Conférence *Inside Bitcoin* à New York.

La chaîne de **confiance**

Inventée pour éviter les banques, la technologie de la chaîne de blocs, ou *blockchain*, de bitcoin pourrait finalement leur rendre service

Andreas Adriano et Hunter Monroe

LE PLUS gros avantage des espèces réside dans la simplicité des transactions, qui se résument à des échanges en main propre. Nul besoin de fournir son nom, ses coordonnées, sa date de naissance, son numéro de sécurité sociale, ou son bulletin de salaire. Le liquide génère une relation de confiance instantanée.

La circulation de gros montants en espèces étant tout sauf pratique, des systèmes de paiement papier, puis électroniques, ont été créés. Toutefois, sans espèces, il est compliqué et onéreux d'instaurer la confiance. Pour obtenir une carte de crédit ou de débit, le demandeur doit répondre à un long questionnaire, et la banque émettrice doit vérifier ses réponses et son crédit. L'utilisation de la carte requiert ensuite une infrastructure complexe assurant la rapidité, la fiabilité et la sécurité des transactions, sans compter que le commerçant cède un pourcentage sur chaque vente.

Les virements interbancaires nationaux sont régis par les systèmes opérés relevant des banques centrales, tandis que les virements internationaux impliquent parfois d'autres banques commerciales. De plus, ces transactions peuvent prendre plusieurs jours. De même, alors que l'on associe les opérations électroniques boursières à l'instantanéité, le règlement des transactions peut prendre deux à trois jours et impliquer des conservateurs intermédiaires, des notaires, des chambres de compensation et autres dépositaires centraux de titres. Avant le règlement, les institutions financières doivent réserver d'importants volumes de liquidités ou d'autres actifs liquides pour couvrir leurs positions en cas de défaut de paiement.

Plus simple et moins cher

La technologie peut-elle rendre les choses aussi simples et bon marché qu'avant? Oui, grâce à bitcoin, la monnaie numérique dont certains prédisent qu'elle va sonner le glas des banques, mais que d'autres considèrent comme un système de Ponzi et une arme financière pour les criminels. Bitcoin, ou plus précisément la technologie sous-jacente des «registres distribués», ou de la «chaîne de blocs», pourrait engendrer un reformatage complet de la finance (encadré 1).

L'histoire de bitcoin débute lorsque Satoshi Nakamoto — pseudonyme de son inventeur inconnu — envoie un article et un logiciel sur

une liste de diffusion d'activistes, les «cypherpunks», convaincus de l'impact social et politique de la cryptographie. Le concept est très vite décliné en ligne. Partie d'un taux de change de 0,0007 dollar pour un bitcoin en 2009, la monnaie numérique atteint la parité en février 2011, avant de culminer à 1.242 dollars en novembre 2013. En 2016, elle flotte au-dessus des 400 dollars. La valeur des bitcoins en circulation dans le monde équivaut à environ 6 milliards de dollars (contre environ 1.500 milliards pour le billet vert).

Bitcoin a d'abord séduit les libertaires désireux d'effacer ou, *a minima,* de contourner les banques et banques centrales. Alors que la flambée du cours a donné lieu à une ruée vers l'or bis, le relatif anonymat et la facilité des transactions ont attiré les trafiquants de drogue et d'autres criminels. En 2013 et 2014, de grandes opérations de répression ont envoyé quelques entrepreneurs de la première heure derrière les barreaux, ternissant au passage la réputation de l'initiative.

Les entrepreneurs technologiques et le secteur financier ont vite identifié le tigre sous le capot : la technologie des registres distribués, qui vérifie et enregistre les transactions de pair à pair, sans autorité centrale. Elle chamboule le principe élémentaire de la validation de l'ensemble des transactions par un comptable central, indépendant et fiable, souvent une banque centrale (voir graphique).

Avec bitcoin, tous les internautes peuvent valider et enregistrer des transactions avec leur propre copie du registre. Ils regroupent les transactions d'une période donnée dans un bloc, suivi d'un cachet infalsifiable. Chaque bloc est lié au précédent, d'où la notion de «chaîne». La finalisation du bloc requiert un travail informatique, travail pour lequel des «mineurs» concurrents sont rémunérés en bitcoins. En combinant approche pair-à-pair et sécurité cryptographique, le bitcoin est ainsi devenu la première monnaie numérique à s'imposer, après plusieurs décennies d'échecs.

