Nous nous réjouissons de relancer la rubrique « L'ABC de l'économie », qui avait été mise sur la touche fin 2015. Cette rubrique explique les concepts économiques de tous les jours. Consultez aussi les vidéos de « L'ABC de l'économie » en anglais à l'adresse www.fandd.org.

Que sont les cryptomonnaies ?

L'avènement de monnaies d'un nouveau genre présente des avantages, mais ne va pas sans risques

Antoine Bouveret et Vikram Haksar

ELLES SONT APPARUES par centaines, sous des noms fantaisistes : primecoin, dash, ou encore electra. Elles ont suscité une sorte de culte dans les milieux technophiles. Leurs cours sont extrêmement fluctuants. Certains pensent que ces bribes de code informatique sont vouées à remplacer un jour les échanges monétaires actuels. Questions : de quoi au juste ces cryptomonnaies sont-elles faites et pourquoi des gens leur accordent-ils la moindre valeur ? Pour y répondre, commençons par retracer l'évolution de la monnaie à travers les âges.

À quoi sert la monnaie ?

La monnaie fait office de réserve de valeur, permet d'acquérir des biens et services, et sert d'unité de compte pour évaluer un bien. Avant l'avènement de la monnaie, les sociétés humaines échangeaient directement biens et services : un boisseau de blé contre un cochon, par exemple. Ce n'était guère efficace. La complexité croissante des sociétés a fait naître des systèmes de paiement en matières naturelles telles que coquillages, cuivre, argent ou or. Certains États se sont dotés d'une monnaie fiduciaire (qui n'a pas de valeur intrinsèque, sinon la promesse du paiement), telle que les billets qui circulaient en Chine au VIII^{e} siècle sous la dynastie Tang.

La plupart des monnaies fiduciaires primitives n'étaient ni très stables ni communément acceptées, car les gens ne croyaient guère que l'émetteur honorerait ses engagements de paiement. Les gouvernants cédaient à la tentation de recourir à la planche à billets pour acheter des biens ou relever les salaires, ce qui nourrissait l'inflation (souvenons-nous des brouettes de billets nécessaires pour aller faire son marché en Allemagne, après la Première Guerre mondiale). De nos jours, les banques centrales cherchent à maintenir la stabilité des prix en régulant l'offre de monnaie au nom de l'État.

Comptabilité et registres

L'expansion et la complexité croissantes du système financier ont nécessité la création d'intermédiaires

fiables et de systèmes comptables crédibles. L'apparition de la comptabilité en partie double en Italie durant la Renaissance fut une innovation majeure qui renforça le rôle des grandes banques privées. Les temps modernes virent l'émergence des banques centrales au sommet des systèmes de paiement. Du fait de l'informatisation de la comptabilité des banques, le rôle de coordinateur des banques centrales s'est accentué.

Comment le système fonctionne-t-il ? Les institutions financières établissent dans leurs registres les soldes des comptes de leurs clients, tandis que la banque centrale valide dans son fichier central les transactions entre institutions financières. Par exemple, Mehrnaz puise de l'argent sur son compte auprès de la banque A pour acheter des biens à Marie, dont le compte est domicilié à la banque B. La banque A débite le compte de Mehrnaz. La banque centrale transfère les fonds de la banque A à la B et enregistre la transaction dans son fichier central. La banque B ajoute alors les fonds au compte de Marie. Par conséquent, le système est fondé sur la confiance envers la banque centrale et sur son aptitude à préserver l'intégrité du fichier central et à veiller à ce que les mêmes fonds ne fassent pas double emploi.

