Comment ça marche les bitcoins (2)

Crédit Photo : Steve Jurvetson

Dans l'article précédent, je vous ai fait un rapide descriptif de trois grandes familles de chiffrement. Dans le cas du bitcoin, ce sont principalement la seconde et la troisième qui nous intéressent.

Comme vous ne le savez peut-être pas, la base du bitcoin est un problème mathématique à résoudre. Vous résolvez le problème, vous créez de nouveaux bitcoins et ils sont à vous. Ceci n'est possible que parce que l'ensemble des logiciels gérant les bitcoins sont d'accord sur une règle commune et un challenge commun.

Le challenge en question consiste, pour simplifier, à trouver une chaîne de carractères dont le début du double hashage SHA256 contient un certain nombre de bits à 0. Plus la difficulté augmente, plus le nombre de bits à 0 à trouver augmente.

Explications :

Si vous vous souvenez de l'article précédent, le chiffrement unidirectionnel consiste à transformer une chaîne de caractères en un autre de façon irréversible. Dans le cas de SHA256, la taille de la chaîne finale est de 32 octets (256 bits) quelle que soit la taille de la chaîne d'entrée. Il existe quantité d'outils pour générer des hash SHA256. On en trouve même en ligne, par exemple ici.

Si on donne à cet outil la chaîne »le message » à manger, on trouve 351eceaa68567f1f88b4861b6605f0b1b1ba1501c32ff9a9def5455f8cbfa332. Une seconde fois, et on obtient f430363f9b312525854a2668cb0c255e720cf814dee44d4942ec3a358c69228c. Je vous laisse faire la conversion en binaire, f=1111, 4=0100, 3=0011, 0=0000 etc …

On voit donc ici que le hash en question commence par un 1. Il n'a donc jamais été un bon candidat pour devenir un paquet de bitcoin. A contrario, le mot « neutralité », doublement

hashé, donne 2037c4eb5b3372ca082b20c0b6ae43b582665050299e9c771df1277359ee1f0c qui commence donc par deux zéros, ce qui a dû en faire un bon candidat au tout début de l'histoire du bitcoin. Actuellement, pour « trouver » un bloc de bitcoins, il faut aligner 107 zéros binaires en début de double-hash. Le dernier hash trouvé a été 00000000000001F5D0EAD9D0E7F93E50DF9402A93D4758320983E0A396F782A9.

Le « minage » de bitcoin consiste donc en gros à inventer des chaines de caractères, à les faire passer deux fois dans une moulinette qui calcule le hash SHA256 et à vérifier le nombre de zéro qui s'alignent au début de sa représentation binaire. Au tout début de l'histoire du bitcoin, un seul zéro en début de chaîne suffisait. Il en faut maintenant beaucoup plus. Tout est, au final, une question de chance, une chaîne de caractère correspondante pouvant être trouvée immédiatement, même de tête (même si personne ne mine des bitcoins à la main).

Le nombre de zéros requis pour générer un bloc de bitcoin valide est réévalué automatiquement par tous membre du réseau tous les 2016 blocs générés pour faire en sorte qu'avec la puissance de calcul moyenne disponible pendant les deux dernières semaines, les 2016 prochains blocs soient trouvés dans les deux prochaines semaines, ce qui maintient donc en théorie une création de 6 blocs par heures en moyenne.

Pour vous donner une idée, un processeur core2duo d'intel qu'on trouve dans bon nombre d'ordinateur de bureau est capable d'effectuer cette opération de double hashage entre 3 et 6 millions de fois par seconde. La puissance minière globale actuelle est estimée à 70Thash/s (soit 70 000 000 000 000 hash testés par seconde sur l'ensemble du réseau bitcoin) pour une production constante d'un bloc toutes les 10 minutes.

La corollaire est donc qu'avec votre ordinateur capable de générer 6 millions de hash par secondes, vous avez une chance non négligeable de tomber sur une bonne chaîne tous les… 200 ans.

La taille originale d'un bloc de bitcoin était de 50 unités. Elle est divisée par deux tous les 210000 blocs générés, elle est donc actuellement de 25BTC par bloc. Nous en sommes, à l'heure qu'il est, à 231803 blocs générés pour un peu plus de 11 millions de bitcoins.

En conclusion, avec le temps qui passe, la taille d'un bloc de bitcoin diminue et avec l'augmentation du nombre de mineurs en activité, la probabilité d'obtenir un bloc diminue également.

Le nombre de bitcoins possibles est intrinsèquement limité à 21 millions par le protocole. La difficulté étant peu ou prou maîtrisée dans le temps, on est en mesure de prévoir que 98% des bitcoins auront été minés entre 2025 et 2030.

Vous pouvez à présent reposer vos pelles et vos pioches. Dans le prochain article, on parlera du réseau peer2peer, de la chaîne de bitcoins, et peut être des transactions et de leur validation si vous êtes sages.