Encadré 1

Vous avez reçu un paiement

Plusieurs startups assurent déjà des services de paiement et d'envoi de fonds bon marché en remplaçant les devises par les bitcoins. Au lieu de facturer 8 % pour un envoi de fonds, Circle Internet Financial le fait gratuitement. Son appli convivial incorpore des fonctionnalités façon réseaux sociaux telles que les images et les émoticônes, séduisant une clientèle jeune biberonnée aux smileys.

Une fois leur profil associé à un compte bancaire ou à une carte, les utilisateurs se «textent» de l'argent aux quatre coins de la planète. Les transactions passent par bitcoin, mais peu importe le processus. Si le bénéficiaire n'est pas sur bitcoin, l'argent peut être retiré avec des «portefeuilles numériques» (applis de stockage de bitcoins ou d'autres monnaies) ou, moyennant une modique commission, aux guichets de sociétés de transferts de fonds utilisant bitcoin.

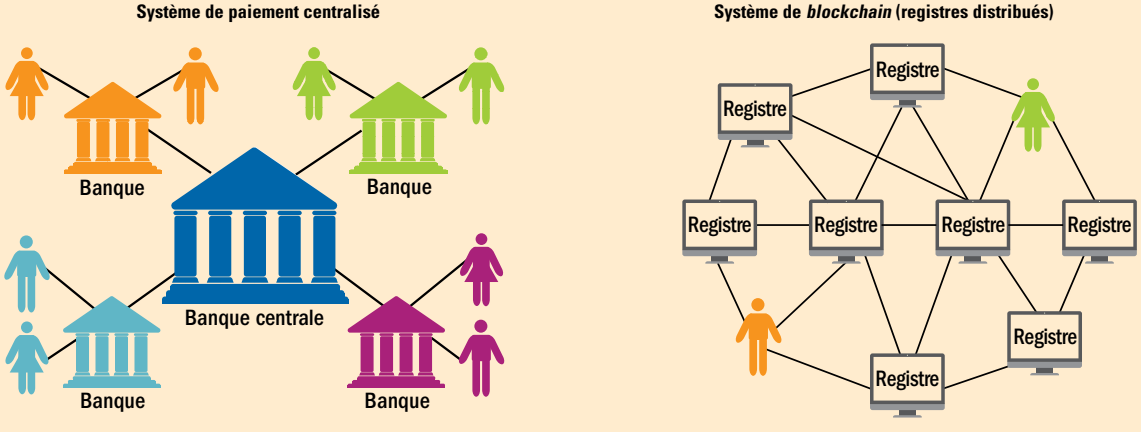
«C'est comme envoyer un e-mail», explique le PDG de Circle, Jeremy Allaire. «On se moque de la façon dont le message est acheminé.» Et d'expliquer comment sa nounou philippine, qui en était de 50 dollars par envoi de fonds au pays, a vu cette commission passer à 0,75 dollar. Et encore, parce que sa famille n'utilise pas Circle. Les transactions étant très rapides, la volatilité du bitcoin ne pose pas problème.

Circle combine l'attrait du numérique avec quelques caractéristiques rassurantes. L'entreprise est enregistrée en tant que prestataire de services monétaires, ce qui lui permet de fournir de nombreux services bancaires, sauf les prêts ou les investissements avec l'argent des clients. Elle bénéficie également d'une garantie des dépôts du gouvernement américain. Après avoir récemment obtenu une licence au Royaume-Uni, elle a formé un partenariat avec Barclays Bank.

À l'instar de nombreux patrons de startups aux prémices de l'Internet, Allaire, dont les caisses sont bien alimentées par des capital-risqueurs, ne se soucie pas de la rentabilité à court terme. «Notre activité consiste à pénétrer un marché qui rapporte des milliers de milliards de dollars aux banques de détail. Il y a des parts de marché colossales à ébranler ou à s'accaparer avec des produits bancaires numériques», estime-t-il. N'a-t-on pas vu, au début des années 2000, de nombreuses entreprises échouer en se focalisant trop sur la conquête de clients et en négligeant de les rentabiliser? «Les grandes entreprises web ont toutes commencé par s'atteler sans relâche à fournir un service gratuit qui a apporté une grande plus-value aux consommateurs. Elles ont continué pendant des années jusqu'à atteindre une ampleur significative.»