ILLUSTRATION : THE NOUN PROJECT / MASSUPA KAEWGAHYA

Dans le cas de nombreuses cryptomonnaies, par contre, il n'y a pas besoin d'un agent central fiable. Elles utilisent la technologie des registres partagés, du type chaînes de blocs, pour créer un registre (essentiellement une base de données) fonctionnant en réseau. Pour empêcher le double emploi des mêmes fonds, chacun des usagers vérifie et valide les transactions au moyen de technologies issues de l'informatique et de la cryptographie. Une fois que les membres du réseau parviennent à un consensus décentralisé, la transaction est ajoutée au registre et validée. Le registre donne un historique complet des transactions liées à une cryptomonnaie donnée, qui est permanent et ne peut pas être modifié par un seul individu. Ce système de validation consensuelle des transactions entre comptes au sein d'un réseau constitue une avancée technologique fondamentale.

Les usagers du réseau qui vérifient et valident les transactions sont en général récompensés en cryptomonnaie fraîche. Beaucoup de cryptomonnaies sont aussi pseudo-anonymes : le détenteur d'un compte détient deux clés. L'une est publique, par exemple un numéro de compte ; la deuxième clé, privée, est nécessaire pour achever la transaction. Reprenons l'exemple précédent : Mehrnaz veut payer en cryptomonnaie les marchandises que Marie lui vend. Pour ce faire, elle déclenche la transaction à l'aide de sa clé privée, ABC, et Marie s'identifie avec la sienne, XYZ. Les membres du réseau vérifient que ABC dispose des fonds qu'elle veut virer à XYZ en résolvant une énigme cryptographique. Une fois le problème résolu, la transaction est validée, un nouveau bloc représentant la transaction est ajouté à la chaîne de blocs, et les fonds sont transférés du compte d'ABC à celui de XYZ.

Avantages et inconvénients

Nous savons maintenant comment la technologie fonctionne. Revenons à la genèse des cryptomonnaies. La première, bitcoin, a été créée en 2009 par un programmeur (ou un groupe de programmeurs) sous le pseudonyme de Satoshi Nakamoto. En avril 2018, il y avait, d'après coinmarketcap.com, plus de 1.500 cryptomonnaies, les plus utilisées étant bitcoin, ether et ripple.

En dépit du battage médiatique, les cryptomonnaies ne remplissent pas les fonctions de base de la monnaie : réserve de valeur, achat des biens et services et unité de compte. Parce que leurs cours sont extrêmement fluctuants, elles ne peuvent jusqu'à présent guère servir d'unité de compte ni de réserve de valeur. N'étant pas largement acceptées, elles ne peuvent pas servir de monnaies d'échange. À la différence de la monnaie fiduciaire, le coût de production de maintes cryptomonnaies est élevé, du fait qu'il faut une grosse quantité d'énergie pour alimenter les ordinateurs nécessaires pour résoudre les énigmes cryptographiques. Enfin, l'émission décentralisée signifie qu'aucune entité ne se porte caution pour les cryptomonnaies si bien que leur acceptation est basée uniquement sur la confiance des usagers.

Les cryptomonnaies et les technologies qui les sous-tendent ont des avantages, mais aussi des inconvénients. La technologie des registres partagés pourrait diminuer le coût des transferts internationaux, notamment les envois de fonds, et favoriser l'inclusion financière. Actuellement, les transferts de fonds peuvent s'effectuer en quelques heures, au lieu de plusieurs jours. La technologie peut être utile en dehors du secteur financier. Elle peut, par exemple, servir à stocker en toute sécurité des documents importants, tels que les dossiers médicaux ou les titres de propriété. En revanche, beaucoup de cryptomonnaies étant pseudo-anonymes, elles risquent fort d'être mises au service du blanchiment de capitaux ou du financement du terrorisme, s'il n'y a pas d'intermédiaire pour vérifier l'intégrité des transactions ou l'identité de leurs auteurs. Les cryptomonnaies pourraient aussi éventuellement compliquer la tâche des banques centrales, si elles affectaient la gestion de la masse monétaire et donc la conduite de la politique monétaire. FD

La technologie des registres partagés pourrait diminuer le coût des transferts internationaux, notamment les envois de fonds, et favoriser l'inclusion financière.

ANTOINE BOUVERET est économiste et **VIKRAM HAKSAR** directeur assistant au département de la stratégie, des politiques et de l'évaluation du FMI.