BITCOIN ET *BLOCKCHAIN* : QUELLES OPPORTUNITÉS ?

JEAN-MARC FIGUET*

Depuis l'avènement de la monnaie comme intermédiaire des échanges entre agents économiques, ses formes ont évolué. Les métaux précieux ont été remplacés par les monnaies-papier convertibles en or qui elles-mêmes, depuis la fin des accords de Bretton Woods, ont été remplacées par les monnaies fiduciaires émises par les banques centrales. La monnaie n'a donc pas de forme particulière, mais évolue avec le temps. Le dénominateur commun est la confiance de la communauté des usagers qui confère à la monnaie une valeur d'échange permettant de conclure définitivement une transaction. Hicks (1967) considère que la forme importe peu. Ce qui importe finalement ce sont les fonctions que la monnaie assure : moyen de paiement, unité de compte et réserve de valeurs. Mishkin (2004, p. 44) définit d'ailleurs la monnaie comme « *anything that is generally accepted in payment for goods and services or in the repayment of debts* ». La monnaie peut être considérée comme une convention entre les agents puisque, selon Orléan (2004, p. 26), « la "substance" de la monnaie, c'est l'accord qui se fait autour d'elle pour la considérer comme richesse sociale à l'issue d'un processus autoréférentiel ».

L'évolution technologique a conduit à la création et à l'émergence d'une nouvelle forme de monnaies : la monnaie virtuelle ou digitale, baptisée aussi crypto-monnaie ou monnaie marchandise synthétique (Selgin, 2013). Ces monnaies électroniques sont créées à partir d'un protocole cryptographique de pair à pair, donc sans banque centrale (Narayan *et al.*, 2016). Au sens strict du terme, il s'agit de monnaies privées au sens de Hayek (1976, p. 13) : « *The further pursuit of the*

* Professeur, Larefi, université de Bordeaux. Contact : jean-marc.figuet@u-bordeaux.fr.

suggestion that government should be deprived of its monopoly of the issue of money opened the most fascinating theorical vistas and showed the possibility of arrangements which have never been considered. » Hayek envisageait qu'un agent privé puisse émettre la monnaie légale à la place de l'État. Dans le cas des monnaies virtuelles, l'émetteur n'est pas le fait d'un agent, mais d'un réseau collaboratif ouvert à tous. Plusieurs centaines de ces monnaies sont actuellement en circulation, dont litecoin, peercoin, auroracoin, dogecoin, ripple, etc. Le site coinmarket.com recense, en avril 2016, plus de six cents monnaies virtuelles dont la capitalisation avoisinerait 8 Md$. La plus importante d'entre elles est le bitcoin dont la capitalisation serait supérieure à 6 Md$. Le bitcoin a été créé en 2008 par le collectif Satoshi Nakamoto pour qui : « *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.* » (Nakamoto, 2008, p. 1).

L'émergence de ces monnaies digitales constitue une innovation qui suscite l'intérêt des banquiers centraux et des régulateurs (Banque de France, 2013 ; EBA, 2014 ; BCE, 2015 ; CPMI, 2015), des banques commerciales (par exemple, Santander InnoVentures, 2015) et des économistes en tant qu'objet d'analyse (Blundell-Wignall, 2014 ; Böhme *et al.*, 2015 ; Velde, 2015). La problématique est de définir la nature de ces crypto-monnaies et leur impact sur les systèmes monétaires et financiers contemporains. Autrement dit, ces monnaies virtuelles remplissent-elles les fonctions traditionnellement attribuées à la monnaie ? Quels sont les bénéfices et les risques liés à leur utilisation ? Nous montrons que le bitcoin n'a pas aujourd'hui les attributs d'une monnaie traditionnelle. Néanmoins la technologie utilisée, la chaîne de blocs (*blockchain*), peut conduire à une évolution de l'organisation centralisée des paiements et des transactions financières. Le mouvement, qualifié de disruptif, posera cependant des problèmes opérationnels et juridiques que les régulateurs devront gérer.

Le bitcoin : une monnaie ?

Après avoir rappelé les principes de fonctionnement de base du bitcoin, nous analysons ses caractéristiques monétaires.

Les caractéristiques du bitcoin

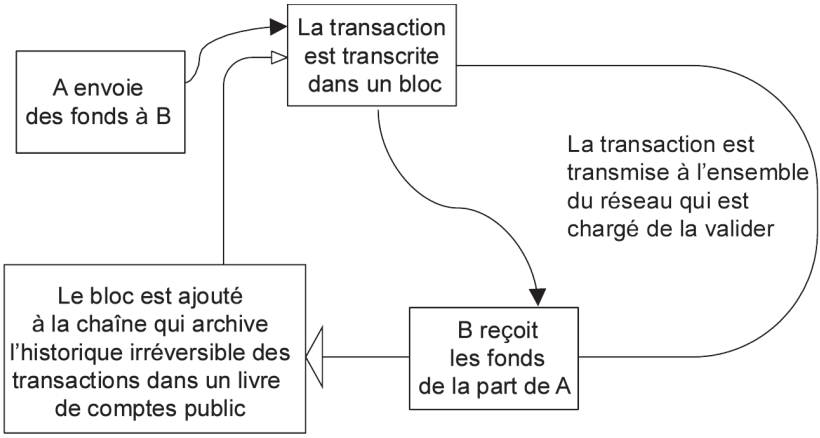
Une monnaie virtuelle est une suite de 0 et de 1. Dans le cas du bitcoin, le protocole cryptographique implique que seuls 21 millions d'entre eux seront créés d'ici à 2140. En mars 2016, plus de 15 millions sont en circulation. Chaque agent peut obtenir des bitcoins en les achetant sur des plateformes d'échange contre de la monnaie traditionnelle (euro, dollar, etc.), en réalisant des transactions en bitcoins,

