

ÉTUDE DE DOSSIER

Cadre de direction 2020

Lancé il y a plus de dix ans en pleine crise financière, le bitcoin avait pour ambition de remplacer un système monétaire basé sur la confiance dans les banques centrales et leurs monnaies légales. Au-delà de cette 'crypto-monnaie' dont les mouvements spectaculaires -à la hausse et à la baisse- ont été largement commentés, une (r)évolution digitale est en cours dans le domaine monétaire et celui des systèmes de paiements.

À partir des documents ci-joints, vous répondrez aux questions suivantes :

1. Présentez les différents types de crypto-actifs privés et leurs caractéristiques principales.
2. Analyser les types de risques qui peuvent être liés au développement de ces crypto-actifs.
3. En mobilisant des exemples précis, analyser les raisons diverses pour lesquelles différentes juridictions réfléchissent aujourd'hui au développement de monnaies digitales de banque centrale.
4. Dresser une taxonomie des monnaies digitales de banque centrale envisagées, et leurs implications potentielles.
5. Can private digital currencies replace legal currencies? (*Réponse à rédiger en langue anglaise*)

Les questions sont indépendantes ; nous vous recommandons toutefois de les traiter dans l'ordre. Il n'est pas nécessaire de recopier l'intitulé des questions.

LISTE DES DOCUMENTS JOINTS

1. **Quand les entreprises auront leur propre monnaie** – Raphaël Bloch
www.lesechos.fr – 24/12/2019 – 2 pages
2. **Blockchain : pourquoi JP Morgan crée sa propre crypto-monnaie JPM Coin** – Delphine Cuny
www.latribune.fr – 14/02/2019 – 2 pages
3. **Les monnaies digitales sont-elles « disruptives » pour les banques centrales ?** – Laurent Clerc
www.anales.org – Réalités industrielles, Novembre 2017 – 4 pages
4. **A Chinese digital currency is the real threat, not Facebook's Libra** – Kenneth Rogoff
www.theguardian.com – 11/11/2019 – 2 pages
5. **Les crypto-monnaies** – J.-Pierre Landau – Rapport au Ministre de l'Économie et des Finances
www.vie-publique.fr – 04/07/2018 – 16 pages (extrait)
6. **Benoît Coeuré and Jacqueline Loh: Bitcoin not the answer to a cashless society**
www.bis.org – 13/03/2018 – 2 pages
7. **Michel Aglietta : « Une monnaie mondiale et privée, c'est absurde et dangereux »** – Delphine Cuny
www.latribune.fr – 17/07/2019 – 2 pages
8. **Les dimensions technologiques et socio-politiques des crypto-monnaies** – Bruno Biais
www.tse-fr.eu – Toulouse School of Economics, Avril 2018 – 5 pages
9. **Central banks and payments in the digital era** – BIS Annual Economic Report 2020
www.bis.org – 8 pages (extract)
10. **The rise of digital currency** – Tobias Adrian, Tommaso Mancini-Griffoli
<https://voxeu.org> – 09/09/2019 – 5 pages
11. **The Riksbank proposes a review of the concept of legal tender**
www.riksbank.se – 29/04/2019 – 1 page
12. **La Chine mise sur les devises 2.0 après le lancement du Libra** – Nessim Aït-Kacimi
www.lesechos.fr – 06/09/2019 – 1 page
13. **Could Facebook's Libra Affect National Economies and Interest Rates?** Joseph Gagnon, Gonzalo Huertas
www.piie.com – 28/08/2019 – 2 pages
14. **Vers la fin du paiement cash ?**
www.lemonde.fr – 09/06/2020 – 2 pages
15. **Buyer beware : hundreds of bitcoin wannabes show hallmark of fraud**
Shane Shifflett, Coulter Jones – www.wsj.com – 17/05/2018 – 1 page
16. **Digital Currencies, Stablecoins, and the Evolving Payments Landscape** – Speech Governor Lael Brainard
www.federalreserve.gov – 16/10/2019 – 5 pages

Quand les entreprises auront leur propre monnaie

Et si demain les entreprises se passaient des monnaies nationales ? Impensable il y a encore quelques mois, cette idée est désormais une réalité. Facebook veut lancer la sienne en 2020. Et le géant américain est loin d'être seul.

La presse du monde entier est en alerte ce 18 juin 2019. Après des fuites en série, Facebook doit enfin lever le voile sur son projet très attendu de « Facebook Coin ». Vont-ils vraiment le faire ? Personne ne semble y croire tant l'idée de monnaie se confond avec celle d'État. Mais Mark Zuckerberg n'a pas froid aux yeux. Dans la matinée, le réseau social annonce qu'il va bien créer avec une vingtaine de partenaires sa propre monnaie : la « libra ». Un certain émoi s'empare alors de la planète financière.

Six mois plus tard, l'effervescence est quelque peu retombée. Sous la pression des États, certains partenaires du milliardaire de 35 ans (Visa, Stripe, etc.) ont même quitté l'aventure. Mais la future libra prend forme. Il y a quelques semaines, l'association qui réunit tous les membres du projet (Uber, Spotify, le français Iliad...) a dévoilé ses premières avancées : plus de 50 000 transactions ont été effectuées avec succès sur la version test du réseau. Autrement dit, un utilisateur de Facebook peut potentiellement acheter des produits et envoyer des libras via le réseau social qui réunit WhatsApp, Messenger et Instagram. « *Le calendrier de lancement est maintenu pour 2020* », confirme une source interne au projet.

« Un nouveau monde »

La perspective d'un monde rempli de monnaies d'entreprises reste encore un fantasme. Mais Zuckerberg et ses partenaires ont clairement ouvert une brèche. Un peu partout sur la planète des sociétés réfléchissent à des systèmes similaires. Walmart dépose des brevets à tour de bras. La messagerie russe Telegram doit lancer le « Gram » en 2020. Le patron de Twitter voit le bitcoin comme une solution d'avenir. Amazon et Google planchent eux aussi sur de possibles applications... Pourquoi ne le feraient-elles pas ?

Tout est désormais possible. « *La monnaie est devenue une simple ligne de code* », souligne David Bounie, professeur d'économie à Télécom Paris. Internet a bouleversé l'économie : les consommateurs achètent directement en ligne, sur leurs ordinateurs, leurs smartphones. Ils manipulent toujours moins de monnaies physiques et le nombre de portefeuilles numériques explose. « *L'économie d'internet avait tout, il lui manquait juste des monnaies natives*, explique Clément Jeanneau de Blockchain Partner. *La technologie a réglé le problème et les entreprises en profitent* ».

Dans ce nouveau monde, les entreprises n'ont plus besoin des banques et des intermédiaires pour être en relation avec leurs clients et échanger de la valeur... Surtout, ces monnaies numériques sont programmables. Facebook et d'autres peuvent prévoir des incitations, des réductions sur tel ou tel produit si les consommateurs utilisent leur monnaie.

« *Nous avons encore du temps pour nous adapter, mais il ne faudra pas non plus trop tarder* », confie le responsable d'un géant français du paiement. Lors de la présentation du projet Libra, David Marcus, son concepteur, avait d'ailleurs insisté sur cet aspect : « *Les monnaies sont un nouveau champ d'exploration* ».

Une phase transitoire

Reste que la future libra et les autres projets ne peuvent pas encore se passer de l'euro, du dollar ou de la livre sterling. D'abord parce que les États ne vont pas se laisser faire. « *Ils vont essayer de les empêcher, mais ils ne pourront rien faire. Ça fait 20 ans qu'on essaye d'arrêter le pair à pair* », explique un avocat.

La chance de l'euro et du dollar c'est que les monnaies numériques ont encore besoin d'elles pour être stables, et donc utilisables dans le commerce. La future libra -un stablecoin- sera par exemple indexée sur un panier de cinq devises (dollar, euro, livre sterling, yen, dollar singapourien).

Cette situation n'est toutefois pas gravée dans le marbre. « *La confiance dans l'euro ou le dollar ne dépend que de celle que l'on met dans les institutions* », explique David Bounie. Le jour où les consommateurs auront davantage confiance dans les entreprises que dans les gouvernements, les choses pourraient vite basculer.

