Vous entendez peut-être parler, surtout sur ce blog, du Bitcoin. Mais qu'est-ce donc ? Et bien, il s'agit d'une monnaie. Rien de moins, rien de plus.

Mais au fond, qu'est-ce qui caractérise une monnaie ? C'est un instrument dans lequel vous placez une certaine confiance. La confiance de pouvoir, plus tard, l'échanger contre des biens ou des services dont vous avez besoin. Ce qui vous pousse, vous-même, à l'accepter en échange d'un service ou d'un bien. Dans la plupart des cas, la monnaie n'est qu'un instrument et n'a pas de valeur intrinsèque ou alors une valeur intrinsèque plus faible que la valeur faciale. Depuis plusieurs années, la monnaie est même devenue principalement virtuelle : il s'agit d'un chiffre qui s'affiche sur un écran. Avez-vous déjà songé que vous travaillez uniquement pour augmenter un chiffre sur un « compte » ?

Afin de maintenir la confiance, il faut que la monnaie soit suffisamment rare et difficile à produire. C'est une des raisons qui ont fait que, très tôt, les hommes ont adopté l'or, l'argent ou les coquillages comme monnaie : rare, difficile à trouver ou à contrefaire et facile à transférer ou à diviser en plus petites parties.

Mais les billets de banques ou les chiffres sur un ordinateur peuvent être reproduits très facilement. Une rareté artificielle est donc maintenue par les états et les banques. L'importance de la monnaie fait que ceux qui la contrôlent, les états et les banques, ont un pouvoir énorme.

Bitcoin est également une monnaie virtuelle. Il s'agit simplement d'un chiffre sur un ordinateur. Mais grâce à un algorithme mathématique complexe, il est possible de le rendre  inmultipliable sans recourir à une autorité centrale. Toute personne qui envoie un bitcoin le perd donc, comme pour n'importe quelle monnaie. Cela fonctionne tellement bien que des internautes ont commencé à avoir confiance dans le fait qu'il pouvait acheter des biens, des services, des euros ou des dollars avec des bitcoins. Le Bitcoin a donc acquis une valeur proportionnelle à cette confiance.

**Comment fonctionne Bitcoin ?**

Pour simplifier très grandement, chaque bitcoin est en fait la solution à un problème mathématique ultra-complexe. De par sa conception, nous savons qu'il existe un total de 21 millions de solutions différentes à ce problème mathématique. Mais les solutions les plus simples étant trouvées les premières, il devient de plus en plus difficile de trouver de nouvelles solutions. À ce jour, 11 millions de bitcoins sont en circulation, de nouveaux bitcoins apparaissent chaque jour chez les « mineurs », personnes équipées de matériel pour la recherche de solutions. Nous savons qu'il n'y aura jamais plus de 21 millions de bitcoins en circulation et chaque nouveau bitcoin est plus difficile à trouver que le précédent.

Un bitcoin est donc unique et rare. Mais il est divisible presqu'à l'infini, ce qui permet de ne pas limiter les échanges.

Le problème qui se pose ensuite est la double dépense. Comment s'assurer que lorsque je donne un bitcoin à quelqu'un, je n'en garde pas une copie. La solution est conceptuellement simple : le logiciel qui permet d'envoyer et de recevoir des bitcoins télécharge, en peer-to-peer, l'historique de tous les propriétaires successifs. Si je donne un bitcoin à Alice mais que j'essaie de le garder pour le dépenser une seconde fois chez Bob, Bob verra immédiatement, dans l'historique du bitcoin en question, qu'il a déjà été donné à Alice. Bob le refusera donc.

Il s'agit évidemment d'une simplification outrancière (et fausse par certains aspects) mais qui vous donne une idée de ce qu'est le bitcoin.

**Comment obtenir des bitcoins ?**

La première chose à faire c'est d'avoir un portefeuille pour recevoir des bitcoins. Vous pouvez soit vous créer un compte sur un service de portefeuille Bitcoin soit installer un client bitcoin sur votre ordinateur. Votre portefeuille peut générer des adresses de réception qui ressemble à **18Trqk3tKkF8vNoW6am5rx8K6wUSQAqo1q.**

Muni de cette adresse, vous pouvez échanger vos euros ou vos dollars contre des bitcoins. Cet échange peut se faire en direct avec une connaissance ou un ami. Ou bien, vous pouvez vous rendre sur un site d'échange de bitcoins. Le plus connu est sans conteste MtGox, par lequel transite la toute grande majorité des échanges bitcoins/dollars. Mais l'utiliser implique pas mal de contraintes de sécurité. Un échange plus simple d'accès est Bitstamp. Une fois votre compte créé là-bas, vous pouvez faire un versement en euros, qui sera converti en dollars. Avec ces dollars, vous pourrez acheter des bitcoins et vous les envoyer sur votre adresse.