ou en participant à la surveillance du réseau et à la création de nouveaux blocs de transaction (activité de minage). La monnaie est stockée dans un porte-monnaie virtuel attaché à un compte. L'ensemble des comptes sont inventoriés dans la chaîne de blocs qui est un registre décentralisé et, *a priori,* infalsifiable du fait du protocole cryptographique. La chaîne de blocs est une technologie algorithmique qui établit la confiance entre deux parties inconnues sans intermédiaire de confiance.

L'intérêt de ce système collaboratif ouvert est que n'importe qui peut consulter les transactions réalisées depuis l'origine, ce qui évite notamment le problème de la double dépense (Dwyer, 2014). Cette technologie est fondée sur un registre comptable en ligne (*distributed ledger*) accessible à tous les ordinateurs connectés qui vérifient l'origine des bitcoins et valide les transactions. Buterin (2015, p. 2) définit la chaîne comme « une couche informatique au-dessus de tout ordinateur y participant qui est un moyen de créer un système sûr à partir de composants individuels qui potentiellement ne le sont pas ».

Le schéma 1 retrace les étapes d'une transaction en bitcoins.

Schéma 1
Une transaction en bitcoins



Les mineurs

Les mineurs, dont une analyse détaillée est fournie par Velde (2015), jouent un rôle central. Ils valident les transactions dans un bloc en résolvant un problème mathématique reposant sur une fonction de hachage (dont le résultat est un *hash*). Les mineurs assurent le rôle de certificateurs. Toutes les dix minutes environ, une page est ajoutée (« miner un bloc ») à la chaîne de blocs existants. Le mineur le plus rapide pour résoudre le problème reçoit une prime de 25 bitcoins

(*coinbase*). Cette prime constitue le processus de création monétaire : la monnaie virtuelle est créée en contrepartie du temps de calcul des ordinateurs. Il n'y a théoriquement ni barrière à l'entrée, ni barrière à la sortie dans ce système de pair à pair. Le marché des mineurs est un marché contestable au sens de Baumol *et al.* (1982). N'importe quel agent peut intégrer la chaîne en mettant la puissance de son ordinateur à disposition du réseau pour miner les prochains blocs. Pratiquement l'offre de bitcoins étant temporellement croissante à taux décroissant, le minage d'un bloc devient de plus en plus difficile selon la formule :

$$\text{Difficulté} = \frac{\text{Temps moyen (en s)} \times \text{Taux de hachage/s}}{2^{32}} \quad (1)$$

La rentabilité de l'activité de minage est décroissante dans le temps. Par contre, le coût de production est croissant. Les mineurs doivent en effet investir dans des ordinateurs dont la puissance de calcul est de plus en plus importante pour augmenter la probabilité de résoudre les premiers le problème. Le marché des mineurs est passé par différentes phases. Au départ, des particuliers pouvaient miner. Mais la croissance de la complexité du problème à résoudre (donc de la puissance de calcul) a conduit à une concentration du marché dominé aujourd'hui par quelques *pools* (F2Pool, AntPool, BitFury, BTCChina Pool, BW.COM, etc.). Le risque serait désormais de voir un *pool* obtenir au moins 51 % de la puissance de calcul. Le *pool* pourrait alors systématiquement encaisser la prime, dépenser plusieurs fois le même bitcoin, bloquer les transactions des tiers, réécrire la chaîne de blocs, donc provoquer l'effondrement de la valeur du bitcoin, etc., ce qui irait à l'encontre des objectifs d'un mineur rationnel, sans compter le coût exorbitant d'une telle attaque. Selon le site bitcoin.watch, la puissance totale du réseau bitcoin serait, en mars 2016, de l'ordre de 1 200 000 pétahash (1 péta = 10^{15}) par seconde, ce qui en ferait aujourd'hui le réseau mondial le plus puissant. Cette course à la puissance est, selon Dupré *et al.* (2015, p. 6), « un élément destructeur de commun d'un point de vue écologique », car elle est énergivore. Pour les mineurs, le niveau des coûts n'est en rien problématique, car ils objectent que la production de moyens et de services de paiement traditionnels implique des coûts bien plus importants (coûts de production, de stockage, de surveillance, etc.) que ceux qu'ils supportent. Et l'émission décentralisée d'une monnaie virtuelle n'implique aucun revenu de seigneuriage, contrairement à l'émission centralisée d'une monnaie fiduciaire.