C'est déjà le cas dans certains pays d'Amérique du sud (Venezuela, Argentine...) où les cryptomonnaies comme le bitcoin s'apprécient en fonction des tensions économiques et politiques. Facebook a d'ailleurs prévu de pouvoir faire évoluer le protocole de la libra afin de se passer de son panier de devises...

Conscients du problème posé par cet avenir proche, les États ont commencé à réagir. La Chine a accéléré à l'automne son projet de crypto-yuan. Dans les tuyaux depuis des mois, il sera disponible courant 2020, selon Pékin, même si de nombreux experts doutent du calendrier.

Confiante dans la puissance du billet vert, la Réserve fédérale américaine (Fed) n'a, elle, pour l'heure pas jugé bon d'accélérer sur un éventuel dollar numérique. À l'inverse, la Banque centrale européenne (BCE) a déjà fait savoir qu'elle ne resterait pas inactive. Rien de concret n'a encore été annoncé, mais l'institution souhaiterait avancer sur son projet d'euro numérique.

« *Ma conviction personnelle est qu'étant donné les développements que nous voyons, non pas tant dans le bitcoin que dans les projets de stablecoins... nous ferions mieux d'être à l'avant-garde* », a expliqué Christine Lagarde lors de sa première conférence de politique monétaire à la tête de l'institution.

Retour vers le futur

Les États ont toutefois la mémoire courte. Il n'y a pas si longtemps, les entreprises avaient pour la plupart leurs monnaies. « *La monnaie est une invention des marchands pour faciliter les échanges et non une invention de l'État* », rappelle Philippe Simonnot, docteur d'Économie et ancien professeur à La Sorbonne.

En 1910, les États-Unis comptaient encore plus de 1 000 monnaies privées... Les industriels, les commerçants, les pétroliers avaient toutes les leurs. Mais cette multiplicité ralentissait l'économie. Le dollar permit justement de régler le problème en unifiant le marché.

Pourquoi les nouvelles monnaies privées marcheraient-elles mieux alors ? Parce qu'elles sont justement interoperables. Alors que les précédentes ne pouvaient pas s'échanger entre elles, les nouvelles le peuvent. Et de manière quasi instantanée. Facebook l'avait annoncé le 18 juin : les monnaies numériques sont là pour durer.

Raphaël Bloch

Blockchain : pourquoi JP Morgan crée sa propre crypto-monnaie JPM Coin

La plus grande banque américaine en termes d'actifs et la première au monde en capitalisation boursière, JP Morgan, a annoncé ce jeudi le test réussi d'une monnaie digitale, indexée sur le dollar, pour des paiements entre acteurs institutionnels. Explications.

Incroyable, mais vrai. La banque JP Morgan Chase, dont le patron Jamie Dimon avait traité le Bitcoin d'arnaque, est la première banque au monde à lancer sa propre crypto-monnaie, le JPM Coin. Il s'agit d'une monnaie digitale, s'appuyant sur la technologie Blockchain, née avec le Bitcoin, justement, il y a dix ans, mais elle est indexée sur le dollar et sert à des transferts d'argent instantanés entre des comptes d'acteurs institutionnels, de grands investisseurs, d'autres banques, de grandes entreprises, mais pas les particuliers.

La plus grande banque américaine en termes d'actifs, et la première au monde en capitalisation boursière, prend tous ses concurrents de vitesse et s'impose comme la première institution financière de cette taille à se lancer de plain-pied dans l'univers des crypto-actifs. Goldman Sachs hésite depuis des mois à ouvrir un desk de trading sur les crypto-actifs mais la chute des cours l'an dernier (plus de 70 % pour le Bitcoin par exemple) semble l'avoir incité à repousser ce projet. Fidelity a annoncé en octobre la création d'une filiale consacrée aux services en crypto-actifs, notamment la conservation.

"Le JPM Coin n'est pas de l'argent en soi. Il s'agit d'une pièce numérique représentant les dollars des États-Unis détenus dans des comptes spécifiques de JPMorgan Chase N.A [North America, ndlr]. En résumé, un JPM Coin a toujours une valeur équivalente à un dollar américain. Lorsqu'un client envoie de l'argent à un autre via la Blockchain, les JPM Coins sont transférés et échangés instantanément pour un montant équivalent en dollars américains, ce qui réduit le temps de règlement habituel" explique Umar Farooq, responsable de la Blockchain et des services numériques de trésorerie chez JP Morgan dans une présentation en ligne.



[Le schéma expliquant le transfert d'argent en utilisant le JPM Coin. Etape 1, l'émission: le client dépose de l'argent sur un compte spécifique et reçoit un équivalent en JPM Coins. Etape 2, le transfert : ces JPM Coins sont utilisés pour des transactions sur la Blockchain avec d'autres clients de JP Morgan. Etape 3, le remboursement : les détenteurs de JPM Coins les échangent contre des dollars chez JP Morgan.]

Un JPM Coin = un dollar

La banque américaine insiste sur le fait qu'elle croit surtout dans le potentiel de cette "technologie de registre distribué", de stockage et de transmission d'information qu'est la Blockchain, qu'elle tient à distinguer des crypto-monnaies proprement dites, qui font l'objet de spéculations et de montagnes russes.

"Nous avons toujours cru au potentiel de la technologie Blockchain et nous soutenons les crypto-monnaies tant qu'elles sont correctement contrôlées et réglementées. En tant que banque réglementée à l'échelle mondiale, nous pensons que nous avons une opportunité unique de développer cette capacité de manière responsable sous la supervision de nos régulateurs" explique le responsable Blockchain de la banque américaine.

"L'échange de valeur, telle que de l'argent, entre différentes parties sur une Blockchain nécessite une devise numérique ; nous avons donc créé la pièce JPM" relève-t-il.

La banque américaine tient aussi à distinguer son JPM Coin des "stable coins", d'autres monnaies digitales indexées sur des monnaies fiduciaires comme USDC de Circle, Tether, Gemini, etc : sa monnaie digitale sera

remboursable en monnaie fiduciaire détenue par JP Morgan, qui met en avant son "*bilan forteresse*" de 2 600 milliards de dollars.

"En d'autres termes, un JPM Coin représente 1 dollar" assure calmement JP Morgan.

À terme, le JPM Coin sera aussi indexé sur les autres principales devises.

Un prototype bientôt en production

JP Morgan dévoile peu de détails sur la technologie utilisée : il s'agit d'une Blockchain privée, "*permissionnée*" (avec accès restreint aux membres autorisés), développée par la banque "*et/ou des partenaires*". Les JPM Coins seront émis sur la Blockchain Quorum, une version privée de la Blockchain Ethereum que JP Morgan a développée, et devraient être "*utilisables sur tous les réseaux Blockchain standards*". La banque précise que la création de ce "coin" n'a pas d'impact avec son "réseau d'information interbancaire" sur la Blockchain, l'Interbank Information Network, qui a fédéré plus de 75 banques, qui ne transfère que de la donnée, pas de la valeur, entre banques "correspondantes" (activité qui consiste à fournir un compte à une banque étrangère pour des opérations en devises locales).

Elle souligne d'ailleurs son expertise en matière de Blockchain et les "*centaines de millions de dollars dépensés chaque année dans la cybersécurité*", ainsi que ses contrôles robustes en matière de KYC (la connaissance client) et de lutte contre le blanchiment.

JP Morgan précise toutefois que son JPM Coin n'est encore qu'un prototype, qui entrera bientôt en production. Il sera testé avec un petit nombre de ses clients institutionnels dans un premier temps, avant d'être étendu au cours de l'année. La banque n'exclut pas totalement d'en étendre un jour l'usage aux clients finaux des institutionnels.

La nouvelle a troublé et agacé l'économiste Nouriel Roubini, le plus virulent détracteur de la Blockchain et des crypto-monnaies, qui a réagi sur Twitter :

"En quoi la nouvelle prétendue crypto monnaie de JPMorgan a quoi que ce soit à voir avec la blockchain/crypto ? Elle est privée, non publique, "permissionnée" et pas sans autorisation, basée sur les autorités de confiance vérifiant la transaction et non sans confiance, centralisée et non décentralisée. L'appeler crypto est une blague".

Tokenisation de la monnaie et ubérisation des banques

De nombreuses institutions financières sont en quête d'une solution pour échanger plus rapidement de la valeur en numérique, sans les délais habituels de règlement-livraison, de compensation entre banques ou courtiers. Même des banques centrales réfléchissent à la façon de "tokeniser" (transformer en "*token*" ou jeton numérique) la monnaie fiduciaire.

