Comment ça marche les bitcoins (4)

Crédit photo : 401(K)

Avec le dernier article, vous avez théoriquement une bonne vue de ce qu'est la chaîne des bitcoins. Je récapitule, elle est composée de blocs dont le double hachage SHA256 donne une chaîne de 32 octets qui commence par un certain nombre de zéros qui représentaient la difficulté du moment lors de la création du bloc. Cette chaîne sert à constituer le bloc suivant, permettant de s'assurer que la chaîne est valide de bout en bout.

L'unicité de la chaîne est garantie par le fait que les clients du réseau bitcoin ont pour consigne de toujours choisir la chaîne la plus longue possible si ils ont plusieurs alternatives, situation qui n'arrive heureusement que peu fréquemment.

Maintenant, comment se passent les transactions ? Pour comprendre, vous devez remonter au premier article qui décrit le fonctionnement du chiffrement asymétrique. Chaque participant au réseau bitcoin dispose d'un couple clé privée / clé publique qui a été automatiquement généré par son ordinateur lors du premier lancement du logiciel bitcoin. La clé publique représente son identité sur le réseau bitcoin et la privée est jalousement conservée localement par l'ordinateur.

L'unité la plus petite en bitcoin (le Satoshi) se trouve à huit décimales après la virgule. On peut donc virtuellement (concrètement c'est encore assez difficile) faire une transaction de 0.000000001 bitcoin. Vous allez me dire, « comment est-ce possible alors que les bitcoins ne soient définis aujourd'hui que par des blocs de 50 ou 25 unités ? »

Partons d'un bloc vierge de 50 bitcoins, encore sous la houlette du mineur qui l'a découvert. Admettons que ce mineur souhaite transférer ces 50 bitcoins en totalité. Une transaction va être créée qui va, pour simplifier, prendre le bloc comme référence (input) et indiquer l'adresse publique du destinataire comme sortie (output).

Le bloc originellement miné contient déjà la signature de son mineur associé sous forme d'une transaction à lui même. C'est un petit détail volontairement omis dans les articles précédents, mais il permet, puisque cette signature est incluse dans le hash servant à créer le bloc suivant, de toujours connaître le mineur originel d'un bloc.

Mathématiquement la transaction consiste, pour simplifier, à ce que le propriétaire du bloc signe le hash du bloc en question assorti de la clé publique du destinataire. Le résultat sera donc une chaîne de caractère contenant à la fois l'identifiant du bloc, l'identifiant du bénéficiaire et la signature de l'émetteur.

Comme pour le minage, l'ensemble du réseau bitcoin va valider cette transaction en vérifiant que l'émetteur est bien le propriétaire du bloc en question. Une fois un certain nombre de validations reçues l'argent sera considéré comme ayant été transféré au destinataire. La transaction suivante ne se basera non plus sur le bloc d'origine mais sur la transaction précédente, créant ainsi une chaîne valide et vérifiable de l'ensemble des transactions permettant de remonter à l'émetteur du bloc puis de vérifier sa validité dans l'ensemble de la chaîne.

C'est bien joli, mais vu comme ça, ça ne permet de transférer les bitcoins que par paquets de 50 ou de 25 en fonction du bloc qu'on a sous la main. Pas super pratique.

Du coup, il est possible de faire une transaction d'un bloc complet en affectant plusieurs destinataires et différents montants. Admettons que j'ai mon bloc de 50 bitcoins et que je veuille en envoyer 25 à Tatie Martine. Le logiciel bitcoin va créer une transaction avec mon bloc originel en entrée et deux sorties, l'une de 25 bitcoins à destination de Tatie Martine, et l'autre de 25 à… moi-même.

On se retrouve ainsi, pour les transactions suivantes, avec une référence à cette précédente transaction qui a coupé le bloc en deux. Cette transaction suivante (par exemple Tatie Martine qui envoie 10 bitcoins à son fils) fera référence à la transaction de 25 bitcoins entre moi et Tatie Martine.

La conclusion est un peu déroutante, puisque dans la vraie vie on a l'habitude de pouvoir distinguer les 50 pièces de 1 euro qu'on a dans la main, mais le constat est sans appel, dans un bloc de 50 bitcoins, rien ne différencie les 5 milliards de Satoshi qui le compose. Et c'est heureux, sinon, il faudrait à minima 5 milliards de bits, quelque chose comme 600Mo d'espace disque, au bas mot, pour stocker un bloc de bitcoin.

La différenciation se fait au niveau des transactions, chacune d'elle étant en mesure de découper la précédente en plusieurs morceaux.

Je vois d'emblée venir les questions qui taraudent l'esprit de ceux qui ont eu le courage de me suivre jusqu'ici :

- ou et comment sont stockées les transactions
- à chaque transaction effectuée, la chaîne des bitcoins voit sa taille augmenter, et plus

ça va, plus il y en a.

Ce sera l’objet du prochain article dans lequel j’essaierai, tant bien que mal, de vulgariser la théorie des arbres de Merkle, qui permet de solutionner une bonne partie du problème, et de vous expliquer comment les transactions entrent dans la fabrication des nouveaux blocs.