Une autre manière bien plus intéressante est de fournir vos services ou vos biens contre paiement en bitcoins. Il vous suffit de générer une adresse par transaction et de la donner à votre client. Le client ne peut pas ajouter de commentaire avec son paiement, ce qui rend Bitcoin un peu complexe et contre-intuitif lors des transactions.

**Comment payer en bitcoins ?**

Dépenser les bitcoins est très simple. Si vous faites un achat sur un site acceptant les paiements en bitcoins, vous verrez tout simplement l'adresse de réception du vendeur. Dans votre client bitcoin (en ligne ou sur votre ordinateur), introduisez cette adresse et le montant. Voilà, c'est aussi simple que ça. À titre d'exercice, copiez/coller **18Trqk3tKkF8vNoW6am5rx8K6wUSQAqo1q** et envoyez moi ce que vous voulez, par exemple 0,01 bitcoin. Voilà, vous venez de faire un paiement. Ce paiement est anonyme : je n'ai aucun moyen de savoir qui me l'a envoyé. Notons que cet anonymat n'est pas absolument garanti si les investigateurs disposent de moyens suffisants.

Cette facilité et cet anonymat sont une force mais également un danger pour les utilisateurs peu avertis. En effet, imaginons que votre fournisseur d'accès internet décide de remplacer automatiquement les adresses Bitcoin dans les sites que vous visitez par ses adresses à lui. En toutes bonne foi, vous allez envoyer un paiement à l'adresse qui s'affiche sur votre écran. Mais votre destinataire ne recevra rien. Il est donc important de garantir la validité d'une adresse de paiement et Bitcoin ne résout pas ce problème.

**Comment garder ses bitcoins en sécurité ?**

Si vous avez installé un client Bitcoin sur votre ordinateur, il est impératif de sauvegarder votre fichier wallet.dat et de bien vous souvenir de son mot de passe. Si vous perdez l'un ou l'autre, vos bitcoins sont perdus sans espoir. Vos économies sont donc à la merci d'un crash disque ou d'un vol de laptop si vous n'y prenez garde. D'un autre côté, votre fichier wallet.dat ne doit pas tomber en de mauvaises mains.

Quand aux services de portefeuille Bitcoin en ligne, ils sont la proie des pirates ou des arnaqueurs. J'avais ainsi décidé de ne pas mettre mes œufs dans le même panier en mettant des bitcoins sur TradeHill, qui a fait faillite en emportant tous les bitcoins, sur Bitcoin7, qui a disparu du jour au lendemain et sur Bitmarket, dont le propriétaire s'est fait voler les bitcoins. Une belle leçon…

Garder ses bitcoins en sécurité nécessite donc une attention et une expertise assez pointue.

**L'avenir du Bitcoin**

Malgré ses défauts, Bitcoin permet de s'affranchir du contrôle des banques et des états. Personne ne

contrôle Bitcoin. C'est pourquoi certaines personnes font confiance au Bitcoin. Cette confiance se traduit par une montée des prix. Cette montée des prix est elle même entretenue par les spéculateurs : les personnes qui ne font pas spécialement confiance au Bitcoin mais qui espèrent que les prix vont monter et qui ne font qu'acheter pour revendre plus tard. La proportion entre les spéculateurs et ceux qui achètent des bitcoins pour les dépenser, que ce soit maintenant ou plus tard, est tout à fait inconnue.

Personne ne peut prédire l'avenir. Il est très important de garder à l'esprit que tout achat de bitcoins à titre d'investissement est à haut risque. On n'investit que ce qu'on peut se permettre de perdre totalement.

Dans un futur proche, Bitcoin pourrait résoudre ses problèmes et, en se simplifiant, devenir pour la monnaie ce que l'email est à la communication et finir par s'échanger à plus de 1000$ le bitcoin. De même, une faille dans l'algorithme mathématique pourrait être découverte et faire tomber à zéro la valeur du Bitcoin en quelques heures.

De mon côté, je vous ai déjà raconté comment je voyais l'avenir. À vous de faire confiance au Bitcoin… ou pas !

*Photo par Zach Copley*