"Créer de la monnaie programmable, extrêmement fluide à échanger" expliquait récemment Eric Larchevêque, le cofondateur de l'ex-Maison du Bitcoin et de Ledger, qui confiait sa prédiction que "la Blockchain va se démocratiser par la « tokenisation » de la monnaie fiat [fiduciaire, ayant cours légal], de l'euro ou du dollar, qui va permettre de créer un système financier alternatif au sens technologique."

Un certain nombre de banques (dont Crédit Agricole) testent le protocole de paiement de la startup américaine Ripple, qui utilise la technologie Blockchain, pour accélérer les virements transfrontaliers notamment et s'approcher du temps réel, quand cela prend trois jours sur le réseau interbancaire Swift. Le patron de Ripple, Brad Garlinghouse, a d'ailleurs réagi sur Twitter.

"Comme prévu, les banques changent de ton sur la crypto. Mais ce projet JPM passe à côté de l'essentiel : introduire un réseau fermé aujourd'hui revient à lancer AOL après l'introduction en bourse de Netscape" a-t-il raillé, estimant que "les coins de banque ne sont pas la solution."

L'initiative de JP Morgan montre que la banque américaine n'a pas l'intention de se laisser "ubériser" par des startups spécialistes de la Blockchain, technologie qui permet de supprimer les intermédiaires (donc potentiellement les banques), ni d'attendre indéfiniment que les banques centrales s'engagent résolument dans la tokenisation de la monnaie légale. Elle propose d'emblée son alternative commerciale de cash électronique. Un exemple à méditer pour les autres grands acteurs de la finance.

Delphine Cuny

Les monnaies digitales sont-elles « disruptives » pour les banques centrales ?

Par Laurent CLERC

Directeur de la Stabilité financière à la Banque de France ⁽¹⁾

Les monnaies digitales, dont la part dans les transactions reste faible, ne constituent à ce jour un danger ni pour la conduite de la politique monétaire ni pour la stabilité financière. Toutefois, leur essor est spectaculaire. Combinant une nouvelle forme de monnaie et un nouveau système de paiement, elles pourraient s'avérer, dans un futur proche, « disruptives » pour le système bancaire et les banques centrales. Face à de telles évolutions, les banques centrales pourraient être conduites à émettre elles-mêmes de la monnaie digitale selon différentes modalités, que nous présenterons dans cet article. La plupart d'entre elles ont pour corollaire la disparition du système des réserves fractionnaires et, éventuellement, celle du cash et des dépôts bancaires, avec des conséquences importantes pour le mécanisme de création monétaire.

James Tobin, prix Nobel d'économie 1981, considérait que le cumul des fonctions de collecte des dépôts et de distribution du crédit au sein des banques était le fruit d'un « accident historique » (TOBIN, 1985). C'est pourtant sur cette base que repose le cadre opérationnel de nombreuses banques centrales. Or, ce socle est vulnérable, comme l'a illustré la crise financière de 2008, les risques afférents à la distribution du crédit ou ceux affectant la valeur ou la liquidité des actifs adossés à la monnaie pouvant impacter négativement le fonctionnement du système de paiement. Une solution préconisée par James Tobin – mais jugée irréaliste du fait des contraintes technologiques des années 1980 –, pour offrir tous les bénéfices d'un moyen de paiement sans les inconvénients évoqués ci-dessus, serait d'autoriser les particuliers à détenir directement des dépôts à la banque centrale.

Cette proposition ne relève plus aujourd'hui du domaine de la science-fiction : en effet, la Banque centrale de l'Équateur a commencé à émettre de la monnaie digitale afin de favoriser l'inclusion financière dans un pays où une grande partie de la population n'est pas bancarisée. D'autres envisagent de le faire prochainement, comme la Banque centrale de Suède, qui est confrontée à une forte érosion de la demande de cash (SKINGSLEY, 2016). D'autres, enfin, ont lancé des réflexions à ce sujet, notamment l'Angleterre (voir BROADBEND (2016) et BARRDEAR & KUMHOF (2016)), le Canada (voir FUNG & HALABURDA (2016)) et la Chine.

L'essor spectaculaire des monnaies digitales, depuis l'apparition du Bitcoin en 2009, interpelle. Ces monnaies combinent une nouvelle forme de monnaie et un nouveau système de paiement : d'une part, elles correspondent à des actifs présentant des caractéristiques monétaires qui ne sont ni liées à une devise légale particulière ou à un État ni adossées à une dette. Leur valeur intrinsèque est nulle : elle ne dépend que du fait que l'on anticipe qu'elles seront utilisées par de nombreux individus (effet de réseau) et qu'elles auront un pouvoir libérateur (c'est-à-dire une capacité d'acheter des biens et des services, ou de les échanger contre une devise). D'autre part, elles s'appuient sur un registre distribué et sur un réseau de tiers qui ne sont pas (généralement) des banques. L'émergence des monnaies virtuelles permet donc d'ores et déjà de dissocier les deux fonctions qui étaient jusqu'à présent effectuées par les banques, et, peut-être, à terme, de les contourner. Couplées à des plateformes de *crowdfunding*, elles offrent, par exemple, aux particuliers la possibilité de financer des projets bien identifiés, contrairement aux dépôts bancaires, dont l'affectation par les banques est opaque. Elles sont donc potentiellement « disruptives » pour le système bancaire.

(1) Les opinions exprimées dans cet article n'engagent que l'auteur. Elles ne reflètent pas nécessairement celles de la Banque de France ou celles de l'Eurosystème.

Des monnaies de crise ?

Certaines monnaies digitales telles que le Bitcoin (voir NAKAMOTO, 2008), peuvent être considérées, dans une certaine mesure, comme des « monnaies de crise ». En sus du facteur technologique lié au développement d'Internet, leur apparition peut être perçue comme la conséquence d'une perte de confiance de la part de certains agents économiques dans la valeur de la monnaie légale.

La crise de 2008 a en effet montré que le système bancaire est fragile, voire intrinsèquement instable. Pour les tenants de l'école du *Free Banking* (ROTHBARD, 1992 ; DOWD, 1992), cette instabilité intrinsèque explique pourquoi il est nécessaire d'avoir à la fois une réglementation du système bancaire, des banques centrales et un prêteur en dernier ressort. Un tel système est cependant à l'origine de frictions et de contraintes qui empêchent le libre jeu des forces du marché. Il conduit à une allocation sous-optimale des ressources, qui est à l'origine de crises bancaires récurrentes. *A contrario*, l'émergence de monnaies privées, créées et gérées directement par des particuliers assurerait la stabilité financière (les agents seraient mieux à même de gérer leurs propres intérêts) et la stabilité monétaire. Les fondateurs du réseau Bitcoin se sont référés directement à cette école de pensée, ainsi qu'à l'École autrichienne (en particulier, HAYEK, 1976), pour la création de cette monnaie qui se dispense de banque centrale.

L'École autrichienne (voir VON MISES, 1953) considère que l'action des banques centrales est à l'origine de fluctuations économiques indésirables : par la création monétaire, les banques centrales alimentent une croissance excessive du crédit et maintiennent les taux d'intérêt à un niveau artificiellement bas. Dans ce contexte, des déséquilibres financiers apparaissent et se développent jusqu'au point où ils conduisent à un retournement violent du cycle d'activité. La fonction de préservation de la valeur de la monnaie n'est donc pas assurée par les banques centrales. Les théoriciens de l'École autrichienne préconisent l'adoption de l'étalon-or, un système dans lequel la valeur de la monnaie ne peut être aisément manipulée par les autorités monétaires.

De ce point de vue, les politiques de *Quantitative Easing* menées depuis la crise de 2008 seraient la preuve que les banques centrales ne souhaitent pas ou ne peuvent pas – car encore trop dépendantes du pouvoir politique – assurer la stabilité monétaire. Elles généreraient donc un excès d'offre de monnaie.

