée de la chaîne de bloc.

Le minage, une activité risquée, mais potentiellement rémunératrice

La difficulté évolue en fonction de l'état du réseau

Pour des raisons de stabilité du réseau, il a été décidé que le temps moyen de minage d'un bloc devait être de 10 minutes en moyenne. Le réseau s'adapte donc en permanence à la puissance disponible et au nombre de transactions à traiter. En fonction du temps que met le réseau à réellement produire un bloc, le réseau décide d'un chiffre qui correspond à la difficulté du minage. Ce site permet de suivre la progression de la difficulté du réseau Bitcoin : **http://bitcoindifficulty.com/**. Par exemple, s'il manque de puissance pour traiter une croissance du nombre de transactions, la difficulté diminuera légèrement. Si, à l'inverse, la puissance du réseau augmente et que le nombre de transactions stagne, le réseau augmentera automatiquement la difficulté pour conserver un temps de production de bloc d'environ 10 minutes.

La variation de la difficulté de minage est décidée automatiquement par un algorithme connu de tous. Rappelons que le logiciel Bitcoin est open source dont chacun peut consulter le code informatique.

Trouver le bon bloc

Comme son nom l'indique (un peu), le minage s'apparente en fait à une recherche plus qu'à une production à proprement parler. Pour être rémunéré, un mineur doit trouver un bloc. Pour ce faire, il doit exécuter l'algorithme de nombreuses fois jusqu'à ce qu'il tombe sur un résultat qui montre de façon incontestable qu'il a bien trouvé un bloc.

En effet, les systèmes informatiques conçus pour le minage de Bitcoin ne font pour ainsi dire qu'appliquer la fonction cryptographique SHA-256 à une chaîne de caractères. Cette chaîne de caractères correspond à l'identifiant du bloc qu'ils essayent de trouver. Cette fonction cryptographique génère une chaîne de caractères pseudo-aléatoire, que l'on appelle un hash. Voici un exemple de hash :

f813ef9bcc2e731f97577baab11b8d8eb65df081fc392cf400a779f5635

Pour qu'un mineur trouve un bloc, il faut que le hash de ce bloc commence par un certain nombre de zéros. Plus la difficulté est forte, plus le nombre de zéros par lequel le hash doit commencer est grand.

Les ordinateurs des mineurs utilisent donc l'identifiant du bloc, y ajoutent un incrément, puis exécutent de nombreuses fois l'algorithme SHA-256 en augmentant l'incrément à chaque fois. Ils font cela jusqu'à ce qu'ils trouvent un résultat qui commence par le bon nombre de zéros.

Lorsque cela est fait, ils envoient leur découverte aux autres nœuds du réseau. Ceux-ci constatent que le bloc est bien valide et l'ajoute à leur chaîne de bloc. Le mineur est alors rémunéré par le réseau qui émet une certaine somme prévue d'avance.

La récompense est actuellement de 25 BTC par bloc trouvé. Comme il existe un nombre maximum de Bitcoins en circulation, la récompense baisse régulièrement. Elle est divisée par deux tous les 210.000 blocs trouvés.

Pour mieux comprendre, nous allons prendre un exemple :

1. Nous allons appliquer l'algorithme SHA-256 à cette chaîne de caractères au hasard, par exemple : « 12345678910 Bitcoins ».
2. Le résultat est :
   506f841085373238d1f8bc82e234e8b3baddb7b4b6315db3e1750dec6c310d99.
   Ce hash ne commence pas par un zéro.
3. Nous allons rajouter un incrément à la fin de notre chaîne et retenter l'expérience : « 12345678910 Bitcoins-1 », « 12345678910 Bitcoins-2 », etc. pour trouver le premier hash qui commence par un zéro.
4. Nous devons attendre le neuvième incrément : « 12345678910 Bitcoins-9 » qui donne le hash suivant :
   0b82f4fd32f4de56aec4f43d7e46c3b45c6ac45ecd71cb0351716b372e3e9a21.
   Ce hash commence bien par un zéro !

Il nous a suffi de 9 essais pour trouver un hash commençant par un zéro, mais il faut des milliards d'essais aux mineurs avant de trouver un hash commençant par suffisamment de zéros.

Si vous voulez vous amuser avec la fonction SHA-256, essayez ce site : **http://www.xorbin.com/tools/sha256-hash-calculator**.

En soumettant au réseau l'identifiant du bloc, le numéro de l'incrément et le hash commençant par le bon nombre de zéros, le mineur apporte la preuve de son travail et des ressources qu'il a mises en œuvre pour miner le bloc. Le réseau lui octroie sa récompense et le bloc trouve sa place en bout de la chaîne de bloc.

La notion de preuve de travail est centrale dans l'invention du Bitcoin. Sans elle, il ne serait pas possible d'inciter les mineurs à investir dans une grande puissance de calcul et donc impossible de sécuriser la chaîne de bloc et d'empêcher des doubles dépenses, car il suffirait de quelques serveurs aux hackers pour dépasser la puissance du réseau.