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

1. La signature et l'identification d'un document

Un protocole de signature à double clef est la donnée de deux fonctions f et g permettant de signer les messages et d'interpréter les signatures. Ces fonctions sont connues de tous. Nous ne nous préoccupons pas ici de la teneur du message, mais seulement de son identification.

À Alice sont associées deux clefs, A_{pri} (clef privée) et A_{pub} (clef publique). Ce sont des suites de chiffres. A_{pub} est accessible à tous, mais la clef A_{pri} n'est connue que d'Alice. Il est impossible en pratique de déduire A_{pri} de la connaissance de A_{pub}.

Les deux fonctions f et g servent à signer un message et à lire la signature.

Soit M un message à signer. Alice applique f aux données A_{pri} et M : $f(A_{pri}, M) = M'$. Ce sera le message signé par Alice. Toute personne ayant en main M' et connaissant la clef publique d'Alice vérifiera que c'est bien Alice qui a signé le message : pour cela, elle appliquera la fonction de lecture g aux données A_{pub} et M', ce qui donne M, car $g(A_{pub}, M') = M$. Le fait qu'il soit nécessaire d'appliquer la clef publique d'Alice à M' pour prendre connaissance du message empêche toute falsification du message M signé.

Il est parfois commode pour Alice de transmettre à la fois M et M', M' servant seulement à contrôler pour ceux qui le veulent qu'Alice a bien signé M avec sa clef privée.

Il existe de nombreuses façons de construire les fonctions f et g, mais la monnaie *bitcoin* est fondée sur la cryptographie à courbes elliptiques. La courbe employée est celle notée secp256k1. On aurait pu utiliser l'algorithme RSA, plus connu, mais il nécessite des clefs plus longues. La sécurité du système *Bitcoin* repose sur l'inviolabilité de la signature.

Les signatures de Napoléon Bonaparte.

collectif de la monnaie (nous verrons plus loin comment).

La gestion d'un porte-monnaie doit être très soigneuse. Si vous le perdez en l'effaçant par mégarde ou si vous oubliez le code secret qui permet d'y accéder, alors son contenu est perdu, comme quand vous lancez par-dessus bord un porte-monnaie réel au milieu de l'océan. De nombreux *bitcoins* ont ainsi été perdus par des utilisateurs imprudents ou négligents. Il n'est pas impossible non plus qu'on vous vole votre porte-monnaie virtuel, par exemple à l'occasion d'une intrusion dans votre ordinateur par un hacker. Pour éviter cela, certains porte-monnaie contenant d'importantes sommes en *bitcoins* sont gardés sur des ordinateurs non connectés au réseau ou éteints.

La cohérence des comptes, et donc la solidité de la monnaie *bitcoin*, se fonde sur un principe général de la théorie *Money is memory* de l'économiste américain Narayana Kocherlakota. Ce principe s'exprime ici sous la forme suivante :

– toutes les transactions faites depuis le début des *bitcoins,* le 3 janvier 2009, sont publiques et, à chaque instant, la somme totale des *bitcoins* émis est connue de tous, ainsi que le contenu de chaque porte-monnaie (mais pas le détenteur de ce porte-monnaie) ;

– seul celui qui connaît la clef secrète d'un porte-monnaie peut dépenser son contenu en envoyant tout ou partie de ce dernier à un autre porte-monnaie, cela à la vue de tous, ce qui permet à tous de connaître à chaque instant le contenu de chaque porte-monnaie ;

– tous ceux qui le souhaitent peuvent participer au calcul général de la répartition des *bitcoins* entre les porte-monnaie, cela à l'aide de logiciels (libres et gratuits) dont la correction est contrôlable par tous.

On n'utilise pas ici la cryptographie à clef publique pour cacher de l'information, mais pour signer les transactions. Toute transaction est irréversible, sauf accord explicite des deux contractants pour réaliser une transaction inverse. Quand vous avez dépensé l'argent d'un porte-monnaie, personne n'a autorité pour demander à celui qui a reçu l'argent de le rendre. C'est là une grande différence avec les monnaies numériques à autorité de contrôle centralisée où, assez fréquemment, des transactions sont annulées, parfois plusieurs jours après leur réalisation, ce qui donne lieu à toutes sortes d'escroqueries. L'absence d'autorité centrale et l'anonymat des comptes font qu'il sera très difficile d'agir sur celui qui détient le porte-monnaie ayant reçu vos *bitcoins*... même s'il ne vous livre pas l'achat que vous pensiez régler.

Ce système simplifié des *bitcoins* a une faille qui a contraint son inventeur à ajouter une série de dispositifs cryptographiques au mécanisme de base. La faille est que le propriétaire d'un porte-monnaie pourrait tenter de dépenser deux fois l'argent qu'il contient. Ces doubles dépenses seraient impossibles si les échanges étaient instantanés sur le réseau et si tout propriétaire d'un porte-monnaie participait au calcul continu du contenu de tous les porte-monnaie : sous cette hypothèse de connectivité totale et parfaite, celui qui recevrait l'argent d'un porte-monnaie déjà vidé (ou insuffisamment pourvu) refuserait la transaction, qui serait simultanément considérée invalide par tous.

Des améliorations

Malheureusement, les échanges électroniques ne sont pas instantanés, et certaines parties d'un réseau sont parfois temporairement déconnectées du reste. De plus, tous les utilisateurs de *bitcoins* ne souhaitent pas participer à la vérification continue de toutes les transactions et au recalcul permanent du solde de la totalité des comptes, car cela demande une grande puissance informatique et beaucoup de mémoire. Il faut donc améliorer le modèle.

Les améliorations se fondent sur une série de protocoles qui rendent la monnaie *bitcoin* résistante aux pannes du réseau ou de certaines machines et aux tentatives de manipulation de la monnaie ou de tricheries (dont les doubles dépenses). Ces perfectionnements rendent aussi facultative la participation au contrôle global des porte-monnaie ; pour éviter que trop peu de nœuds du réseau participent