Les utilisateurs

Pour se procurer des bitcoins, un agent doit télécharger un logiciel libre et ouvert (par exemple, Bittorrent) lui permettant de créer un compte à partir duquel il va échanger une monnaie légale contre des bitcoins, puis réaliser des transactions. À chaque compte sont associées deux clés. La première est totalement publique et permet de débiter ou créditer le compte. La seconde est purement privée et permet à son détenteur d'initier les transactions. Si l'agent décide de gérer seul son compte, son anonymat peut être préservé. Le protocole permet d'assurer la confidentialité des données par la cryptographie asymétrique : les informations financières et les identités des utilisateurs sont protégées. Il peut aussi en confier la gestion à une plateforme. Il en existerait actuellement une cinquantaine, dont les deux plus importantes sont OKCoin pour le yuan et Bitfinex pour le dollar. Dans ce cas, il doit fournir des renseignements sur son identité. Si le détenteur perd l'une de ses clés, il n'a aucun moyen de les récupérer : les bitcoins sont définitivement perdus, car il est techniquement impossible de les reproduire. Il en va de même si l'ordinateur est perdu, volé ou victime d'un piratage. Dans tous les cas, le détenteur ne peut se retourner vers aucune institution, ni faire agir une quelconque assurance. Un autre problème se pose lorsque la plateforme, gestionnaire du compte, est victime de hachage ou fait faillite. Il n'existe pas d'assurance des dépôts sur le bitcoin. Ainsi la faillite, *a priori* frauduleuse, de la plateforme MtGox, en février 2014, au Japon aurait impliqué la disparition de 850 000 bitcoins (voir, par exemple, Ali *et al.,* 2015 ou Böhme *et al.,* 2015). Moore et Christin (2013) étudient le fonctionnement de quarante plateformes entre 2010 et 2013 et montrent que dix-huit d'entre elles ont fermé, impliquant dans près de la moitié des cas des pertes irréversibles pour les déposants. En août 2016, Bitfinex a été victime d'un piratage informatique impliquant la perte de 120 000 BTC (bitcoins).

Selon Yermak (2013), les utilisateurs seraient essentiellement des férus de nouvelles technologies et des libertaires qui veulent s'affranchir de la tutelle des États. L'usage des bitcoins serait relativement concentré aux États-Unis et en Chine. Les Chinois l'utiliseraient notamment pour acheter des biens à l'étranger et envoyer des fonds aux expatriés (Collomb, 2015). Les paiements transfrontières offrent légitimement un potentiel de développement puisque les transactions en bitcoins n'impliquent pas de frais de change et permettent de contourner SWIFT et les systèmes de paiement nationaux. Pour Nakamoto (2008), l'absence d'intermédiaires réduit les coûts de transaction supportés par les utilisateurs et constitue un avantage décisif du bitcoin vis-à-vis des monnaies traditionnelles. Folkinshteyn *et al.* (2015)

estiment le coût moyen des transactions en bitcoins entre 0 % et 1 %, alors qu'une transaction bancaire classique coûterait entre 2 % et 5 %.

Si le bitcoin semble un avantage en termes de coûts, ses utilisations les plus connues actuellement posent problème. Du fait de l'anonymat des transactions, le bitcoin est considéré comme l'un des moyens de paiement privilégiés pour acquérir des biens et des services illégaux (drogue, papiers d'identité, trafic d'armes, meurtre, prostitution, etc.), mais également comme un moyen pour favoriser le financement du terrorisme, l'évasion fiscale ou le blanchiment de capitaux. Ces problèmes ont notamment été révélés lors de la fermeture du site Silk Road par les autorités américaines en octobre 2013 (voir, par exemple, Christin, 2013). Les crises chypriote et grecque ont également montré que le bitcoin permettait de contourner la réglementation sur les mouvements de capitaux. Dans le cas chypriote, en 2013, les titulaires d'un compte de dépôt supérieur à 100 000 euros, notamment les Russes, se sont rués sur le bitcoin pour éviter de participer au *bail in.* En Grèce, en juillet 2015, les transactions en bitcoins ont augmenté de 300 % pour contourner la réglementation sur les retraits bancaires. Le pic des transactions quotidiennes a été ainsi enregistré la semaine du 6 juillet 2015, à la suite du résultat du référendum grec, selon les statistiques de coindesk.com. Des pays à forte inflation, tels que l'Argentine et le Venezuela, qui appliquent des réglementations strictes sur les achats de dollars ont également un pourcentage d'utilisateurs important. Le bitcoin peut ainsi apparaître comme une valeur refuge au point d'en faire une sorte d'or numérique. De nombreux États mettent cependant en garde contre les dangers liés à l'utilisation des monnaies virtuelles. C'est le cas de la France (ACPR, 2014) ou de la Chine. Pour la Banque centrale européenne (BCE, 2015), le bitcoin n'est pas de la monnaie d'un point de vue légal et elle n'envisage pas, pour l'instant, de le réguler. Des pays tels que l'Allemagne le considère comme une monnaie privée, ce qui permet de fiscaliser les transactions. Les États-Unis et le Japon le considèrent comme une marchandise afin de fiscaliser les plus-values.

