4. Les crypto-monnaies, une réalité virtuelle ?

Jean-Guillaume Dumas et Pascal Lafourcade

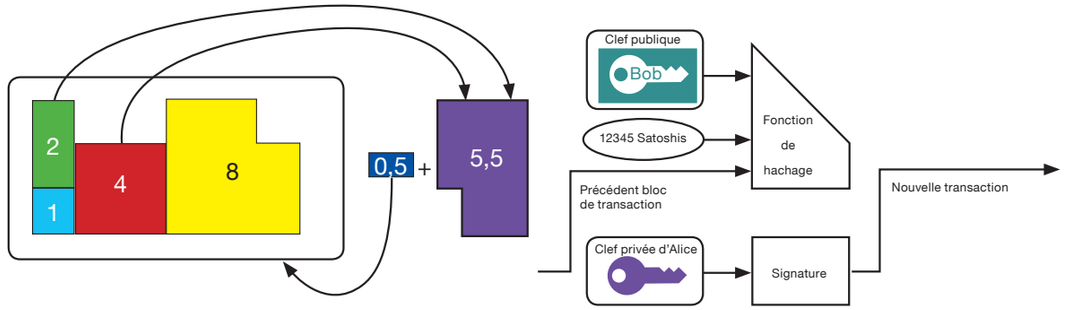
Les monnaies virtuelles permettent de transférer de l'argent sans avoir besoin de support physique et, généralement, sans faire appel à un intermédiaire. Elles doivent avoir au moins les mêmes propriétés de sécurité que les monnaies réelles : permettre les échanges, empêcher la duplication ou encore garantir l'anonymat des transactions. Récemment, plusieurs monnaies virtuelles cryptographiques ont vu le jour, telles que Bitcoin, Peercoin, Primecoin ou Litecoin. Aujourd'hui, ce sont des monnaies alternatives, car elles n'ont de cours légal dans aucun pays, même si elles sont pour l'instant largement tolérées.

Principe des crypto-monnaies

Une crypto-monnaie est une monnaie dématérialisée et souvent décentralisée utilisant des mécanismes cryptographiques pour valider ses transactions. La décentralisation implique qu'il n'est pas nécessaire d'avoir recours à une banque centrale pour émettre la monnaie ni pour gérer les transactions. Par exemple, Bitcoin repose sur certains de ses membres, appelés mineurs, pour assurer la création de monnaie et la validation des transactions effectuées. Par construction, l'émission de monnaie est limitée à un nombre maximum de devises, fixé par avance (21 millions de Bitcoins), environ la moitié étant en circulation à ce jour. L'émission de devises et la validation des transactions reposent en général sur le concept de preuve de travail, ou minage, par analogie avec les chercheurs d'or travaillant dans les mines. Pour valider les transactions courantes, un membre actif du système doit avoir résolu un calcul difficile, celui qui réussit à faire ce travail est récompensé en devises nouvellement créées.

La sécurité de ces systèmes repose sur une architecture à clé publique. Dans l'exemple des transactions en Bitcoins, chaque utilisateur possède un ou plusieurs comptes Bitcoin, correspondant à une clé publique, et une clé secrète (connue uniquement de lui), permettant de signer électroniquement les transactions. Les Bitcoins sont obtenus soit lors de transactions avec d'autres utilisateurs, soit comme récompenses de minage. Pour dépenser des Bitcoins, il faut que l'utilisateur en possède suffisamment. Ensuite, l'intégralité des pièces utilisées lors d'une transaction en Bitcoins doit être dépensée. Ainsi, supposons qu'Alice possède dans son portefeuille 1, 2, 4 et 8 Bitcoins et qu'elle souhaite transférer 5,5 Bitcoins à Bob. Elle peut utiliser ses deux « pièces » de 4 et 2 Bitcoins afin de transférer 5,5 Bitcoins à Bob et 0,5 Bitcoin à elle-même (figure).