Le système mis en place par le réseau Bitcoin répond directement à ce souci. Le processus de création monétaire y est complètement automatisé, de sorte que le rythme de la création de monnaie est prédéterminé et, qu'à terme, la quantité de monnaie créée par le système est fixe (21 millions de Bitcoins en 2050). Le processus « d'extraction » ou de création de Bitcoins est complexe, et donc coûteux. Il porte le nom de « minage ». Ce « minage » est un procédé qui utilise les ordinateurs de certains utilisateurs (appelés les « mineurs ») pour effectuer des calculs mathématiques de plus en plus complexes destinés à confirmer les tran-

sactions et à assurer ainsi la sécurité du réseau. La complexité de ces calculs ne cesse d'augmenter, de manière à maintenir constante la fréquence de validation des transactions (une création de « bloc » toutes les 10 minutes). Les « mineurs » qui parviennent à résoudre ces équations complexes collectent les frais de transaction ainsi que les Bitcoins nouvellement créés, à un rythme qui décroît de façon géométrique de 50 % tous les 4 ans. Toutefois, l'analogie avec l'étalon-or de l'École autrichienne s'arrête là, car il n'existe aucun mécanisme qui relierait la valeur d'une unité de Bitcoin à une référence externe.

Les risques inhérents aux monnaies électroniques pour le cadre opérationnel des banques centrales

Le cadre opérationnel des banques centrales repose sur deux piliers : un système de paiement partitionné et un système des réserves fractionnaires.

Le système de paiement partitionné

Dans le système de paiement actuel, les réserves des banques auprès de la banque centrale jouent un rôle essentiel : elles constituent en effet l'actif dans lequel se soldent les transactions interbancaires. Seules les banques ont un accès direct à ces réserves. Une transaction entre le client A1 (de la Figure 1 ci-après), qui possède un compte à la banque A, avec le client B2, qui a son compte à la banque B, ne peut s'effectuer que *via* les comptes de ces deux banques, à la banque centrale. Ce règlement s'effectue en réserves. Par le mécanisme des réserves obligatoires, les banques sont dans l'obligation de conserver des réserves auprès de la banque centrale. Ce mécanisme a pour effet d'élargir le déficit de liquidité du système, lequel ne peut être comblé que par la banque centrale *via* ses opérations de refinancement. Celle-ci agit donc en tant que prêteur marginal, ce qui lui permet de fixer le taux d'intérêt auquel sont échangées les réserves. Ce taux d'intérêt sert de référence pour la fixation des autres taux d'intérêt, en particulier bancaires.

Le système des réserves fractionnaires

Les banques disposent d'un pouvoir de création monétaire : en distribuant des crédits à l'économie, elles génèrent dans le système bancaire de nouveaux dépôts,

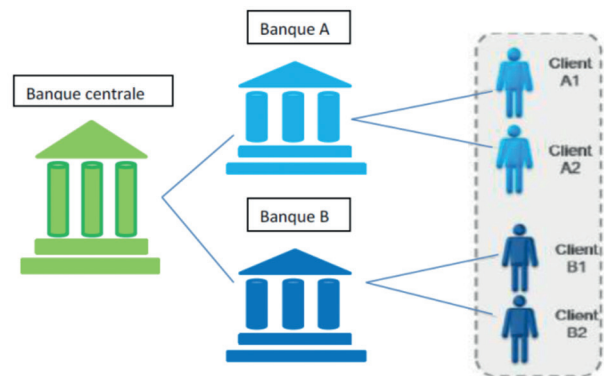


Figure 1 : Système de paiement partitionné.
Source : HE et al. (2016), FMI.

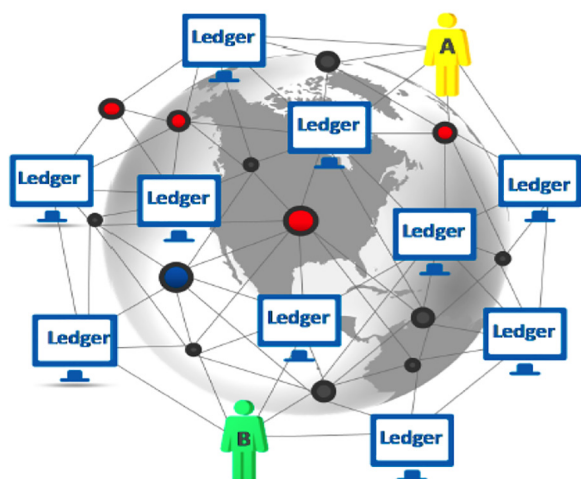


Figure 2 : Système de paiement décentralisé.

Source : HE et al. (2016), FMI.

dont une fraction est détenue par elles, sous la forme de réserves obligatoires déposées à la banque centrale. Le montant de ces réserves est cependant très faible au regard de la création monétaire des banques : on parle donc de système de réserves fractionnaires. En modifiant le taux des réserves obligatoires ou le taux d'intérêt auquel elle refinance les banques, la banque centrale exerce donc une influence sur les conditions de financement de l'économie.

Le caractère « disruptif » des systèmes décentralisés

Les monnaies digitales sont potentiellement « disruptives » pour le système de paiement tel qu'il fonctionne actuellement. Elles rendent en effet possibles des transactions directes entre les individus A et B sans passer par le système bancaire et la banque centrale (voir la Figure 2 ci-dessus). Celle-ci perd une grande partie de son influence sur les conditions de financement, et ce d'autant plus que le système de paiement partitionné ne repose que sur le système bancaire. Les autres intermédiaires financiers, tels que les gestionnaires d'actifs ou les *Fintechs*, en sont exclus. Il existe donc un risque réel de déconnexion entre le système de paiement partitionné et les échanges s'effectuant de façon complètement décentralisée.

Vers une émission de la monnaie digitale par les banques centrales ?

Les bénéfices attendus

Dans l'hypothèse où les monnaies digitales viendraient à se développer fortement, leur émission par une banque centrale permettrait notamment :

- de favoriser la transition vers l'économie digitale, grâce à l'élimination des activités illicites effectuées en cash et aux gains d'efficacité associés à la réduction de l'économie informelle, à l'accroissement de la base fiscale et à la réduction du coût de maintenance du cash (voir ROGOFF, 2014) ;
- de favoriser l'innovation dans les systèmes de paiement, notamment en accueillant de nouvelles entités concurrentes des banques ;
- de fournir de nouveaux outils de gestion du risque sys-

témique en réduisant les risques de concentration et de crédit, ainsi que l'aléa moral généré par la moindre importance des dépôts à assurer ;

- à ladite banque centrale d'utiliser de nouveaux instruments (taux d'intérêt négatifs, « Hélicoptère » de Friedman) et de recouvrer le contrôle du processus de création monétaire ;
- et, enfin, de recouvrer une partie de son seigniorage perdu du fait du déclin du cash et de la marginalisation des réserves.

Différentes modalités envisageables pour l'émission de monnaie digitale

Le statu quo : vers une pérennisation du mode non conventionnel ?

Une solution immédiate serait de conserver le cadre opérationnel actuel et d'autoriser l'utilisation des monnaies digitales. Pour une banque centrale, ce qui importe, c'est que son action affecte directement les décisions des agents. Or, depuis la crise de 2008, la politique monétaire a conservé une certaine efficacité en dépit d'un blocage quasi complet du système bancaire. Grâce à leurs mesures non conventionnelles, les banques centrales ont pu contourner un secteur bancaire fragilisé pour offrir directement des financements à l'économie. Le maintien du mode non conventionnel présente toutefois des inconvénients : le premier est de devoir s'adapter continuellement, au gré des circonstances ; et le deuxième est d'opérer de façon ciblée, au détriment de la dimension transversale de la politique monétaire conventionnelle (*"Monetary policy gets in all of the cracks"*, STEIN, 2012).

L'émission de monnaie digitale en sus de la monnaie papier

Une deuxième possibilité consisterait à conserver l'usage de la monnaie légale et à en émettre une version digitale. La banque centrale ouvrirait ses comptes aux banques, ainsi qu'aux *Fintechs*, auxquelles elle fournirait cette monnaie digitale contre du collatéral (par exemple, des bons du Trésor). Ces institutions pourraient alors utiliser cette monnaie pour accorder des prêts, la banque centrale assurant par ailleurs la convertibilité de la monnaie digitale légale et du cash. L'intérêt pour la banque centrale est, dans un tel cas de figure, de disposer d'un système reposant sur une *blockchain*, ce qui lui permettrait d'avoir une vision en quasi-temps réel des transactions effectuées dans l'ensemble du système financier et, par conséquent, de mesurer le niveau d'endettement de l'économie tout en contrôlant l'offre de monnaie digitale (DYSON et HODGSON, 2016). Ce système impliquerait cependant l'abandon du système des réserves fractionnaires : le taux de réserve passerait à 100 % et les banques perdraient toute capacité de création monétaire. Cette situation correspond au système du *narrow banking*.