Les attributs monétaires du bitcoin

L'analyse économique considère qu'une monnaie remplit trois fonctions simultanément : moyen de paiement, unité de compte et réserve de valeurs. La première fonction est considérée comme essentielle car elle conditionne les deux suivantes.

En tant que moyen de paiement, le bitcoin est actuellement utilisé par environ 100 000 sites marchands dont Dell, Expedia, Microsoft ou PayPal. Barclays envisage, comme test, d'accepter des bitcoins lors de dons à des œuvres de charité. Le périmètre d'acceptabilité reste, pour l'instant, faible. Même si le nombre total de sites marchands au niveau

mondial reste incertain (Netcraft recense, en juillet 2015, plus de 178 millions de sites actifs, mais pas uniquement marchands), l'utilisation actuelle du bitcoin peut se résumer au travers de quelques chiffres. L'e-commerce mondial en 2013 s'élève à 1 173 Md€. Selon les statistiques de la Federal Reserve américaine (Fed, 2015), le volume quotidien des transactions totales en bitcoins serait inférieur à 80 millions, alors que les transactions en dollar scriptural seraient supérieures à 122,4 milliards en 2012. Holden (2015) estime qu'il y aurait 1,3 million d'utilisateurs du bitcoin en 2014 et, potentiellement, 4,7 millions en 2019. L'augmentation du volume des transactions en bitcoins ne serait pas tant le fait d'un panel plus large d'adoptants qu'une intensification des transactions entre utilisateurs habituels. Yermak (2013) recense 70 000 transactions journalières en bitcoins dont 80 % seraient purement spéculatives. Segendorf (2014) estime que les transactions en bitcoins représentent 0,01 % des transactions quotidiennes par cartes bancaires. Le nombre d'utilisateurs et le volume des transactions semblent, pour l'instant, très modestes.

La vitesse de circulation du bitcoin est faible. Seuls 4 % des bitcoins en circulation seraient hebdomadairement utilisés, 24 % dans les trois mois et 50 % dans les six mois. Plus du tiers serait conservé par leurs détenteurs au-delà de l'année. Au total, le bitcoin serait peu utilisé pour des transactions sur biens et services. Son utilisation spéculative peut s'expliquer par l'absence de taux d'intérêt sur cette monnaie. Les gains issus de sa détention ne peuvent alors provenir que des variations de prix qui peuvent être très fortes (cf. *infra*). La rapidité des transactions peut également poser problème. Dans une transaction en monnaie scripturale « classique », l'intermédiaire bancaire permet de garantir au vendeur le règlement réalisé par l'acheteur. Dans une opération en bitcoins, aucun intermédiaire ne peut assumer ce rôle puisqu'elle a lieu dans un réseau de pair à pair, toute transaction étant enregistrée dans la chaîne de blocs. En contrepartie, la vitesse de réalisation des opérations est faible comparée à celle des moyens de paiement scripturaux traditionnels. En effet, la taille d'un bloc est limitée à 1 million d'octets, ce qui implique qu'au plus sept transactions par seconde peuvent avoir lieu. Ce nombre est extrêmement faible comparé, par exemple, au réseau Visa qui traite, en moyenne, 2 000 transactions par seconde et peut monter jusqu'à 4 000. Le tableau (*infra*) recense les transactions en bitcoins du 15 avril 2016 et indique que seulement 2,57 transactions par seconde ont eu lieu en moyenne. Et les transactions sont, pour l'essentiel, irrévocables car il est extrêmement complexe d'annuler une opération une fois qu'elle a été enregistrée dans la chaîne.

Une difficulté supplémentaire d'utilisation tient à la forme des prix qui est peu intuitive. Par exemple, le 15 avril 2016, 1 BTC vaut environ

378 euros, ce qui implique qu'un bien à 1 euro vaut 0,002 645 5 BTC. Le bitcoin est bien divisible, mais son offre étant fortement inélastique, les prix des biens et des services sont affichés avec de nombreux chiffres après la virgule, ce qui ne facilite pas sa diffusion en tant qu'unité de compte. Il n'est finalement pas accepté directement comme moyen de paiement. En effet, les sites fixent d'abord les prix en monnaies traditionnelles (dollar, euro, etc.), puis les convertissent en bitcoins au taux de change courant. Il ne sert donc pas d'unité de compte.

