L'ÉCO EN BREF

Le bitcoin

BANQUE DE FRANCE
EUROSYSTÈME

L'essentiel

En 2008, un certain Satoshi Nakamoto met en ligne un article décrivant le fonctionnement d'un système d'échange numérique appuyé sur une nouvelle technologie, la blockchain. Ce qui s'échange sur ce système, ce ne sont pas des euros ou des dollars, mais des actifs numériques appelés bitcoins. Ces actifs sont créés et échangés par les ordinateurs des utilisateurs, connectés en réseau, au moyen de calculs mathématiques complexes, faisant appel à des techniques de cryptographie (c'est-à-dire de codage de données) : c'est la raison pour laquelle on parle de « crypto-actifs ». Si le bitcoin constitue le crypto-actif le plus médiatisé et le plus valorisé, on recense, mi-2018, plus de 1 600 actifs de ce type dans le monde : l'ether, le ripple, etc.

Les crypto-actifs ne peuvent pas être qualifiés de monnaie car ils n'en remplissent pas les trois fonctions essentielles :

- réserve de valeur : la valeur des crypto-actifs n'est pas suffisamment stable pour que celui qui en détient soit certain de conserver sa richesse dans le temps ;

- instrument de transaction : les crypto-actifs n'ont pas de cours légal, donc rien n'oblige les commerçants, les entreprises ou les administrations à les accepter en paiement, contrairement à l'euro qui est la seule monnaie légale en France ;

- unité de compte : du fait de leur très grande volatilité, les crypto-actifs ne peuvent pas servir à exprimer et à comparer de façon fiable la valeur de biens et de services courants. Dans les faits, très peu de biens ou de services ont un prix libellé en crypto-actifs.

Pourquoi la valeur des crypto-actifs est-elle très volatile ?

La valeur des crypto-actifs ne repose sur aucun sous-jacent économique réel, à l'inverse par exemple des actions qui représentent des parts de capital d'une entreprise. De ce fait, cette valeur peut évoluer très rapidement à la hausse comme à la baisse, indépendamment des évolutions de l'environnement économique. Ils subissent donc une forte volatilité.

Un peu d'histoire

- **2008** Création du protocole informatique du bitcoin par « Satoshi Nakamoto ». Les promoteurs du bitcoin disent être influencés par la crise financière et par les idées de l'économiste F. von Hayek.
- **2009** Première transaction en bitcoin.
- **2010** Premier achat en bitcoin (2 pizzas, pour 10 000 bitcoins).
- **2013** Introduction de la blockchain Ethereum, qui permet aux utilisateurs de créer des contrats intelligents (*smart contracts*).
- **2013** La Banque de France met en garde les investisseurs contre les risques liés aux crypto-actifs.
- **2014** Faillite de la première plateforme d'échange de bitcoins, Mt. Gox, après le vol de 650 000 bitcoins (285 millions de dollars) ; le cours du bitcoin chute fortement.
- **2017** Le cours du bitcoin atteint son plus haut niveau en décembre, à près de 16 000 euros. Il retombe sous les 7 000 euros en mai 2018.
- **2018** L'équivalent de 530 millions de dollars en crypto-actifs est dérobé au cours du piratage de la plateforme japonaise d'échange Coincheck.
- **2018** Le G20 appelle les instances établissant les normes internationales à surveiller les crypto-actifs et leurs risques.

Quelques chiffres

48 *TWh*
Consommation annuelle d'électricité du système bitcoin (équivalent de la consommation de la Nouvelle-Zélande)

95 %
Part des bitcoins en circulation détenue par 2,5 % des investisseurs en bitcoin

1 600
Nombre de crypto-actifs recensés mi-2018

40 %
Part de marché du bitcoin parmi les crypto-actifs

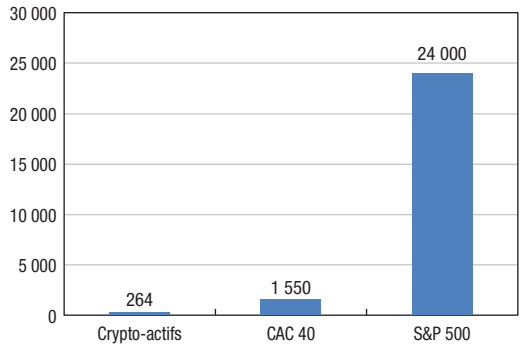
264 *milliards de dollars*
Capitalisation totale des crypto-actifs en juillet 2018

Illustration de cette volatilité : en 2017, la valeur du bitcoin est passée de 946 euros le 1er janvier à un pic de 15 992 euros le 12 décembre, avant de redescendre sous la barre des 7 000 euros le 16 mai 2018.