Un système de paiement partitionné adossé à une blockchain

Dans ce système, la banque centrale sélectionne les banques participantes. Elle émet la monnaie digitale, et les réserves des institutions sont transformées en monnaie centrale digitale. Les prêts accordés par ces institutions sont effectués en monnaie digitale centrale. Les

banques peuvent émettre leur propre monnaie digitale (dont une partie est garantie par leurs dépôts en monnaie centrale digitale auprès de la banque centrale). Le système des réserves fractionnaires est ainsi préservé. Les consommateurs peuvent toujours convertir la monnaie digitale émise par les banques en monnaie légale (cash). L'avantage de ce système réside dans les gains liés à l'utilisation de la *blockchain* (vitesse d'exécution, coûts réduits...). Ses inconvénients résident, quant à eux, dans le pouvoir de manipulation et de fraude des banques qui émettent leur propre monnaie digitale, ainsi que dans le risque de fortes fluctuations de la valeur de ces monnaies par rapport à la monnaie légale.

Une variante consisterait à autoriser un accès indirect *via* des comptes en monnaie digitale. La banque centrale créerait la monnaie digitale et la détiendrait dans des comptes agrégés. Les banques et les *Fintechs* gèreraient ces comptes et les proposeraient à leurs clients. Ces fournisseurs de comptes digitaux fourniraient également tous les services associés (états, codes, numéros de comptes, banques Internet...). Ils ne seraient que des intermédiaires, des administrateurs de comptes. Dans ce système, le taux des réserves serait de 100 % (*narrow banking*).

Un accès direct pour tous à la banque centrale

Un dernier mode d'organisation serait celui où la banque centrale ouvrirait des comptes directs à toutes les entités (les banques, les *Fintechs*, les entreprises et les particuliers). Elle émettrait la monnaie digitale qui se substituerait intégralement au cash. Un tel système admet un marché libre pour les prêts et les dépôts et repose sur un registre distribué. Ce dernier garantit un pseudo-anonymat des transactions et conserve l'historique des événements de crédit. Il se caractérise par une grande fluidité des paiements, les consommateurs pouvant transférer les dépôts d'une banque à une autre très facilement et pour des coûts réduits. Dans un tel système, la banque centrale assure tous les services de gestion des comptes digitaux. Elle entre cependant en concurrence avec les banques commerciales. Comme dans le cas précédent, le taux des réserves serait de 100 %.

Quelques enjeux entourant l'émission de monnaie digitale par les banques centrales

L'un des objectifs recherchés de l'émission de monnaie digitale par une banque centrale est la possibilité d'imposer des taux d'intérêt négatifs. La mise en œuvre de tels taux pourrait néanmoins inciter les agents économiques à détenir l'intégralité de leurs avoirs en cash (dont le taux d'intérêt est nul), ce qui rendrait cette mesure inefficace. Certains préconisent donc l'abandon du cash en cas d'émission de monnaie digitale. En outre, lorsque cette monnaie coexiste avec d'autres formes de monnaie, se pose alors la question de la rémunération des dépôts en monnaie digitale à la banque centrale.

L'émission de monnaie digitale par une banque centrale correspond à une dette qui doit être compensée, dans son

(2) Dans le cas précédent, il ne s'agit pas, à proprement parler, d'une dette, car ce bon ni ne donne droit au versement d'intérêts ni ne possède d'échéance.

bilan, par un actif. En l'absence de rémunération, cet actif peut être un bon perpétuel à zéro coupon émis spécialement par le Trésor. En cas de rémunération, en revanche, le titre émis doit être d'une nature différente, ce qui n'est plus nécessairement neutre pour la dette publique⁽²⁾. Si les comptes digitaux ne sont pas rémunérés (ou s'ils le sont moins que les réserves), les banques bénéficient d'un avantage concurrentiel. Le taux d'intérêt servi doit donc être au moins égal à celui des réserves. Cela en fait un substitut aux réserves, ce qui ouvre la voie à la mise en œuvre des taux négatifs. Toutefois, les comptes digi-taux ouverts auprès de la banque centrale sont *a priori* sans risque, contrairement aux dépôts bancaires. Leur rémunération revient implicitement à mettre en place un plancher de rémunération des dépôts bancaires, et cela crée une incitation à la hausse des taux d'intérêt débiteurs pour attirer la clientèle, avec, potentiellement, un impact défavorable sur la rentabilité bancaire. Il y a donc un risque d'évaporation des dépôts bancaires au profit des comptes existant à la banque centrale. On revient, dans ce cas, au système du *narrow banking* (évoqué plus haut) tel qu'il a été préconisé par un groupe d'économistes, dans les années 1930, sous le nom de « Plan de Chicago » (voir SIMONS *et al.*, 1933).

Au final, plusieurs des options que nous avons présentées ci-dessus ont donc pour corollaire la disparition du système des réserves fractionnaires et, éventuellement, celle du cash et des dépôts bancaires (ce qui pourrait avoir des conséquences importantes pour le mécanisme de création monétaire).

Conclusion

Les monnaies digitales, qui représentent à ce jour un montant très faible des transactions, ne constituent de risque imminent ni pour la conduite de la politique monétaire ni pour la stabilité financière. Leur essor est cependant spectaculaire et elles sont potentiellement « disruptives ».

Leur développement renvoie à l'une des questions fondamentales de la théorie monétaire. Jusqu'à présent, l'origine de la monnaie est expliquée par le problème de la double coïncidence des besoins : dans un système de troc, l'échange de biens ne peut avoir lieu que si le bien en ma possession intéresse la personne avec laquelle je veux échanger. L'introduction de la monnaie, qui agit à la fois comme unité de compte, intermédiaire des échanges et réserve de valeur, résout cette difficulté. Kocherlakota (1996) avance une autre hypothèse selon laquelle la monnaie serait un substitut à la mémoire. Un système de troc peut parfaitement fonctionner dans une société de petite taille. Il suffit pour cela que les individus se souviennent de l'histoire des échanges et de ce qui est dû aux uns et aux autres. À mesure que le temps passe et que la société s'agrandit, cette mémoire des échanges devient de plus en plus difficile à conserver. La monnaie résout, là encore, cette difficulté. Le registre distribué, davantage que les monnaies digitales, offre une solution alternative, puisque ce registre « est mémoire ». Il autorise l'émergence potentielle d'un système de troc généralisé – plus précisément de « crédit », car il introduit une dimension intertemporelle –, sans avoir nécessairement besoin d'une monnaie.

A Chinese digital currency is the real threat, not Facebook's Libra

Western governments need to start thinking about their response to currencies they cannot control.

The Facebook chief executive, Mark Zuckerberg, was at least half right when he recently told Congress that there was no US monopoly on regulation of next-generation payments technology. You may not like Facebook's proposed Libra (pseudo) cryptocurrency, Zuckerberg implied, but a state-run Chinese digital currency with global ambitions is perhaps just a few months away, and you will probably like that even less.

Perhaps Zuckerberg went too far when he suggested that the imminent rise of a Chinese digital currency could undermine overall dollar dominance of global trade and finance – at least the large part that is legal, taxed, and regulated. In fact, US regulators have vast power not only over domestic entities but also over any financial firms that need access to dollar markets, as Europe recently learned to its dismay when the US forced European banks to comply with severe restrictions on doing business with Iran.

America's deep and liquid markets, its strong institutions, and the rule of law will trump Chinese efforts to achieve currency dominance for a long time to come. China's burdensome capital controls, its limits on foreign holdings of bonds and equities, and the general opaqueness of its financial system leave the yuan many decades away from supplanting the dollar in the legal global economy.

Control over the underground economy, however, is another matter entirely. The global underground economy, consisting mainly of tax evasion and criminal activities, but also terrorism, is much smaller than the legal economy (perhaps one-fifth the size), but it is still highly consequential. The issue here is not so much whose currency is dominant, but how to minimise adverse effects. And a widely used, state-backed Chinese digital currency could certainly have an impact, especially in areas where China's interests do not coincide with those of the west.