Tableau
Statistiques des transactions en bitcoins (15 avril 2016)

Nombre de blocs	156
Nombre moyen de blocs/heure	6
Temps moyen pour miner un bloc	9 min 13 s
Nombre moyen de transactions/heure	9 255
Nombre moyen de transactions/seconde	2,57

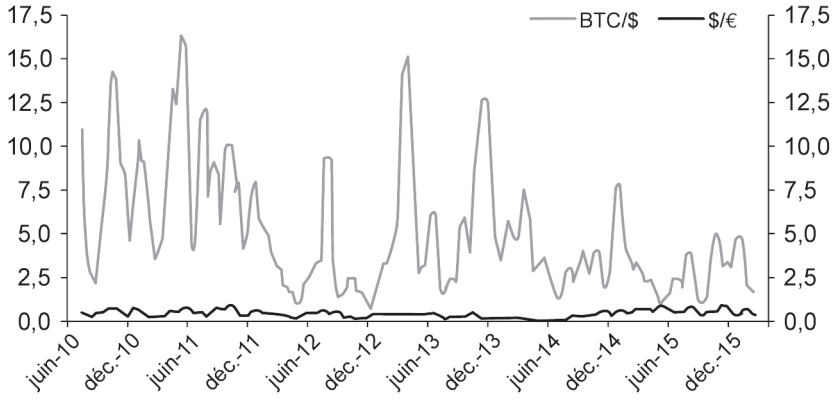
Source : www.coindesk.com/data/bitcoin/.

L'acceptabilité limitée du bitcoin découle de l'absence de cours légal et de sa forte volatilité vis-à-vis des principales devises (cf. graphique *infra*). Comme le rappelle la Banque de France (2013), le « bitcoin n'est adossé à aucune activité réelle et/ou actifs sous-jacents ». Aucune banque centrale ne régule les conditions de l'offre et de la demande au travers de la politique monétaire. Les 3 500 BTC créés quotidiennement par l'activité de minage le sont indépendamment des conditions de l'offre et de la demande. La logique purement mathématique de création manque intrinsèquement de fondements économiques et financiers. Il peut y avoir trop de bitcoins en circulation quand le cours chute et pas assez quand le cours monte, d'où une forte volatilité. Si le protocole cryptographique est inattaquable, l'offre de bitcoins ne peut être certes manipulée, ce qui éviterait toute illusion monétaire du fait de l'absence de biais inflationniste. Pour autant, rien ne garantit que le taux de croissance de l'offre soit économiquement optimal au sens de Friedman (1960). L'offre de bitcoins est totalement indépendante des évolutions économiques. L'absence d'un prêteur en dernier ressort pourrait alors être préjudiciable à la stabilité économique. La crise a rappelé l'utilité de cette fonction pour gérer les crises bancaires (FMI, 2016).

Le cours du bitcoin est complexe à déterminer car il est « déterritorialisé ». Il n'est donc la contrepartie d'aucune base monétaire nationale ou régionale. Cette absence de lien va donc au-delà des propositions de l'école autrichienne qui, si elle défendait l'idée que la monnaie légale ne soit pas émise par l'État, proposait une monnaie rattachée à l'or pour assurer sa stabilité. Une étude économétrique de Ciaian *et al.* (2014) confirme que les déterminants traditionnels des taux de change ne sont

pas significatifs et que des comportements spéculatifs, liés à des rumeurs, peuvent affecter son prix. Depuis son apparition, le bitcoin a été victime de nombreux *flash crashes.* Le plus spectaculaire a eu lieu le 10 avril 2013, lorsqu'il a perdu 61 % de sa valeur en dollars, du fait de l'incertitude sur les conditions du règlement de la crise chypriote.

Graphique
Volatilité BTC/$ et $/€



Source : www.coindesk.com/data/bitcoin/.

Une fonction importante de la monnaie est de permettre aux agents de réaliser des transactions financières. Ceux-ci ont accès à des supports d'épargne, au marché du crédit, à des marchés financiers. Les systèmes bancaires fonctionnent sur le principe de réserves fractionnaires, ce qui permet de créer de la monnaie. L'environnement monétaire proposé par le bitcoin est radicalement différent : pas de réserves fractionnaires, donc pas de marché du crédit, ni de taux d'intérêt. Chaque bitcoin étant unique, aucune duplication n'est possible. Cet environnement explique que les gains proviennent aujourd'hui uniquement des variations de prix. D'où la présence de comportements spéculatifs de la part des détenteurs de bitcoins, conformément à la loi de Gresham.

La volatilité du bitcoin vis-à-vis du dollar est sans commune mesure avec celle du dollar vis-à-vis de l'euro. Cette forte volatilité explique pourquoi le bitcoin n'est pas actuellement utilisé en tant qu'unité de compte car les marchands seraient obligés de calculer en permanence les prix, ce qui impliquerait des coûts de mise à jour significatifs (Lo et Wang, 2014). La variabilité permanente des prix induirait également de l'incertitude pour le consommateur qui est habitué à des prix relativement fixes. La forte volatilité du bitcoin le rend, pour l'instant, incapable de préserver la valeur. Le pouvoir d'achat du bitcoin est donc

fortement instable. Ses variations peuvent exposer ses détenteurs à des pertes ou à des gains spectaculaires. Le bitcoin ne peut être considéré comme un actif parfaitement sûr et liquide.

Le bitcoin ne peut donc être considéré comme une monnaie. Son acceptabilité en tant que moyen de paiement est limitée, sa volatilité est forte pour servir de réserve de valeurs et il n'est pas utilisé comme unité de compte. Cependant le protocole cryptographique sous-jacent semble offrir de nombreuses opportunités dans le domaine de l'authentification des transactions.

