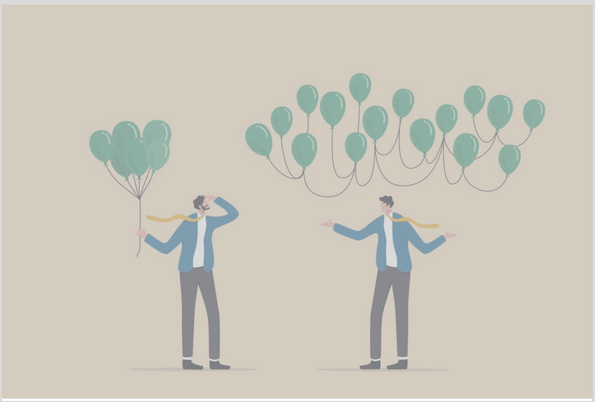


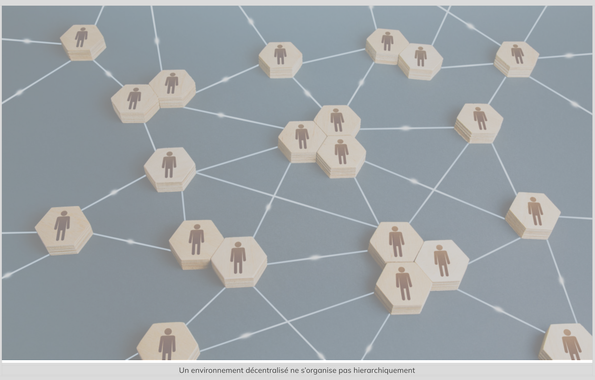
Le grand principe de la décentralisation

Leonardo Gomez Mariaca

Publié le 2022-05-15

Le premier principe à comprendre afin de saisir les enjeux que posent les NFT ainsi que les cryptomonnaies, c'est bien la décentralisation. C'est cette idée qui sépare la notion d'argent électronique, utilisé depuis longtemps par tout un chacun, et une cryptomonnaie. Aujourd'hui, le système financier tourne essentiellement autour des banques : lorsque l'on achète un produit dans un magasin, le prix du produit est débité de notre compte, et cet argent est reçu par le vendeur sur le sien. Les banques assument alors un rôle d'autorité, puisqu'elles valident le paiement, contrôlent la bonne marche de la transaction et conservent une trace de cette dernière. Le système est donc centralisé autour des banques, car l'on peut clairement observer une forme de hiérarchisation : les banques qui s'occupent de la gestion, et en dessous, les clients et clientes.

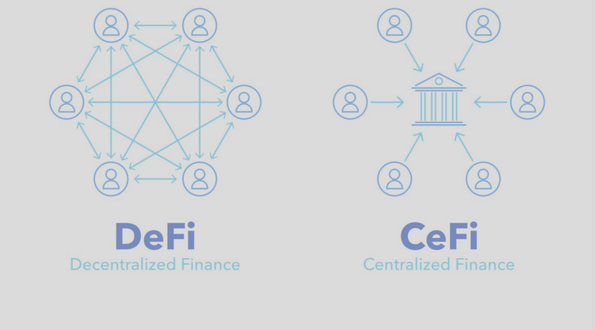
Il a existé de véritables tentatives de créer une monnaie électronique centralisée, la plus célèbre étant l'expérience ratée de e-gold, devise électronique élaborée en 1996 aux USA. E-gold était indexée sur l'or, ce qui signifie que la monnaie était entièrement couverte par de l'or physique. En somme, même si physiquement les lingots d'or restaient à la même place, bien gardés dans le coffre d'une banque, à chaque transaction utilisant e-gold, les lingots changeaient simplement de propriétaire. En 2003, e-gold se plaçait juste derrière Paypal dans les solutions de transferts d'argent sur le web, avec 3,5 millions d'utilisateurs et d'utilisatrices. Toutefois, l'expérience a été de courte durée, puisqu'en avril 2007, la société a été accusé, entre autres crimes, de blanchiment d'argent. Les lingots d'or ont donc été saisis et l'e-gold s'est effondré dans le même temps.



Un environnement décentralisé ne s'organise pas hierarchiquement

Cette petite histoire a pour but de démontrer la difficulté de créer une monnaie virtuelle centralisée autour d'un unique organisateur. Premier problème : quelle confiance lui accorder ? Comment être certain que des dirigeants et dirigeantes de la société ne partent simplement pas avec la caisse, ou qu'il ne fabrique pas discrètement des unités monétaires supplémentaires pour eux ou elles-mêmes ? Deuxième problème : quelle confiance accorder au pays où est installé la société sensée gérer ladite monnaie ? Un gouvernement peut décider à tout moment, sur un prétexte légitime ou illégitime, d'interrompre tout le système, ruinant ainsi tous les utilisateurs et utilisatrices.