Pour valider un bloc de nouvelles transactions, un mineur doit résoudre un objectif de hachage sur une « *blockchain* » : c'est-à-dire trouver une valeur aléatoire qui produira une empreinte commençant par un zéro de plus que le précédent objectif de hachage (à l'heure actuelle, près de 10^{21} calculs par validation pour Bitcoin). Comme le système est distribué, il est possible d'avoir plusieurs chaînes de blocs validant les mêmes transactions, or seule la plus longue persiste. Ainsi pour qu'une transaction soit valide et afin d'éviter la double dépense, il est conseillé d'attendre que 6 blocs soient validés par des mineurs, ce qui correspond à environ une heure de calcul. Par exemple, si Alice souhaite faire une transaction de 12 345 Satoshis (1 Bitcoin vaut cent millions de Satoshi) pour Bob, pour éviter les doubles dépenses, elle doit signer avec sa clé secrète l'empreinte



Fonctionnement d'une transaction en Bitcoins, à gauche un portefeuille, à droite une partie de la chaîne. ■

de cette transaction et de la chaîne de toutes les précédentes transactions au monde (la « *blockchain* »).

Anonymat

Le modèle bancaire traditionnel garantit un certain degré d'anonymat, en limitant l'accès aux informations de transactions aux seules parties intervenant dans la transaction et à leurs banques respectives. Au contraire, le modèle des crypto-monnaies révèle publiquement toutes les transactions passées. Toutefois, une forme différente d'anonymat est préservée, puisque l'identité des possesseurs des clés publiques n'est pas nécessaire, seule une preuve de possession de la clé privée associée (la signature électronique de la transaction) est demandée pour dépenser des devises. La perte ou le vol de cette clé revient à perdre les devises qui y sont associées. De plus, le monde entier peut voir qu'un montant est transféré d'une clé publique à une autre, mais sans lien avec des personnes physiques ou morales. Toutefois, toutes les transactions d'une clé donnée sont liées, donc au moment où une personne entre ou sort du système de la crypto-monnaie, l'anonymat doit être levé, au moins auprès de l'organisme d'échange, et l'ensemble des transactions associées à cette clé peut alors être tracé.

Un nouveau système monétaire ?

Le minage décentralisé, dans lequel n'importe quel agent économique peut créer des devises, et la circulation décentralisée de ces devises sur Internet, dans laquelle aucun acteur ne prélève de commission, revêtent l'apparence du libéralisme économique. En réalité, le danger est que la décroissance des rendements implique que les fermes de minage (groupement de mineurs qui permet de garantir un revenu moyen pour chacun) doivent se concentrer afin de rester rentables. À partir du moment où quelques entités privées possèdent une majorité du marché de la certification des transactions, elles détiennent alors en pratique la capacité d'émission monétaire et l'intérêt d'avoir un système distribué est perdu. En cas de succès des transactions, la limitation du nombre de Bitcoins émis provoque une hausse de sa valeur. Or, si la valeur des devises électroniques est vouée à monter, il est préférable de ne pas les utiliser pour faire des achats et de les épargner. En outre, plus une monnaie a de succès, moins elle est utile pour faire des transactions. Mais, ainsi, si elle devient moins utile, sa valeur peut baisser et éventuellement se réguler.

Pour éviter l'écueil de la concentration des fermes de minage une solution peut être de passer d'une crypto-monnaie à une autre. Toutefois, pour chaque monnaie électronique, sa diffusion et son utilisation croissante ne manqueront pas d'attirer les autorités publiques, qui voudront taxer les transactions virtuelles et demanderont la mise en place de points de contrôle officiels des transactions. La même chose arrive aux systèmes d'échanges, de troc ou de monnaies locales : tant qu'ils restent limités à une petite association d'utilisateurs, les pouvoirs publics ne s'en préoccupent pas. S'ils prennent trop d'ampleur et deviennent un moyen d'évasion fiscale, les autorités s'y intéressent et des tribunaux considèrent que les transactions doivent être taxées comme les autres.

Références bibliographiques

- J.-P. DELAHAYE – *Les preuves de travail (Bitcoin, Spam, etc.)*, Pour la science, avril 2014.
- J.-P. DELAHAYE – *Le Bitcoin : la cryptomonnaie*, Pour la science, décembre 2013.
- J.-G. DUMAS, P. LAFOURCADE et P. REDON – *Architectures PKI et communications sécurisées*, Dunod, 2015.