A US-regulated digital currency could in principle be required to be traceable by US authorities, so that if North Korea were to use it to hire Russian nuclear scientists, or Iran were to use it to finance terrorist activity, they would run a high risk of being caught, and potentially even blocked. If, however, the digital currency were run out of China, the US would have far fewer levers to pull. Western regulators could ultimately ban the use of China's digital currency, but that wouldn't stop it from being used in large parts of Africa, Latin America, and Asia, which in turn could engender some underground demand even in the US and Europe.

One might well ask why existing cryptocurrencies such as bitcoin cannot already perform this function. To an extremely limited extent, they do. But regulators worldwide have huge incentives to rein in cryptocurrencies by sharply proscribing their use in banks and retail establishments. Such restrictions make existing cryptocurrencies highly illiquid and ultimately greatly limit their fundamental underlying value. Not so for a Chinese-backed digital renminbi that could readily be spent in one of the world's two largest economies. True, when China announces its new digital currency, it will almost surely be "permissioned": a central clearing

house will in principle allow the Chinese government to see anything and everything. But the US will not.

Business Today: sign up for a morning shot of financial news

Facebook's Libra is also designed as a "permissioned" currency, in its case under the auspices of Swiss regulators. Cooperation with Switzerland, where the currency is officially registered, will surely be much better than with China, despite Switzerland's long tradition of extending privacy to financial transactions, especially with regard to tax evasion.

The fact that Libra will be pegged to the US dollar will give US authorities additional insight, because (at present) all dollar clearing must go through US-regulated entities. Still, given that Libra's functionality can largely be duplicated with existing financial instruments, it is hard to see much fundamental demand for Libra except among those aiming to evade detection. Unless tech-sponsored currencies offer genuinely superior technology – and this is not at all obvious – they should be regulated in the same way as everyone else.

If nothing else, Libra has inspired many advanced-economy central banks to accelerate their programmes to provide broader-based retail digital currencies, and, one hopes, to strengthen their efforts to boost financial inclusion. But this battle is not simply over the profits from printing currency; ultimately, it is over the state's ability to regulate and tax the economy in general, and over the US government's ability to use the dollar's global role to advance its international policy aims.

The US currently has financial sanctions in place against 12 countries. Turkey was briefly sanctioned last month after its invasion of Kurdish territory in Syria, though the measures were quickly lifted. For Russia, sanctions have been in place for five years.

Just as technology has disrupted media, politics, and business, it is on the verge of disrupting America's ability to leverage faith in its currency to pursue its broader national interests. Libra is probably not the answer to the coming disruption posed by government-sanctioned digital currencies from China and elsewhere. But if not, western governments need to start thinking about their response now, before it is too late.

Kenneth Rogoff

*Professor of economics and public policy at Harvard University
Chief economist of the IMF from 2001 to 2003*

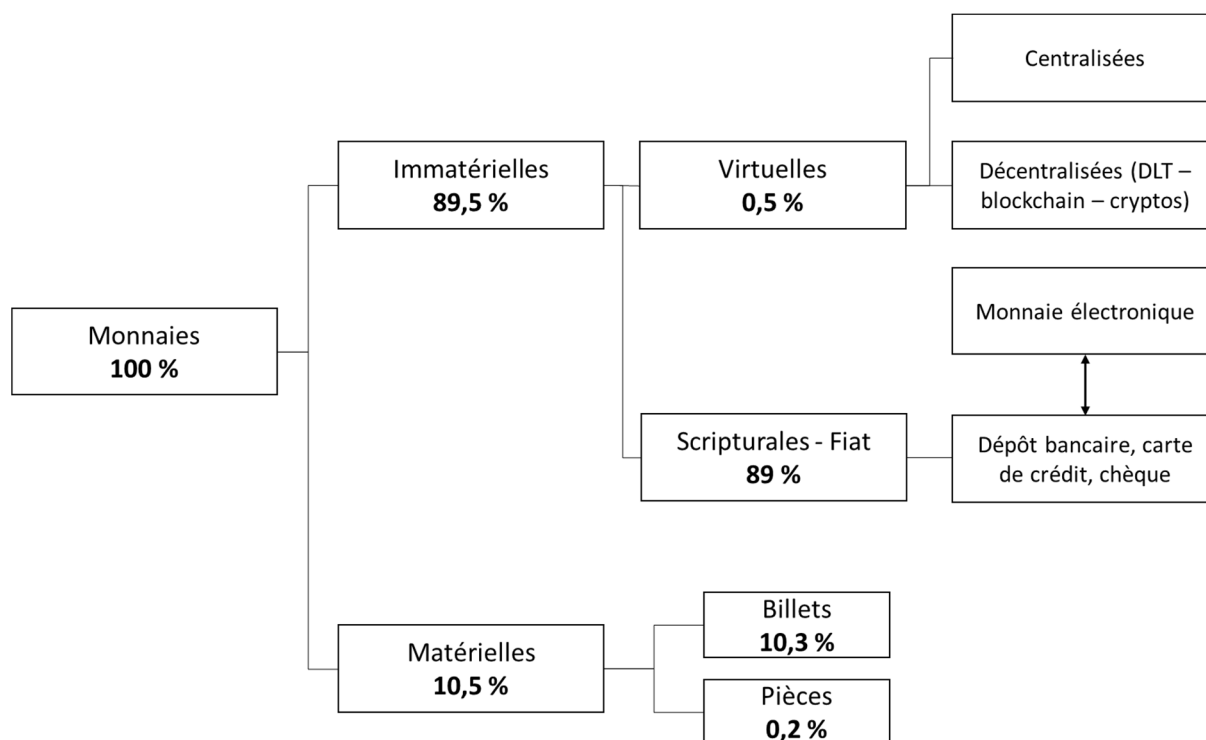
Les cryptos-monnaies

I. QUE SONT LES CRYPTO-MONNAIES ?

Les crypto-monnaies³ sont des monnaies virtuelles, utilisant la cryptographie pour être échangées en toute sécurité sur Internet et qui, pour certaines, sont gérées de manière décentralisée. Trois caractéristiques définissent donc conjointement les crypto-monnaies :

- **Ce sont des monnaies virtuelles**, c'est-à-dire des représentations numériques de valeur purement fiduciaires : elles ne sont émises ou garanties ni par une banque centrale, ni par une institution de crédit ou monétaire⁴ ;
- **Elles utilisent la cryptographie** : elles sont conçues et adaptées pour transmettre de la valeur sur Internet dans un environnement totalement ouvert et public, et en toute sécurité.
- **La plupart, mais pas toutes, fonctionnent dans un système décentralisé**, où l'information est intégralement, simultanément et également distribuée entre tous les participants. Les transactions sont décidées et validées par « consensus ». Beaucoup, mais pas toutes, sont adossées à la technologie blockchain.

Le schéma ci-dessous présente la place des crypto-monnaies dans l'univers des instruments monétaires.



Il ressort très clairement que le poids des crypto-monnaies est aujourd'hui minime, rapporté à l'univers des monnaies avec cours légal, dites monnaies « fiat ».

³ Les banques centrales soulignent, à juste titre, que les crypto-monnaies ne sont pas de vraies monnaies, dans la mesure où elles n'ont pas de cours légal. Leur utilisation comme instruments de paiement et comme réserve de valeur soulève de nombreuses questions et difficultés, analysées dans le présent rapport. L'utilisation du terme de crypto-monnaie peut donc être jugée infondée. Il y est toutefois recouru dans le présent rapport par pure commodité, dans la mesure où les textes légaux y font explicitement référence, ainsi qu'indifféremment au terme de « crypto-actifs ».

⁴ Banque centrale européenne (BCE), *Virtual Currency schemes*, février 2015.

A. La double innovation des crypto-monnaies

Hormis les pièces et billets de banque⁵, toute monnaie est aujourd'hui dématérialisée et « digitale ». Elle existe uniquement sous forme électronique. Il en va de même des actifs et titres financiers. Les crypto-monnaies n'apportent, de ce point de vue, aucun changement.

La révolution est ailleurs et plus profonde, à la fois technologique et monétaire. Ces deux éléments sont présents dans la plupart des crypto-monnaies.