La chaîne de blocs et la finance

L'utilisation de la chaîne de blocs ne se réduit pas aux transactions en bitcoins.

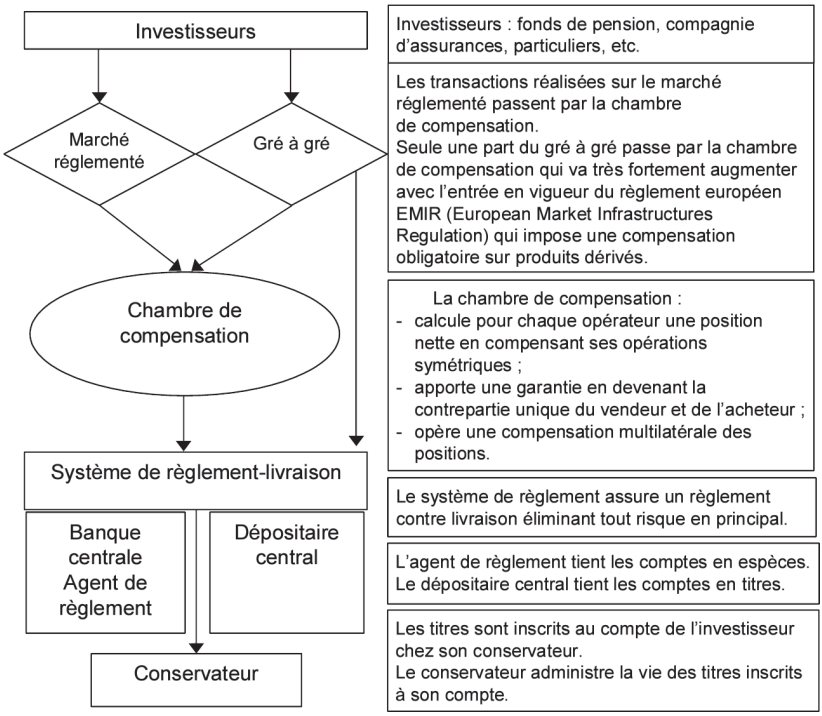
De nombreux domaines pourraient être impactés par cette technologie : l'éducation (certification des diplômes), les actes civils (mariage, divorce, décès, vote, cadastre, etc.), la culture (gestion des droits d'auteurs), la santé (la sécurité sociale envisagerait de tester une chaîne avec les professionnels du secteur), le marché de l'assurance, etc. En cas de généralisation, la persistance des tiers de confiance (banques, avocats, notaires, intermédiaires, etc.) se poserait, puisque la chaîne de consensus permettrait une rencontre directe des contreparties et faciliterait l'exécution de contrats intelligents (*smart contracts* ; Szabo, 1994).

Vers une décentralisation des transactions financières ?

L'un des domaines où l'instauration de chaînes de consensus est l'objet d'une attention particulière est la sphère financière. Par exemple, l'organisation de la gouvernance d'entreprise (Yermak, 2015), des systèmes de paiement (FMI, 2016) ou des marchés financiers (Lee, 2015) pourrait sensiblement évoluer. La chaîne de blocs pourrait favoriser le développement des micropaiements dont le coût est trop élevé pour être rentable, mais aussi des paiements internationaux dont le traitement est encore long et coûteux. Ainsi les transactions de change pourraient être réglées sans passer par le système de *correspondent banking* qui impacte les coûts et les délais. Les opérations de *trade finance* bénéficieraient d'une simplification des étapes et des procédures de vérification permettant aux entreprises d'y recourir plus spontanément. C'est également le cas des opérations sur titres qui se déroule en trois phases (cf. schéma 2 *infra*) : la négociation, la compensation et le règlement-livraison. Les deux dernières étapes nécessitent l'intervention de plusieurs structures intermédiaires qui enregistrent les opérations, calculent les positions et vérifient la bonne fin des transactions. L'actuel processus postmarché prend au moins deux

jours, parfois plus, notamment pour les transactions internationales, et se révèle coûteux et risqué pour les contreparties. La chambre de compensation, les systèmes de règlement-livraison et de paiement, le conservateur doivent être réglementés et surveillés par les régulateurs. La chaîne de blocs est un vecteur d'instantanéité. La mise en place d'un registre dupliqué et partagé entre investisseurs et certificateurs pourrait simplifier le *reporting,* assurer la traçabilité des transactions, raccourcir les délais, abaisser les coûts des opérations postmarché et les risques de contrepartie. Sur les marchés OTC, les transactions jusqu'ici opaques deviendraient spontanément transparentes et consultables par tous. Et, à la différence d'un marché financier standard, la chaîne de blocs pourrait fonctionner 24 heures/24, 7 jours/7.

Schéma 2
Chaîne de traitement des titres, cas d'un achat de titres



Source : Banque de France (2015).

On peut également envisager que les votes aux assemblées générales, le versement des dividendes et des coupons puissent transiter par la chaîne de blocs. La technologie implique alors une banalisation des agents financiers qui ne sont plus des intermédiaires incontournables des opérations financières.