Les investisseurs ne peuvent récupérer leurs fonds en devises que si d'autres utilisateurs désirent acquérir les mêmes crypto-actifs. De ce fait, le cours d'un crypto-actif peut à tout moment s'effondrer si les investisseurs voulant vendre ne trouvent pas d'acquéreurs et se retrouvent détenteurs d'actifs illiquides. Cette situation évoque des précédents de bulles spéculatives.

Pour le moment, le risque de déstabilisation du système financier est cependant limité, car la valeur totale estimée de l'ensemble des crypto-actifs existants est très faible au regard de l'encours des actifs financiers plus classiques, et notamment des capitalisations des grands indices boursiers.

Comparatif des capitalisations en juillet 2018
(en milliards de dollars)



Sources : Bloomberg (CAC 40 : bourse de Paris ; S&P 500 : bourses américaines) ; coinmarketcap.com (crypto-actifs).

Les crypto-actifs et vous

Si la technologie sous-jacente de la blockchain utilisée par les crypto-actifs représente une innovation prometteuse, les crypto-actifs n'en comportent pas moins des risques pour leurs détenteurs. Il y a bien sûr le risque de perte financière lié à la volatilité des cours. Il existe également un risque de fraude important : des escrocs proposent à la vente des crypto-actifs qui en réalité n'existent pas ; des pirates informatiques attaquent les plateformes d'échange de crypto-actifs pour dérober le contenu des portefeuilles électroniques. En outre, l'anonymat qui caractérise la plupart des crypto-actifs favorise un risque d'utilisation de ces actifs à des fins criminelles (vente sur internet de biens ou services illicites), de fraude fiscale, de blanchiment ou de financement du terrorisme.

La prévention de ces différents risques appelle un encadrement réglementaire des activités liées aux crypto-actifs, notamment pour lutter contre le blanchiment des capitaux et le financement du terrorisme, protéger les investisseurs, préserver l'intégrité des marchés, y compris face au cyber-risque, et enfin, préserver la stabilité financière si ces activités devaient continuer à se développer. À cette fin, la Banque de France et l'Autorité de contrôle prudentiel et de résolution ont proposé de créer un statut spécifique pour les entreprises qui offrent des services en crypto-actifs. Néanmoins, compte tenu du caractère transfrontalier de ces activités, en lien avec l'utilisation d'internet, une pleine maitrise des risques nécessitera une coordination au niveau international (notamment dans le cadre du G-20).

Comprendre

Comment fonctionne la blockchain ?

Le bitcoin et les autres crypto-actifs s'appuient sur une technologie appelée « blockchain » (« chaîne de blocs »). Concrètement, les utilisateurs de la blockchain émettent des messages chiffrés qui sont rassemblés en blocs de données liés entre eux. Chaque bloc a sa signature cryptographique unique, qui dépend des informations qu'il contient et de la signature du bloc qui le précède, ce qui permet de le situer dans la blockchain. L'ensemble de la chaîne constitue ainsi une base de données sécurisée contenant l'historique de tous les échanges pour un crypto-actif donné, depuis la création de la chaîne.

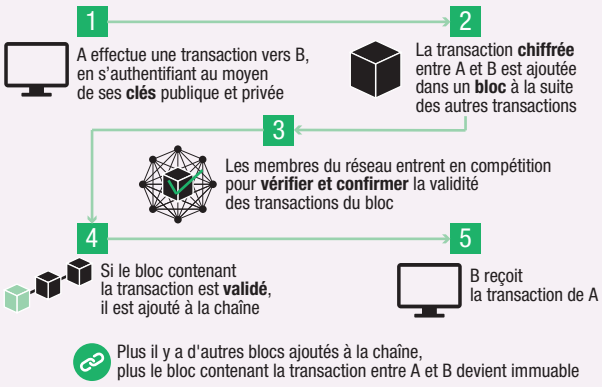
Pourquoi la blockchain est-elle si intéressante ?