Décentralisation

Dans le système bancaire traditionnel, la banque centrale trace les paiements entre clients. Avec la technologie de la *blockchain,* les transactions sont enregistrées sur un réseau d'ordinateurs et validées par de nombreux individus.



Quelle est l'ampleur du phénomène? «Bitcoin offre la possibilité inédite à un internaute de transférer un élément de propriété numérique à un autre internaute de manière à ce que l'opération soit garantie sûre et protégée, que les deux parties sachent que le transfert a bien eu lieu, et que personne ne puisse contester sa légitimité. Les implications de cette nouveauté sont énormes», estimait l'entrepreneur américain Marc Andreessen dans le *New York Times* en janvier 2014.

Ce pionnier d'Internet a inventé le premier navigateur largement utilisé et a fondé Netscape en 1993, alors qu'il était encore étudiant. Il est aujourd'hui à la tête d'Andreessen Horowitz, l'un des fonds de capital-risque les plus influents de la Silicon Valley. Les capital-risqueurs gagnent de l'argent en dégotant les grandes nouveautés au stade embryonnaire. Andreessen et nombre de ses homologues qui ont financé les créateurs du web actuel misent désormais sur bitcoin et sa *blockchain*. Ils y voient une innovation capable d'instaurer, entre deux inconnus qui ne se voient pas, la même confiance que la monnaie fiduciaire. Pour certains, cette capacité à éluder les tiers de confiance en fera l'invention la plus révolutionnaire depuis Internet, à savoir une technologie de rupture qui bouleverse, voire détruit, les modèles traditionnels. L'Amazon des librairies ou l'Uber des taxis. Le chamboulement de l'industrie financière, secteur le plus cadenassé de la planète, constitue un tout autre défi. Au vu des nombreux défauts du système, cette entreprise est possible, et même souhaitable, comme Martin Wolf l'a écrit dans le *Financial Times,* mais très compliquée à tous les niveaux : juridique, financier et opérationnel.

Depuis toujours, l'industrie financière cherche à résoudre le problème de la confiance en jouant le rôle d'intermédiaire fiable entre des individus et des entreprises qui ne se connaissent pas. Quant aux banques centrales et aux régulateurs, ils étayent cette confiance grâce à leur supervision et à la garantie des dépôts. Les banques sont payées pour effectuer les transactions par cartes ou virements, par exemple, car les banques et la banque centrale se reconnaissent en tant qu'homologues dignes de confiance. Cette activité est très rémunératrice : selon McKinsey&Company, les services de paiement internationaux rapportent aux banques la somme colossale de 1.700 milliards de dollars par an, soit 40 % de leur chiffre d'affaires. Plus étonnant : malgré l'innovation technologique, le coût de l'intermédiation financière aux États-Unis n'a pas beaucoup évolué depuis le début du XX^{e} siècle, selon une étude citée par l'économiste en chef de la Banque d'Angleterre, Andrew Haldane. Dans un rapport de 2012, la Banque centrale européenne (BCE) estimait qu'hormis les commissions que nous payons tous, les coûts indirects représentent 1 % du PIB, soit 130 millions d'euros par an pour la seule Union européenne. Le coût de l'envoi de fonds à l'étranger est encore plus élevé : près de 8 % selon la Banque mondiale. Pourtant, certaines startups, la plupart utilisant bitcoin, rendent cette opération aussi simple et peu coûteuse que l'envoi d'un e-mail (encadré 2).

Transformation du secteur financier

Selon ses partisans, la technologie de bitcoin peut transformer fondamentalement le secteur financier, en raccourcissant, par exemple, le délai de règlement des opérations sur titres. Cette accélération réduit le volume de fonds à mettre de côté pour couvrir les risques de crédit et de règlement, de la même façon qu'une transaction en espèces ne requiert aucune garantie.