Les risques

Au-delà des bénéfices escomptés de l'utilisation des chaînes de blocs aux transactions financières, un certain nombre d'obstacles, notamment techniques et juridiques, demeurent en suspens.

Les plus évidents sont les risques opérationnels. Premièrement, un risque de blocage des transactions peut survenir. Dans sa configuration actuelle, le nombre de transactions que peut valider la chaîne de blocs est limité à sept par seconde (voir précédemment). Cela ne pose pas de problème sur un marché étroit comme celui du bitcoin. En revanche, cette caractéristique technique est incompatible avec les marchés financiers où les effets d'engorgement pourraient conduire à un blocage. Des solutions sont actuellement testées pour permettre à la chaîne de traiter les volumes des marchés financiers. Deuxièmement, dans le cas des échanges de bitcoins, le risque de piratage de la chaîne n'est pas rentable car les valeurs en jeu ne sont pas suffisantes (voir *infra*). La situation pourrait être différente pour les opérations financières. Par exemple, les transactions quotidiennes de change sont supérieures à 5 000 Md$ et pourraient inciter des mineurs à réécrire la chaîne pour capter frauduleusement tout ou partie des flux.

Le statut des mineurs pourrait poser problème s'ils opéraient sur les marchés financiers. Aujourd'hui, la seule barrière à l'entrée dans la chaîne est la puissance de calcul. Aucune réglementation, ni aucune surveillance ne leur sont imposées, comme c'est le cas pour les intermédiaires financiers. Dès lors, rien ne garantit que les mineurs inspirent aux investisseurs le même niveau de confiance que les intermédiaires financiers dans le règlement des transactions. La gouvernance de la chaîne doit être également un sujet de préoccupation. Actuellement, elle n'a, comme Internet, ni propriétaire, ni autorité de régulation, puisque le principe fondateur de la chaîne de blocs est : « *Code is law.* » Mais, comme l'indique le Committee on Payments and Market Infrastructures (CPMI, 2015), « l'organisation décentralisée, son ouverture et sa gouvernance flexible impliquent que les problèmes futurs peuvent ne pas être correctement anticipés ». Le règlement des conflits est un problème central en l'absence d'une autorité de régulation, de lois et de juridiction. Comment et à quel coût un investisseur lésé pourrait-il faire valoir ses droits dans un environnement décentralisé sans tiers de confiance ? Une solution, actuellement testée par des établissements financiers (projet R3), consiste à mettre en place leur propre chaîne de blocs. Les mineurs sont alors préalablement agréés. La validation des transactions est du ressort d'un ensemble présélectionné de nœuds et non de la totalité des certificateurs, ce qui doit contribuer à une plus grande fluidité des transactions par rapport à une chaîne de

blocs publique. La chaîne peut être totalement privée : seuls les membres agréés peuvent y réaliser des transactions pour leur propre compte et/ou pour celui de tiers. Elle peut être semi-privée si les opérations peuvent être commencées par n'importe quel agent, mais certifiées par les membres agréés. On peut envisager l'existence de chaînes de place et/ou de chaînes dédiées à des transactions spécifiques. Si un tel environnement émerge, les régulateurs devront surveiller la véracité des chaînes. Selon Santander InnoVentures (2015), la généralisation des chaînes permettrait aux banques d'économiser jusqu'à 20 Md$. Se poserait alors la question du partage de cette économie avec les utilisateurs finals.

CONCLUSION

Le bitcoin ne peut pas être considéré comme une monnaie : l'absence de valeur intrinsèque et de cours légal se traduit par une forte volatilité de son prix qui ne lui permet pas de remplir les fonctions monétaires traditionnelles. En revanche, la chaîne de blocs offre des opportunités de modifier les pratiques centralisées et intermédiées des marchés financiers. Cette possible évolution s'accompagnera de l'émergence de risques opérationnels et juridiques que les régulateurs devront évaluer et surveiller.

BIBLIOGRAPHIE

ACPR (Autorité de contrôle prudentiel et de résolution) (2014), « Position de l'ACPR relatives aux opérations sur Bitcoins en France », Position 2014-P-01, 29 janvier, http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201401-Position-2014-P-01-de-l-ACPR.pdf.

Ali S. T., Clarke D. et McCorry P. (2015), « Bitcoin: Perils of an Unregulated Global P2P Currency », Newcastle University, *Technical Report Series,* nº 1470.

Banque de France (2013), « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus,* nº 10, décembre.

Banque de France (2015), « Les infrastructures des marchés financiers traitant les titres », www.banque-france.fr/stabilite-financiere/infrastructures-des-marches-financiers-et-moyens-de-paiement-scripturaux/infrastructures-des-marches-financiers/traitantlestitres.html.

Baumol W., Panzar J. et Willig R. (1982), *Contestable Markets and the Theory of Industry Structure,* Harcourt Brace Jovanovich.

