LOGIQUE & CALCUL

Bitcoin, la cryptomonnaie

La cryptographie et la puissance des réseaux ont rendu possible l'existence de monnaies purement numériques et dépourvues d'une autorité centrale de contrôle.

Jean-Paul DELAHAYE

Une nouvelle monnaie purement électronique intéresse de plus en plus. Ne s'appuyant sur rien de tangible, le total des devises sorties d'un protocole cryptographique vaut aujourd'hui l'équivalent de un milliard d'euros.

Le *bitcoin* a été proposé en 2008 et mis en œuvre le 3 janvier 2009 par un chercheur, ou peut-être plusieurs, caché sous le pseudonyme de Satoshi Nakamoto. La logique de cette monnaie numérique et la confiance qu'elle inspire seront le but de notre analyse. Le sujet est passionnant du fait de l'originalité, du mystère et du succès de cette construction informatique ; il est important, car on a affaire à un nouveau type de monnaie susceptible de jouer un rôle central en économie ; et il est délicat, car personne ne sait ce que ce montage numérique va devenir.

D'une certaine façon, toutes les monnaies sont électroniques : depuis longtemps, presque toutes les opérations bancaires se réduisent à des jeux d'écritures opérés dans les mémoires des ordinateurs. Cela signifie que l'on sait faire des systèmes informatiques robustes manipulant l'argent, même quand il s'agit de dizaines de milliards d'euros. Certes, les pannes, les « bugs », les virus, les pirates informatiques existent, mais on réussit assez bien à s'en protéger : l'informatisation du stockage et du transfert massif d'argent n'a pas entraîné de catastrophes. Les crises financières comme celle de 2009 n'ont pas pour origine le dysfonctionnement ou la fraude informatique, mais des erreurs d'analyse économique et financière commises par des humains, qui sont par ailleurs parfois trop voraces, voire malhonnêtes.

Pas d'autorité centrale

Aujourd'hui, toute monnaie repose sur une autorité centrale : une banque, adossée à un État ou à une association d'États. C'est aussi le cas de tous les systèmes de pseudo-monnaies électroniques privées, les monnaies « complémentaires » ou « alternatives ». Elles permettent des paiements par Internet *(Paypal)*, le commerce au sein d'un jeu sur le réseau (le dollar *Linden* de *Second Life*) ou la fidélisation des clients (les *miles* des compagnies aériennes, les points que votre superette inscrit sur votre compte à chaque passage aux caisses).

Les *bitcoins* sont conçus pour s'autoréguler. Le bon fonctionnement des échanges est garanti par une organisation générale que tout le monde peut examiner, car tout y est public : les protocoles de base, les algorithmes cryptographiques utilisés, les programmes les rendant opérationnels et les données des comptes.

À tout instant, chacun peut savoir combien il y a de *bitcoins* sur chaque compte existant et participer à la vérification des nouvelles transactions. Cette transparence totale n'empêche pas l'anonymat, les propriétaires des comptes n'étant pas tenus de se déclarer. C'est presque un paradoxe : tout mouvement de *bitcoins* est public et, pourtant, l'anonymat des détenteurs est protégé.

La possession des *bitcoins* est matérialisée par une suite de chiffres et de lettres qui constituent un porte-monnaie virtuel (ou compte). Une personne peut détenir plusieurs porte-monnaie. Le porte-monnaie comporte le montant en *bitcoins* de l'argent qu'il contient, une clef publique qu'on peut laisser circuler et une clef privée qui doit rester secrète, car son détenteur peut dépenser l'argent du porte-monnaie.

Tout support convient pour conserver la suite de symboles constituant votre porte-monnaie : papier, clef USB, la mémoire, etc. Grâce à des logiciels adéquats, vous pouvez gérer votre porte-monnaie sur votre ordinateur ou votre téléphone. Nombre de ces logiciels sont développés dans le cadre d'un projet *open source* : les programmes ne sont pas secrets et ceux qui le veulent peuvent contrôler ce qu'ils font et même contribuer à leur amélioration *(voir https://multibit.org/)*.

Pour avoir des *bitcoins* sur un compte, il faut soit qu'un détenteur de *bitcoins* vous en ait donné, par exemple en échange d'un bien, soit passer par une plate-forme informatique qui convertit des devises classiques en *bitcoins*, soit les avoir gagnés en participant aux opérations de contrôle