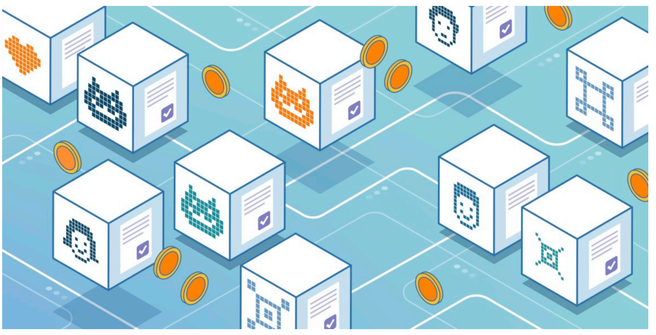
La blockchain et l'idée du bitcoin

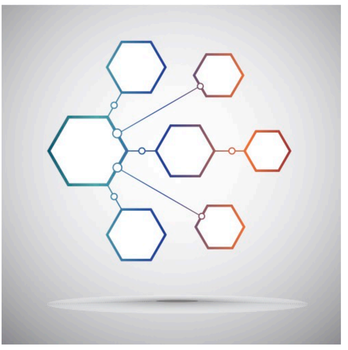


La "blockchain" n'est rien d'autre qu'une série public de transactions qu'ils faut "miner", soit contrôler et vérifier.

Leonardo Gomez Mariaca

Publié le 2022-05-17

Si dans le dernier article, nous avons abordé le grand principe de la décentralisation sur lequel repose le fonctionnement de toutes les cryptomonnaies, nous allons ici approfondir le sujet autour du concept de la blockchain, et pour cela, il va falloir parler du bitcoin. Comme nous l'avons vu précédemment, la sécurité sur laquelle repose tout le principe de la décentralisation est de rendre l'information de la transaction publique, afin que chacun et chacune puisse quotidiennement vérifier que la monnaie qu'il ou elle reçoit est effectivement réelle. Dans l'exemple que nous avions utilisé dans le dernier article, nous avions parlé d'un grand tableau blanc sur lequel il faudrait inscrire la transaction à la vue de toutes et tous. Si l'on reporte ce tableau au monde numérique, on découvre la blockchain. Chaque bitcoin est ainsi tracé, suivi de propriétaire en propriétaire, et c'est cette information qui est maintenue publique afin d'éviter la fausse monnaie. Bien entendu, les propriétaires sont anonymisé derrière des numéros de comptes, mais ces derniers et ces dernières sont toujours identifiables. Pour faire un parallèle afin de bien comprendre la révolution du système financier que cela implique, imaginons que les banques publiaient toutes leurs transactions sur internet. Ce serait, à l'heure actuelle, une violation impossible du secret bancaire.



La "blockchain" est comme une montagne de données qu'il faut miner pour en extraire de l'or, ici l'or étant le bitcoin et la montagne des transactions.

Mais concrètement, qui a la charge de la vérification des transactions ? Dans nos précédents exemples, nous avons simplifiés en affirmant qu'il s'agissait des propriétaires de la monnaie, mais c'est un travail à plein temps. En réalité, un acteur tiers s'y dédie, et sa méthode de travail est la suivante : il va valider les transactions par groupe, par bloc, et non pas transaction par transaction, ce qui prendrait beaucoup. trop de temps. C'est de là que provient le nom de « blockchain », puisqu'il valide à la chaine des blocs de transaction. Cet acteur tiers, c'est un « mineur », nom qui a été choisi pour rester dans la métaphore de la roche. Ce ne sont pas des personnes physiques, mais des ordinateurs extrêmement puissant, dédiés à faire tourner des programmes conçus pour le contrôle des transactions bitcoins. Tous les mineurs sont soumis à la concurrence, et le premier mineur qui termine de contrôler un bloc de transaction est récompensé, et c'est là le génie de l'opération, en bitcoin ! Ainsi, ceux qui sont chargés de surveiller le bon fonctionnement du système le font dans un intérêt de gain financier, ce qui vient boucler la boucle : le réseau bitcoin est ainsi autonome.

À ce système il faut ajouter un autre concept, celui du « halving », que l'on traduit par « réduire de moitié ». Le principe est le suivant : les mineurs sont récompensés en bitcoins après avoir validé un « bloc » de transactions bitcoin, mais cette récompense, ce salaire, est divisé par deux tous les quatre ans. Avant d'expliquer le pourquoi de ce principe, quelques précisions sont nécessaires : la première transaction bitcoin jamais enregistrée a eu lieu le 3 janvier 2009. À l'époque, la récompense promise aux mineurs pour la validation d'un « bloc » de transaction était de 50 bitcoins. En 2012, cette dernière est passée à 25 bitcoins, à 12.5 en 2016 et à 6.25 en 2020. En 2024, elle passera à 3.125 : ces chiffres ne sont pas déterminés par une durée de temps, mais bien par le nombre de blocs : cette réduction de moitié a lieu tous les 210 000 blocs validés, et sachant qu'en moyenne, un bloc est validé toutes les 10 minutes, on obtient une durée moyenne entre deux « halving » de quatre ans environ. Cela veut dire qu'il existe un nombre maximum de bitcoin que le système peut supporter, dépasser ce chiffre reviendrait à ne pas récompenser les mineurs. Ce chiffre, c'est 21 millions. Ce chiffre est prévu et inscrit dans l'algorithme même du bitcoin. Cela signifie qu'aujourd'hui, il existe un peu près à 19 millions de bitcoins en circulation, et qu'il ne peut en exister qu'au maximum 21 millions.

Les mineurs contrôlent les transactions et sont récompensés en bitcoins, c'est donc un système hermétique.

On peut alors légitimement se poser la question du pourquoi les mineurs continuent le travail de contrôle des transactions bitcoins tout en sachant que leur récompense est réduite de moitié au fil du temps. L'intérêt premier vient de l'augmentation de la valeur du Bitcoin, qui, nous le savons, augmente de manière chaotique, mais augmente bel et bien. On peut aussi se poser la question de l'effondrement du système une fois arrivé au 21 millions de bitcoins, mais en vérité, cette limite algorithmique ne restreint nullement le développement du bitcoin et de ses usages. Même si le bitcoin devenait la première monnaie au monde, il existerait toujours assez de bitcoins pour toutes les transactions, on fragmenterait simplement le bitcoin en plus petits morceaux. On paierait avec des millionièmes de bitcoin par exemple. Se plaindre de la limite du bitcoin reviendrait à s'inquiéter de la quantité d'or physique dans le monde : il y en aura toujours assez pour effectuer toutes les transactions, l'or n'a d'importance qu'en terme de valeur, et si l'or devait tout d'un coup jouer un rôle financier encore plus important, son cours augmenterait simplement. C'est la même chose pour le bitcoin. Le fait qu'il existe un bitcoin supplémentaire toutes les 10 minutes, c'est très littéralement de la création physique de monnaie, ce qui sous- entend de l'inflation. À ses débuts en 2009, le taux d'inflation annuel du bitcoin était bien supérieur à 100%, avant de rapidement diminuer entre 2012 et 2016 avant de passer sous la barre des 10%. Le prochain article sera dédié à la relation entre le « halving » et l'inflation, et nous aborderons également les processus de sécurité globale du système.