1

Monnaie et cryptographie

Qu'est ce que la monnaie ?

La monnaie est un instrument créé par l'homme ayant trois fonctions :
- une réserve de valeur : quand je possède une pièce ou un billet, je possède de la valeur, je peux la vendre ou l'échanger ;
- une unité de compte permettant le calcul économique ou la comptabilité : cet objet vaut deux euros, ce service mille yens ;
- un intermédiaire : la monnaie permet d'échanger des biens et services et de payer des dettes et obligations (elle a un « pouvoir libératoire »).

La monnaie fiduciaire (euro, dollar, etc.) est une institution constitutionnelle rattachée à un territoire marchand appelé « marché national ». La monnaie est l'instrument de paiement en vigueur dans ce territoire à une époque donnée, du fait de la loi et des usages.

Qu'est ce qui donne de la valeur à la monnaie ?

La monnaie en tant que telle n'a pas de valeur : elle se matérialise (de moins en moins) par des pièces en métal et des bouts de papier et (de plus en plus) par des 0 et des 1. Ce qui donne de la valeur à une monnaie et qui en est une caractéristique indissociable, c'est la confiance. Je reconnais

qu'une monnaie a de la valeur car j'ai confiance dans cette monnaie, autrement dit, je sais que je vais pouvoir l'échanger facilement contre un service, un bien ou une autre monnaie car elle va être acceptée par le pourvoyeur de ce service, de ce bien ou de cette autre monnaie. Autrefois adossée à des matières précieuses, la monnaie tire sa valeur de la confiance que nous avons en l'autorité publique qui l'émet et y appose son nom, sa signature et son sigle. Depuis la fin du système de Bretton Woods, il ne reste que les États pour donner confiance et conférer de la valeur aux monnaies.

Les évolutions récentes de la monnaie

La monnaie a connu trois évolutions majeures au XX^{e} siècle : elle a cessé d'être indexée sur des matières précieuses, sa masse a explosé et elle a connu une importante vague de dématérialisation. Les espèces, même si elles sont encore très présentes dans notre quotidien, ne représentent plus qu'une toute petite partie de la masse monétaire et sont en voie de disparition dans plusieurs pays (en Suède, pays précurseur dans le domaine monétaire).

L'arrivée d'Internet, puis des smartphones a accéléré ce mouvement de dématérialisation et ouvert la voie à de nouveaux modes de paiement : Paypal, Apple Pay, virements en ligne et autres solutions de paiement dématérialisé ou avec portable. Le système actuel des monnaies fiduciaires, avec le rattachement de chaque devise à un territoire donné, est de moins en moins adapté à un monde globalisé et constamment en ligne. La fluidité des échanges est un facteur clé du développement de l'humanité, et la monnaie est un des outils fondamentaux qui rend celui-ci possible (avec les communications et les transports).

La crise latente du système des monnaies fiduciaires

Ce qui donne de la confiance et donc de la valeur dans les monnaies, à savoir les États et, derrière eux, le système des banques centrales et commerciales, a été mis à mal en 2008 avec la crise des subprimes et les quasi-faillites d'États comme la Grèce, le Venezuela ou Chypre. Les banques centrales injectent tellement d'argent dans le système et les États sont tellement endettés que le système monétaire ressemble de plus en plus à une fuite en avant, ce qui érode lentement mais sûrement la confiance et donc la valeur des monnaies fiduciaires, également appelées fiat. On peut se demander à qui profite cette injection d'argent dans le système, car la masse de la population ne semble pas en profiter, pas plus que les États ne semblent économiser.

Sans système alternatif, nous ne pouvions nous en remettre qu'au système des monnaies fiduciaires établi par les gouvernements et les banques.

Qu'est-ce que la cryptographie ?

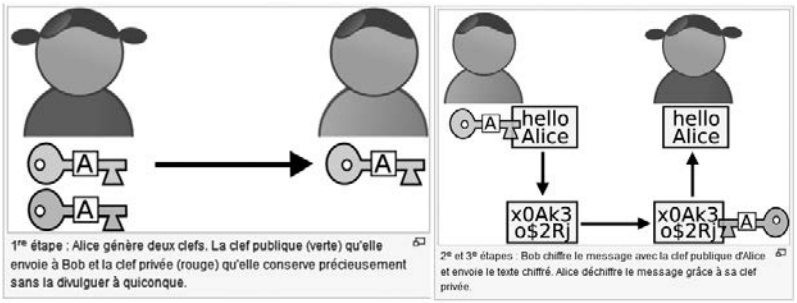
La cryptographie

La cryptographie est une technique basée sur des caractères (chiffres, lettres…) permettant de protéger des messages en les rendant inintelligibles (en les chiffrant). Le mot « cryptographie » vient des mots en grec ancien « kruptos » (caché) et « graphein » (écrire). En cryptographie classique, dite symétrique, le chiffrement est la transformation, par le biais d'une clé, d'un message compréhensible (un « texte clair ») en message incompréhensible (un « texte chiffré ») pour celui qui ne possède pas la clé de déchiffrement. Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre.

La cryptographie asymétrique

C'est pour répondre à cette problématique que la cryptographie asymétrique a vu le jour à la fin du XX^e siècle. En cryptographie asymétrique, chacun a sa clé, ce qui évite de devoir envoyer de manière confidentielle la clé de déchiffrement à son correspondant. Cette cryptographie asymétrique est utilisée par toutes les cryptomonnaies. Aller dans un sens est facile et dans l'autre quasiment impossible.

Ces fonctions à sens unique sont des fonctions mathématiques. La cryptographie asymétrique est basée sur la distinction données publiques/privées et sur deux clés : la clé publique, qui permet de chiffrer (rendre le message inintelligible) et qui peut être mise à disposition de tous, et la clé privée, qui permet de déchiffrer et qui doit rester absolument secrète. C'est exactement ce système de public key/private key qui est utilisé dans les cryptomonnaies. Ce système a deux avantages majeurs. La confidentialité du message est assurée par l'utilisation de la clé publique pour chiffrer et de la clé privée pour déchiffrer celui-ci. Autre avantage : celui de l'authenticité de l'expéditeur, qui utilise la clé publique du destinataire pour coder un message que seul le destinataire pourra décoder, car lui seul possède la clé privée correspondant à sa clé publique. La cryptographie asymétrique est déjà utilisée depuis longtemps par les banques et Internet pour coder des données et des messages, par exemple des mots de passe.



Source : Wikipedia