La liste des utilisations potentielles est plus longue encore. Pensez aux titres immobiliers — les acquéreurs américains s'assurent généralement contre des requêtes inattendues sur le titre qu'ils achètent — ou au processus d'achat, d'enregistrement et de paiement de taxes pour une voiture. Une chaîne de blocs pourrait délivrer un justificatif de propriété numérique infalsifiable ainsi qu'un historique de possession complet. Les contrats intelligents à exécution automatique font également fantasmer. Imaginez une assurance voyage qui vous rembourse

Encadré 2

Questions fréquentes sur bitcoin

Q : Le bitcoin est-il la seule monnaie numérique?

R : Non, il existe plus de 700 «crypto-monnaies». Le bitcoin est la plus connue, celle qui possède la plus forte valeur, la meilleure liquidité et la plus large acceptation. Il devance largement l'ether.

Q : Les crypto-monnaies sont-elles sécurisées?

R : Des piratages, des vols et même de faillites de bureaux de change ou de fournisseurs de portefeuilles numériques ont été recensés, mais ils sont de moins en moins fréquents.

Q : Sont-elles volatiles?

R : Très volatiles. Le bitcoin flotte au-dessus des 400 dollars depuis le début de l'année, il s'échangeait pour moins de 300 dollars en mai 2015, mais a dépassé les 1.200 dollars en 2013.

Q : Est-ce un bon investissement?

R : Un investissement hautement spéculatif, car il n'y a ni garantie d'une banque centrale, ni soutien par un gouvernement. L'investisseur est livré à lui-même.

Q : Est-ce un bon système de paiement?

R : Cela revient moins cher que les envois de fonds et virements traditionnels, et peut se révéler très pratique, notamment pour les paiements par smartphone. Les transactions étant rapides, la volatilité ne pose pas problème.

Q : Comment les achète-t-on?

R : De nombreux bureaux de change tels que Coinbase, Localbitcoins et CoinDesk vendent et achètent des bitcoins. Il existe aussi de plus en plus de distributeurs automatiques qui convertissent des devises traditionnelles en bitcoins.

Q : Comment les stocker?

R : Le plus pratique est de télécharger un portefeuille numérique sur un smartphone, bien adapté aux petits achats. Le stockage de gros montants est plus complexe. Certains disposent d'un ordinateur dédié hors ligne et ont recours au cryptage et à des mots de passe très robustes.

Q : Où les utiliser?

R : L'acceptation est limitée mais en progression. Quelques commerçants en ligne ainsi que certains magasins acceptent les bitcoins.

«Dans les technologies actuelles, rien n'empêche le règlement instantané.»

automatiquement en cas d'annulation de vol, ou encore un prêt auto qui neutralise l'allumage du véhicule en cas de non-paiement. La technologie de la *blockchain* alimente également une alternative à bitcoin appelée ether (dont la monnaie vaut environ 800 millions de dollars), qui attire l'attention du grand public ces derniers temps. Contrairement à bitcoin, son créateur est connu. Il s'agit de Vitalik Buterin, Russo-canadien de 22 ans ayant quitté l'université.

Vice-président des technologies de *blockchains* chez IBM, Jerry Cuomo identifie des applications potentielles de chaînes de blocs privées à usage spécifique pour améliorer la transparence par le biais de la conformité et du contrôle. À l'opposé du secret et de l'anonymat liés à bitcoin. «Bitcoin a décidé d'être anonyme par nature», indique-t-il. Toutefois, «il est parfaitement possible de créer une chaîne de blocs avec différents niveaux d'accès, sur laquelle les participants ne voient pas les actions des autres, mais où les contrôleurs et les régulateurs sont omniscients, à un niveau supérieur».