C'est ici qu'il faut parler d'Internet. Internet a ouvert une voie différente : la possibilité de s'organiser comme un réseau, et non comme une hiérarchie. Bien entendu, il est possible pour un réseau sur le net de s'organiser autour d'un système hiérarchique, en admettant l'idée d'un nœud central par lequel tout doit passer avant de repartir ailleurs. C'est cette organisation qu'utilise les banques pour leurs cartes bancaires notamment. Mais avec Internet, le système peut également admettre une totale décentralisation, les informations ne devant pas obligatoirement passer par un nœud central, un serveur central, mais bien de serveur en serveur, concept appelé « de pair en pair », soit « peer to peer », abrégé P2P. On s'est alors rapidement demandé s'il était possible de créer une monnaie sur ce modèle décentralisé, et donc sans qu'il ne soit obligatoire de passer par un tiers de confiance pour valider et enregistrer les transactions, comme une banque.



La finance s'organise autour d'un acteur central: la banque. Ce n'est pas le cas dans un système décentralisé.

Dans le monde physique, ce serait possible et même plutôt facile : il suffirait qu'un groupe de personnes imprime des billets uniques et impossible à falsifier, qu'ils et elles détruisent ensuite les machines et les presses ayant servi à la création des dits-billets afin d'éviter que qui que ce soit ne puisse un jour en réimprimer de nouveaux, et enfin, qu'ils et elles se distribuent les billets. À partir de là, il n'y a rien à faire, du moment que l'un ou l'une utilise le billet, il ou elle n'en est plus le ou la propriétaire, il n'y a pas besoin d'une banque pour contrôle cela. C'est d'ailleurs comme cela que fonctionne aujourd'hui nos billets de banque, avec la seule différence que les banques n'ont pas détruits les presses : elles sont toujours libres de réimprimer des billets.

Toutefois sur Internet, les notions d'« unique » et d' « infalsifiable » n'ont pas de sens : la duplication fait partie de la substance même du numérique. Un exemple très simple : si l'on envoie une photo à quelqu'un par mail, on la possède toujours sur son ordinateur. On a envoyé une copie de la photo, et pas la photo en tant qu'entité virtuelle. Alors comment faire circuler sur le net une monnaie numérique qui serait infalsifiable ? Afin de bien comprendre le principe de base sur lequel repose le fonctionnement de la décentralisation des cryptomonnaies, faisons une expérience de pensée : prenons une centaine de personnes dans une salle, et admettons que l'on décide d'utiliser comme monnaie de simples feuilles de papier blanches, que n'importe qui peut trouver dans le commerce.

Personne ne prendrait cette « monnaie » au sérieux, simplement parce que cette dernière est trop facilement duplicable. Mais si maintenant, chacun ou chacune appose sa signature sur les feuilles de papier qu'il ou elle possède, et qu'à chaque fois qu'il ou elle utilise une feuille, qu'il ou elle échange donc sa « monnaie », le nouveau ou la nouvelle propriétaire inscrit à son tour sa signature, il devient très difficile de produire une copie de cette feuille. En effet, si je reçois donc une feuille sans aucune signature, je sais que cette dernière est forcément fausse. Pour que ce principe fonctionne, il faut admettre que les signatures sont infalsifiables, ce qui est le cas avec les cryptomonnaies, mais nous aborderons ce point précis dans un futur article.

Toutefois, la simple signature ne suffit pas, puisqu'un petit groupe de personnes pourrait acheter des feuilles blanches dans le commerce, apposer leurs signatures, se les échanger entre eux pour augmenter le nombre de signatures et donc la crédibilité d'authenticité de la feuille, de la « monnaie », puis remettre cette dernière dans le système pour la faire circuler. Afin d'éviter cela, un deuxième élément est essentiel : il faut que l'information de la circulation des feuilles, de la « monnaie » soit publique. Dans notre exemple, chaque transaction serait affichée dans un grand tableau blanc au centre de la salle. Quand je reçois une feuille, j'y inscrit donc ma signature, mais j'indique aussi sur le tableau que j'ai reçu cette fameuse feuille. Je peux ainsi à tout moment constater la liste des signatures, et la comparer aux signatures présentes sur ma feuille, puisque si l'on me propose une feuille avec des signatures que je ne peux retrouver sur le tableau, je sais de façon certaine qu'il s'agit là de fausse « monnaie ».

C'est ainsi, dans les grandes lignes, que fonctionne les cryptomonnaies, sans avoir recours à un contrôle centralisé : ce sont les participants et participantes qui font office de garde-fou, puisque ce sont eux et elles qui contrôlent régulièrement la bonne tenue de l'ensemble du système. Les « signatures » sont des numéros de compte, et le « tableau » est la base de données de l'ensemble des transactions, accessibles et partagée par l'ensemble des utilisateurs et utilisatrices. C'est ce que l'on appelle la « blockchain », et ce sera le sujet du prochain article de ce blog.