1. L'innovation technologique

Beaucoup des technologies de base utilisées par les crypto-monnaies, comme les registres distribués, les techniques cryptographiques et les signatures électroniques, existent depuis plusieurs décennies. L'innovation vient de la combinaison de ces diverses techniques dans un projet ambitieux et cohérent.

L'innovation dans les procédures et dans les registres : la blockchain

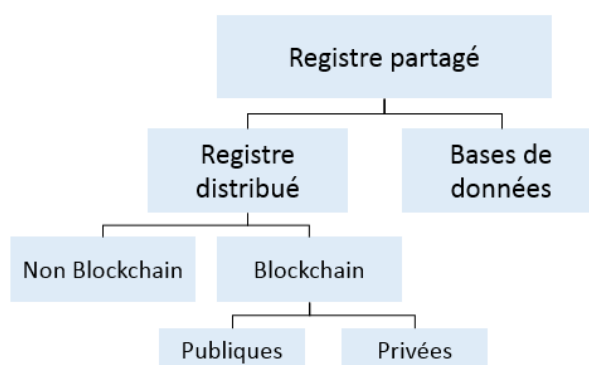
- **La technologie des registres distribués (DLT)** : ce sont des registres sécurisés, pouvant être partagés simultanément et de manière synchronisée par une multitude de participants, lesquels peuvent être ou non pré-sélectionnés ;
- **La blockchain elle-même qui est une forme particulière de registres distribués dans laquelle :**
Les données sont regroupées en blocs successifs dans un registre distribué, sur lequel l'intégralité des informations relatives aux transactions effectuées est stockée dans des blocs.
Ces blocs sont séquentiellement liés les uns aux autres et numérotés. Un lien cryptographique est établi entre chaque bloc et le suivant. Il est rétrospectivement impossible de modifier, même infinitésimalement, un bloc de la chaîne sans que tous les suivants soient complètement bouleversés de manière immédiatement visible⁶. C'est le grand intérêt de la blockchain. Elle est immuable. On ne peut revenir sur ce qui a été inscrit.
- **Les procédures de consensus** : elles permettent aux participants au réseau de valider collectivement les transactions.

Ces trois composants ne sont pas nécessairement liés et présents dans toutes les crypto-monnaies. On les retrouve intégralement dans Bitcoin et Ether, mais pas dans d'autres crypto-monnaies. Par exemple, Ripple, la troisième plus importante crypto-monnaie, a des registres distribués et des règles de consensus, mais pas de blockchain. La crypto-monnaie IOTA ne s'appuie pas sur une blockchain et la décentralisation n'y est pas totale. Dans les blockchains privées, entre participants se faisant confiance (avec éventuellement des crypto-monnaies attachées), la décentralisation est limitée et les procédures de consensus sont moins développées voire inexistantes, car rendues moins nécessaires.

⁵ Qui représentent généralement moins de 10 % de la masse monétaire totale (10 % dans la zone euro).

⁶ La fonction de hachage.

Le schéma suivant permet de situer la technologie blockchain dans le cadre existant :



La digitalisation de la valeur

C'est une deuxième innovation que les crypto-monnaies contribuent à promouvoir. Elle est moins présente dans le discours public, mais probablement beaucoup plus significative pour l'avenir. Il s'agit de la capacité à représenter numériquement de la valeur et à la transférer en toute sécurité entre individus sans aucun intermédiaire – constituant ainsi une sorte de « billet de banque » digital. Les représentations digitales de valeur sont couramment appelées des « jetons » ou plus fréquemment encore, par leur nom anglais, des « tokens ». La cryptographie moderne permet, le cas échéant, de faire cette opération de manière anonyme. La deuxième partie du rapport discute les perspectives ouvertes par cette innovation.

2. L'innovation monétaire

Pour mieux en saisir la portée, il est utile de décrire les caractéristiques du système monétaire actuel et de mesurer en quoi les crypto-monnaies s'en distinguent.

Les banques, la banque centrale et la monnaie

Dans les économies modernes, la monnaie est majoritairement constituée de dépôts bancaires. Pour l'essentiel, la monnaie est donc créée, détruite et transférée par les banques. Cette monnaie dite « de banque » a plusieurs caractéristiques notables :

- Pour posséder la monnaie et l'utiliser, il faut disposer d'un compte bancaire, nécessaire à l'inclusion financière au sein d'une société ;
- Toute transaction monétaire s'accompagne d'un mouvement de comptes bancaires. Elle est identifiable et traçable. Elle peut être surveillée et règlementée ;
- La monnaie est une créance sur une personne morale identifiable, en l'occurrence la banque. Un dépôt bancaire confère à son titulaire des droits sur la banque, notamment celui de convertir son dépôt en billets, lesquels ont un cours légal ;
- La monnaie de banque est une monnaie « privée ». Elle est donc vulnérable à une perte de confiance dans les banques qui l'ont émise ;
- Mais elle bénéficie, à plusieurs titres, d'un soutien (« *backing* ») public, par le biais de mécanismes d'assurance et de dépôt ou d'un accès au refinancement de la banque centrale ;
- Par ailleurs, c'est la banque centrale qui émet la monnaie servant de « base » au système, ce qui lui confère son cours légal ;

La monnaie électronique et les paiements

De nombreux instruments permettent aujourd'hui d'utiliser et de mobiliser la monnaie de banque. S'agissant des paiements de détail, ces progrès ont donné naissance à de nouveaux supports : cartes bancaires, virements par Internet, monnaie stockée sur téléphones mobiles.

Qualifier ces supports de « monnaie électronique » peut donner à penser qu'ils sont différents de la monnaie « de banque » et que les crypto-monnaies s'inscrivent dans un continuum entre les différentes formes de monnaies électronique.

Cette double impression est trompeuse.

La monnaie électronique n'est pas une nouvelle forme de monnaie. Elle est une des formes modernes que prend la monnaie de banque. Techniquement, il ne s'agit pas de monnaie, mais d'instruments de paiement qui permettent de mobiliser et d'utiliser la monnaie de banque.

Les détenteurs de monnaie électronique sont parfois dispensés d'avoir eux-mêmes un compte bancaire et leurs avoirs sont conjointement regroupés dans le compte bancaire de l'opérateur. Leur identité bancaire se résume à leur numéro de téléphone. Il y a là un instrument puissant d'inclusion financière. Il n'est pas étonnant que ces innovations se développent particulièrement dans les pays émergents à faible bancarisation. Mais un téléphone mobile reflète toujours un compte bancaire : il doit être approvisionné (à partir d'un autre compte) pour être utilisable.

Les crypto-monnaies

Les crypto-monnaies sont fondamentalement différentes. Comme la monnaie de banque, elles n'ont aucune valeur intrinsèque, et sont totalement dématérialisées et digitales. Mais chacune de leurs autres caractéristiques se situe à l'opposé des monnaies existantes :

- Elles se créent et circulent indépendamment de toute banque et sont détachées de tout compte bancaire ;
- Elles ne représentent pas une créance sur une quelconque personne physique ou morale ;
- Il s'agit de monnaies purement privées, sans cours légal, qui ne sont convertibles au pair en aucune monnaie légale⁷ et ne bénéficient d'aucun soutien public, direct ou indirect ;
- Elles sont libellées en unités de compte spécifiques, sans rapport avec les monnaies existantes.

Au-delà de la prouesse technologique et de l'apparente proximité avec les monnaies électroniques, il est important de mesurer que les crypto-monnaies constituent une expérience monétaire sans réel précédent. Les formes de monnaie ont constamment évolué dans l'histoire, sous l'effet de la technologie, des institutions ainsi que des conventions sociales. Néanmoins, toutes les monnaies qui se sont développées et imposées dans les économies capitalistes possédaient l'une ou l'autre – ou plusieurs – des caractéristiques suivantes :

- Soit une valeur intrinsèque (les monnaies et pièces en métal précieux) ;
- Soit une contrepartie sous forme d'actif physique ou financier servant à gager leur valeur. C'est le cas de l'étalon-or. Ce fut également le cas, sous une forme différente, des billets émis aux États-Unis par des banques privées pendant la période de « *free banking* »⁸, et dont la valeur (au demeurant variable) était gagée par les actifs et le capital des banques émettrices ;
- Soit un soutien public, avec cours légal et refinancement par la banque centrale.

