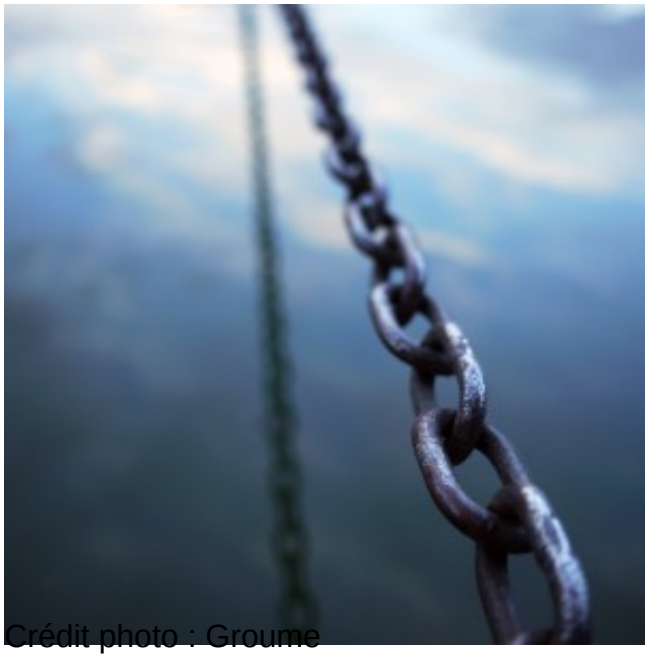
Comment ça marche les bitcoins (3)



Crédit photo : Groume

Dans l'article précédent, je vous expliquais comment on fabrique des bitcoins.

Vous avez théoriquement donc compris que les bitcoins sont organisés en blocs (d'abord de 50 bitcoins, puis 25, puis 12.5, etc. jusqu'à ce que les 21 millions de bitcoins prévus par le protocole soient minés). Un bloc est une bête chaîne de caractère dont la propriété est que, passée deux fois dans l'algorithme SHA256, elle génère une chaîne de 32 octets qui commence par un certain nombre de zéros, le nombre de zéros nécessaires pour trouver un bloc valide est calculé toutes les deux semaines en fonction de la puissance minière disponible pour faire en sorte qu'un nouveau bloc soit créé toutes les 10 minutes.

Mais pour éviter que de petits rigolos créent des blocs avec X fois la même chaîne, le challenge est volontairement plus complexe. Il ne faut en fait pas seulement trouver une chaîne dont le double hash donne un certain nombre de zéros mais une chaîne qui, combinée au hash du précédent bloc trouvé, donne un hash qui contient un certain nombre de zéros.

Par exemple, si on reprend le mot « neutralité » qui, une fois passé deux fois dans SHA256, donne une chaîne binaire commençant par deux zéros, et qu'on admet qu'il s'agit du premier bloc de 50 bitcoins créés, la chaîne qu'il faudra trouver pour le second bloc contiendra obligatoirement le hash de « neutralité ».

La conséquence de cette difficulté supplémentaire est que lorsqu'un nouveau bloc est créé et envoyé sur le réseau par la personne qui l'a miné, l'ensemble des mineurs arrêtent leur travail pour le reprendre à partir du hash de ce nouveau bloc.

Vous voyez donc se dessiner le fonctionnement global de l'engin : le réseau bitcoin est

composé d'ordinateurs qui discutent ensemble en permanence (en peer2peer comme votre bittorrent) et qui passent leur temps à ajouter des caractères après le hash du dernier bloc qu'ils ont reçu pour pouvoir trouver le suivant. Lorsque l'un des ordinateurs trouve le bloc qui correspond au challenge du moment, il l'envoit à ceux à qui il est connecté qui vont, chacun, vérifier s'il est valide (présence du hash du dernier bloc connu et bon nombre de zéros dans le hash final) et, si c'est le cas, vont l'envoyer eux-même aux autres ordinateurs connus, procédant ainsi par inondation dans l'ensemble du réseau.

Tout un chacun connaît ainsi, en quelques secondes, l'ensemble de la chaîne des blocs valides et peut travailler sur le dernier bloc en date.

Il existe une probabilité non négligeable qu'un bloc soit découvert simultanément à deux extrémités du réseau peer2peer (c'est déjà arrivé). On assiste alors à une désynchronisation de la chaîne des bitcoins, certains membres du réseau (plus proche de l'un des mineurs gagnants que de l'autre) faisant confiance à l'un plutôt qu'à l'autre pour recommencer leur travail. Le temps passant, la probabilité que chacune de ces deux chaînes produisent encore un nouveau bloc simultanément finit par tendre vers zéro, le phénomène cesse donc de lui-même dès que l'une ou l'autre des chaines différentes ainsi créée commence à croître plus rapidement que l'autre, l'ensemble des logiciels bitcoins en circulation ayant pour consigne de toujours privilégier la chaîne valide la plus longue.

A cette occasion, des bitcoins sont créés puis détruits dans les heures qui suivent, ce qui peut être un brin déroutant. C'est généralement pour cela qu'on n'utilise pas immédiatement un bloc de bitcoins créé tant qu'on n'est pas certain qu'il a été accepté par un nombre conséquents de membres du réseau en activité au moment de sa création. Le phénomène n'est cependant pas courant.

Les bitcoins sont donc une succession ininterrompue de chaînes de caractères formées du hash de la chaîne précédente et d'un challenge trouvé par un heureux chanceux et chaque membre du réseau dispose de cette chaîne pour pouvoir la vérifier et tenter de miner de nouveaux blocs.

Si vous avez tout bien suivi, vous vous êtes rendu compte qu'une personne malveillante disposant d'une capacité de calcul phénoménale pourrait ruiner l'ensemble assez facilement. Il suffirait de reprendre les calculs à partir du premier bloc de bitcoins créés et de parvenir à créer rapidement une chaîne un peu plus longue que la chaîne existante actuelle. Une simple connexion au réseau bitcoin avec cette nouvelle chaîne plus longue que l'existante ferait disparaître l'existante (et tous les bitcoins associés) instantanément et le nouvel arrivant serait donc seul maître à bord avec l'ensemble de la masse monétaire dans les mains.

Il n'est d'ailleurs pas impossible que des gens travaillent à la réalisation de ce genre d'exploit, mais sa faisabilité s'éloigne à mesure que le bitcoin se popularise, les ressources techniques nécessaires pour créer une chaîne alternative devenant chaque jour plus grandes.

Au prochain épisode, on abordera le fonctionnement des transactions entre participants du réseau bitcoin qui sont effectuées à partir de cette chaîne.