Si les expérimentations sur les *blockchains* sont surtout le fait des startups, IBM fait partie des quelques mastodontes à tâter le terrain. En décembre dernier, il a rejoint la Linux Foundation pour diffuser la technologie avec un logiciel *open source* (ouvert aux programmeurs, contrairement aux systèmes propriétaires comme Windows). De grandes banques telles que JPMorgan Chase & Co. et des entreprises technologiques comme Cisco et Intel collaborent à cette initiative. En février, la bourse de Tokyo s'est associée à IBM pour tester les *blockchains* dans l'enregistrement des opérations sur les marchés de petites transactions, et la bourse australienne a demandé à la startup Digital Asset Holdings d'appliquer la technologie des registres distribués aux opérations de compensation et de règlement. Un consortium de 42 banques internationales travaille avec un nouveau venu, R3, pour développer des technologies standardisées de registres distribués.

Il sera en effet capital de définir des normes. Tout nouveau cycle d'innovation voit différents acteurs appliquer autant de méthodes différentes, engendrant une véritable mosaïque d'approches technologiques. Certains s'inquiètent de voir partir en fumée des années d'efforts destinés à intégrer l'industrie financière mondiale. Dans le cadre de l'initiative *Single Euro Payments Area* (SEPA), les autorités ont mis douze ans, à compter de la mise en circulation de l'euro en 2002, à intégrer les plateformes technologiques et les procédures commerciales, ceci afin que les virements transfrontaliers entre les 35 pays participants soient aussi simples et peu coûteux que des opérations domestiques.

En tant que directeur général de l'infrastructure de marché et des paiements de la BCE, Marc Bayle supervise le SEPA et d'autres initiatives d'intégration continentales telles que TARGET2, le système de règlement des paiements en espèces dans la zone euro, et T2S, son pendant pour les titres. S'il suit l'évolution des *blockchains* avec intérêt, il n'est pas impressionné par certaines promesses, comme le raccourcissement des délais de règlement. «Dans les technologies actuelles, rien n'empêche le règlement instantané. Le problème vient de la structure des marchés. Si un gestionnaire de fonds à Miami veut investir à Francfort, il devra tenir compte de nombreuses contraintes juridiques, opérationnelles, fiscales et financières. Il fera peut-être appel à des intermédiaires compétents dans ces configurations transfrontalières entre les États-Unis et l'UE/l'Allemagne», explique Marc Bayle.

Utile pour les banques centrales?

Il n'exclut pas la possibilité de voir la chaîne de blocs ou une technologie de registres distribués similaire évoluer et devenir utile aux banques centrales, malgré les limitations actuelles et la tension conceptuelle entre les registres distribués et centraux. Si le remplacement des principaux systèmes de paiement de la BCE par la technologie de la *blockchain* n'est pas à l'ordre du jour, il est étudié dans certaines niches pour stimuler les opérations sur des titres plus exotiques dans les marchés secondaires. «Il faut voir si cette technologie peut contribuer à faire baisser les coûts et à renforcer les systèmes. Mais il faut aussi penser à son impact sur l'intermédiation financière, le rôle des banques et d'autres acteurs du marché, ainsi que notre capacité en tant que régulateur», ajoute Marc Bayle. Certains se demandent si bitcoin et les autres applications de la *blockchain* pourraient ébranler la politique monétaire et la stabilité financière, mais la majorité s'accorde à écarter tout risque immédiat.

Il est sûrement trop tôt pour savoir si la *blockchain* est «le nouvel Internet» ou une simple évolution. La Silicon Valley regorge de concepts surestimés qui se sont révélés irréalisables et d'entreprises révolutionnaires qui ont disparu au bout de quelques années, mais certaines ont quand même eu un certain impact. Le navigateur web Netscape d'Andreessen a été acheté par AOL en 1999 pour plus de 4 milliards de dollars. AOL, qui n'est plus que l'ombre du géant qu'il fut, a été racheté par Verizon en 2015 pour à peu près le même montant. Bitcoin ou une autre technologie de *blockchain* pourrait très bien imploser à cause d'un faille encore inconnue ou bien de l'œuvre d'un pirate du style agitateur.

La partie ne fait que commencer. Comme Bill Gates l'a un jour déclaré : «Nous surestimons toujours le changement qui aura lieu dans les deux prochaines années et sous-estimons celui qui se produira dans dix ans.» ■

Andreas Adriano est chargé de communication principal au Département de la communication du FMI. Hunter Monroe est économiste principal au Département des marchés monétaires et de capitaux du FMI.