BCE (Banque centrale européenne) (2015), *Virtual Currency Schemes. A Further Analysis*, www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

Blundell-Wignall A. (2014), « The Bitcoin Question: Currency versus Trust-less Transfer Technology », *OECD WP on Finance, Insurance and Private Pension*, nº 37.

Böhme R., Christin N., Edelman B. et Moore T. (2015), « Bitcoin: Economics, Technology and Governance », *Journal of Economic Perspectives*, vol. 29, nº 2, pp. 213-238.

Buterin V. (2015), « On Public and Private Blockchains », blog Ethereum, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

CHRISTIN N. (2013), « Traveling the Silk Road: a Measurement Analysis of a Large Anonymous Online Marketplace », *Proceedings of the 22nd International Conference on World Wide Web*, pp. 213-224.

CIAIAN P., RAJCANIOVA M. et KANCS D. (2014), « The Economics of BitCoin Price Formation », *arXiv preprint arXiv:1405.4498*, https://arxiv.org/ftp/arxiv/papers/1405/1405.4498.pdf.

COLLOMB A. (2015), « Les nouvelles formes numériques du *shadow banking*: du *crowdfunding* au bitcoin », in Mellios C. et Pluchart J.-J. (éd.), *Le Shadow banking*, Eyrolles, pp. 79-98.

CPMI (Committee on Payments and Market Infrastructures) (2015), « Digital Currencies », Banque des règlements internationaux, novembre, www.bis.org/cpmi/publ/d137.pdf.

DUPRÉ D., PONSOT J.-F. et SERVET J-M. (2015), « Le bitcoin contre la révolution des communs », 5e congrès de l'AFEP, Lyon.

DWYER G. (2014), « The Economics of Bitcoin and Similar Private Digital Currencies », *MPRA Paper*, nº 57360.

EBA (2014), « EBA Opinion on 'virtual currenies' », *EBA/Op/2014/08.*

FED (Federal Reserve) (2015), *Strategies for Improving the US Payment System*, 26 janvier.

FMI (Fonds monétaire international) (2016), « Virual Currencies and Beyond: Initial Considerations », *Staff Discussion Note*, nº 3.

FOLKINSHTEYN D., LENNON M. et REILLY T. (2015), « A Tale of Twin Tech: Bitcoin and the WWW », *Journal of Strategic and International Studies*, vol. 10, novembre, www.researchgate.net/publication/275969675_A_TALE_OF_TWIN_TECH_BITCOIN_AND_THE_WWW.

FRIEDMAN M. (1960), *A Program for Monetary Stability*, Fordham University Press.

GAILLY P. A. (2015), *Nouvelles monnaies : les enjeux macroéconomiques, financiers et sociétaux*, Les Avis du Conseil économique, social et environnemental, avril, www.lecese.fr/sites/default/files/pdf/Avis/2015/2015_10__nouvelles_monnaies.pdf.

HAYEK F. (1976), *Denationalisation of Money: the Argument Refined*, Ludwig von Mises Institute.

HICKS J. (1967), *Critical Essays in Monetary Theory*, Oxford University Press.

HOLDEN W. (2015), *The Future of Cryptocurrency: Bitcoin Altcoin. Impact Opportunities 2015-2019*, Juniper.

LEE L. (2015), « New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market », *S. J. Quinney College of Law Research Paper*, nº 138.

LO S. et WANG C. (2014), « Bitcoin as Money », Federal Reserve Bank of Boston, *Currency Policy Perspectives*, nº 2014-4, www.bostonfed.org/publications/current-policy-perspectives/2014/bitcoin-as-money.aspx.

MISHKIN F. (2004), *The Economics of Money and Financial Markets*, Pearson, 7e edition.

MOORE T. and CHRISTIN N. (2013), « Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk », in *Financial Cryptography and Data Security*, Springer, pp. 25-33.

NAKAMOTO S. (2008), « Bitcoin: a Peer-to-Peer Electronic Cash System », *Consulted*, nº 1, p. 28.

NARAYANAN A., BONNEAU J., FELTEN E., MILLER A. et GOLDFEDER S. (2016), *Bitcoin and Cryptocurrency Technologies*, Princeton University Press.

ORLÉAN A. (2004), *Analyse économique des conventions*, PUF, coll. Quadrige, 2e édition.

SANTANDER INNOVENTURES (2015), *The Fintech 2.0 Paper: Rebooting Financial Services.*

SEGENDORF (2014), « What is Bitcoin? », *Sveriges Riskbank Economic Review*, vol. 2, pp. 71-87.

SELGIN G. (2013), « Synthetic Commodity Money », university of Georgia, *Working Paper*.

SZABO N. (1994), *Smart Contracts*, manuscrit non publié, http://szabo.best.vwh.net/smart.contracts.html.

VELDE R. F. (2015), « Bitcoin pour remplacer les devises ? », *Revue d'économie financière*, nº 120, pp. 105-112.

YERMAK D. (2013), « Is Bitcoin a Real Currency? An Economic Appraisal », National Bureau of Economic Research, *Working Paper*, nº 19747.

YERMAK D. (2015), « Corporate Governance and Blockchains », National Bureau of Economic Research, *Working Paper*, nº 21802.