La nouveauté apportée par le système bitcoin a été de pouvoir faire fonctionner un système de blockchain sécurisée de manière complétement décentralisée. Ceci signifie qu'il n'y a pas, comme dans les systèmes classiques, une entité centrale (telle qu'une banque centrale, par exemple) qui joue le rôle de « tiers de confiance » pour garantir l'authenticité des donneurs d'ordre (c'est-à-dire s'assurer que le détenteur d'un crypto-actif est bien légitime) et l'intégrité des transactions (il n'est pas possible de modifier une transaction enregistrée). Dans les systèmes comme le bitcoin, c'est la technologie associée à la validation des transactions par une majorité des utilisateurs eux-mêmes qui constitue la sécurité de la chaîne. En récompense de leur travail de validation (processus dit de « *mining* »), les utilisateurs, qu'on appelle des « mineurs », obtiennent des bitcoins.

Quelles sont les limites de la blockchain ?

La blockchain fait d'abord face à des contraintes techniques, en tout cas dans ses mises en œuvre les plus répandues. Il en va ainsi des performances atteintes à ce jour pour des blockchains dites « ouvertes » fonctionnant selon un protocole de validation, puisque la puissance de calcul nécessaire à l'enregistrement des transactions augmente au fur et à mesure que le réseau se développe. Au-delà d'un certain seuil, la lenteur de traitement des opérations et le nombre limité de transactions traitées la rendent peu efficace. Par ailleurs, la blockchain n'est pas inviolable. En théorie, le fait que les transactions soient contrôlées par la majorité des utilisateurs garantit sa fiabilité. En pratique, dans certaines configurations qui dépendent des choix technologiques retenus, un mécanisme de collusion entre utilisateurs peut mener à une prise de contrôle : les transactions à valider peuvent alors être choisies, ou encore l'historique modifié. De plus, il arrive que les créateurs du système commettent des erreurs de codage qui rendent les blockchains vulnérables : des pirates sont par exemple parvenus à dérober près de 50 millions de dollars en 2016 en exploitant une faille dans le protocole de la blockchain d'Ethereum.

Concrètement, comment ça marche ?



Source : Banque de France, d'après Blockchain France.

Vers une crypto-monnaie de banque centrale ?

Lorsque l'usage des pièces et des billets diminue au profit de moyens de paiement électroniques (carte, virement, prélèvement), la banque centrale devrait-elle créer une version digitale du billet de banque, qui serait alors une « crypto-monnaie » légale et garantie par les autorités publiques ?

Cette évolution est actuellement à l'étude par la banque centrale de Suède, pays où l'on observe une diminution prononcée de l'usage de la monnaie fiduciaire (c'est-à-dire les billets et les pièces). Concrètement, cela reviendrait à créer une alternative numérique à la monnaie fiduciaire, stockée par les utilisateurs sur un portefeuille électronique, qui fonctionnerait sur une infrastructure entièrement gérée par la banque centrale et différente de celle des autres moyens de paiement électroniques.

Un tel projet n'est, à l'heure actuelle, pas envisagé au sein de l'Eurosystème, où le billet reste d'un usage très répandu et où les utilisateurs disposent d'une large variété d'instruments électroniques de paiement efficaces, sûrs et innovants – à l'image du virement instantané. De plus, une telle évolution soulève – au-delà du traitement technique – des questions qui doivent encore être analysées en termes d'impacts sur la mise en œuvre de la politique monétaire, sur la structure du système financier, ou sur le nécessaire maintien d'un accès – pour les populations les plus fragiles – à des moyens de paiement non digitaux, comme le billet.

Pour en savoir plus

À lire

- L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives, Banque de France, 2018
- Les crypto-monnaies, J-P Landau, rapport au ministre de l'Économie et des Finances, 2018
- Le bitcoin : une fiche pratique, Institut national de la consommation (INC), 2018

À voir

- Le bitcoin, émission « Le gros mot de l'éco », HEC – France 24, 2018
- Le bitcoin peut-il remplacer l'€uro ?, vidéo lauréate du concours étudiants Euro Vidéo Challenge BCE-Journées de l'économie 2017
- Le bitcoin, vidéo et infographie, 2e et 3e lauréates du concours étudiants La finance pour tous 2017

Liens utiles

- Blockchain, ABC de l'économie, Banque de France
- Les ICOs (levées de fonds en jetons numériques), La finance pour tous, 2018
- F. von Hayek, Histoire de la pensée économique, fresque interactive Citéco
- Monnaies locales et crypto-actifs, Mes questions d'argent