⁷ Si les crypto-monnaies ne sont pas convertibles au pair en monnaie légale, elles demeurent convertibles en monnaie légale suivant le taux de change de marché.

⁸ Entre 1837 et 1864.

Les crypto-monnaies qui circulent aujourd'hui n'ont aucun de ces trois attributs. Ce sont des objets monétaires totalement nouveaux. Pour cette raison, elles sont qualifiées de « virtuelles ». Il faut donc s'interroger, au-delà de leur volatilité actuelle, sur leur viabilité à long terme, tant d'un point de vue technologique qu'au regard de l'expérience monétaire qu'elles incarnent et représentent.

Les régimes d'émission

Les créateurs des crypto-monnaies ont accordé beaucoup d'importance et d'attention à leur régime d'émission. Ces régimes, assez divers, combinent un mélange de rigueur, d'ambiguïté et d'innovation aux conséquences parfois incertaines :

- la rigueur provient d'un encadrement de la quantité de monnaie émise. Celle-ci est souvent plafonnée, soit en montant final (Bitcoin), soit en taux de croissance (Ether), soit en montant initial (Ripple) ;
- l'ambiguïté vient des conditions dans lesquelles certains fondateurs se « réservent », à l'émission, une fraction du stock de crypto-monnaie. Quand cette fraction est significative, les fondateurs contrôlent directement l'émission effective de la monnaie en cause, dont la valeur dépendra des conditions de libération de la réserve. Ces conditions ne sont pas toujours clairement précisées lors de l'émission initiale. Sous l'hypothèse naturelle que les fondateurs maximiseront les profits qui en résultent, il se peut que les autres détenteurs se voient imposer des transferts ou des pertes ;
- de nouveaux régimes d'émission des crypto-monnaies se déploient. Certaines sont totalement adossées à un « panier » de monnaies avec cours légal, dont elles forment une représentation digitale. C'est le cas de Saga, créée en mars 2018 et adossée aux droits de tirage spéciaux (DTS), la monnaie interne du Fonds monétaire International (FMI). C'est aussi le cas de Tether, créé en 2016 et théoriquement adossé au pair au dollar pour une capitalisation de marché de 2,5 milliards de dollars. D'autres sont plus ambitieuses et visent à stabiliser automatiquement le taux de change de la monnaie virtuelle par rapport à l'une des grandes monnaies fiat. Ce sont les projets dits de « *stable coins* ». Pour ce faire, l'émission et la destruction de monnaies sont contrôlées par un algorithme qui réagit aux variations de cours. Dans les deux cas, la faisabilité des mécanismes restent à démontrer, de même que leur impact sur la stabilité monétaire et financière.

(...)

II. L'UNIVERS DES CRYPTO-MONNAIES

La dimension monétaire est importante dans le projet qu'incarnent les crypto-monnaies. Mais elle n'est pas exclusive. L'ambition est également, et peut-être d'abord, technologique et économique. Un véritable système de production et d'accompagnement se développe autour de l'activité des crypto-monnaies, dans laquelle la France possède de nombreux atouts. La blockchain elle-même offre de nombreuses perspectives. La possibilité de stocker et de transférer de la valeur sur des unités virtuelles, divisibles et fongibles (les « *tokens* ») peut changer le paysage de la finance, des échanges et de la production. Dans le foisonnement actuel d'initiatives et de projets, il est important de bien identifier les opportunités et d'en mesurer les risques.

A. Deux nouveaux horizons technologiques : la blockchain et la digitalisation de la valeur

1. Les applications et perspectives de la blockchain⁴⁹

L'innovation progresse par vagues successives, avec des phases d'accélération où la diffusion des idées suscite une mobilisation des initiatives, des énergies et des financements. C'est une telle phase que traverse aujourd'hui la technologie des DLT et de la blockchain, grâce, en partie au moins, à l'intérêt et l'engouement que suscitent les crypto-monnaies.

Celles-ci utilisent des blockchains publiques avec accès universel et, donc, des procédures très développées de consensus. Au contraire, beaucoup des applications « non monétaires », dans la finance et l'économie réelle, utilisent des blockchains privées, « avec permission », c'est-à-dire des réseaux fermés, avec un nombre limité de participants.

Ces blockchains privées se construisent autour d'architectures très diverses et présentent plusieurs avantages :

- Des procédures de consensus très allégées avec beaucoup moins de contraintes de validation, puisque les participants sont sélectionnés et se font mutuellement confiance. Les mouvements sont moins coûteux et plus rapides. La technologie peut alors rivaliser en performance avec celle des systèmes centralisés ;
- Une gestion flexible de la confidentialité : s'agissant des données individuelles, elle est souvent imposée par la loi ou la réglementation. Les règles d'accès doivent être conçues en conséquence. Il est possible que les personnes habilitées à « écrire » sur la blockchain – ou d'autres registres distribués – c'est-à-dire celles habilitées à la modifier et la mettre à jour, soient différentes de celles autorisées à la lire. La technologie, qui doit évoluer et se perfectionner, offre déjà une grande flexibilité d'adaptation ;
- Offrir un cadre de gouvernance et d'action collective entre partenaires qui veulent coopérer, mais dont aucun ne veut laisser le leadership aux autres. La blockchain peut servir de support à des projets de place.

Pour ces blockchains, ou registres distribués, fermés, on voit donc se développer aujourd'hui plusieurs voies prometteuses d'applications.

⁴⁹ Cette section s'inspire des travaux du CMBI (*The Potential Impact of Blockchain Technology on Finance: Small, Significant, or Completely Transformative*, en cours de publication) et de Lael Brainard, « *Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?* », 15 mai 2018.

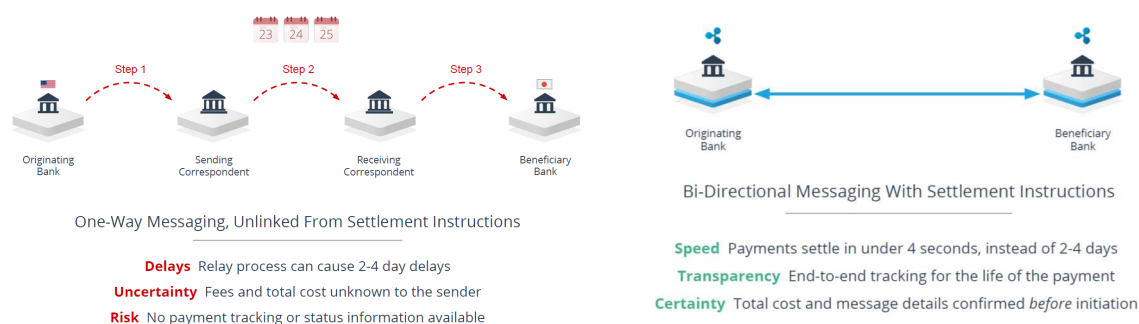
Là où les systèmes traditionnels sont peu efficaces ou peu compétitifs

C'est le cas des paiements transfrontières. Aujourd'hui encore, ces paiements empruntent le plus souvent des circuits complexes, mettant en jeu de nombreux intermédiaires et contreparties, y compris pour les opérations de change. Cette complexité accroît les coûts et multiplie les risques opérationnels. Comparées aux paiements domestiques, les transactions transfrontières restent longues et onéreuses pour les consommateurs, surtout pour les transferts de faibles montants.

Il est donc naturel qu'une fraction de ces paiements – transferts familiaux ou opérés par les migrants – s'effectue déjà par le biais des crypto-monnaies. Des systèmes de « *peer-to-peer* », opérant sans intermédiaire et pouvant fonctionner sur une infrastructure Internet existante, se révèlent très compétitifs.

Plusieurs développements sont en cours. Ripple est un protocole de paiement, décentralisé et semi-fermé, dont la technologie (DLT plus une forme allégée de la blockchain) et la propre crypto-monnaie (dénommée XRP) permettent la transmission très rapide de messages de paiement, dans toutes les monnaies (crypto ou officielles) entre toute localisation dans le monde. Ripple est de plus en plus utilisé, y compris par les banques internationales et systèmes de paiements.

Protocole de paiement offert par Ripple pour les transactions interbancaires



Source : Ripple, Transforming global payments, avril 2018.

La plateforme distribuée Corda, développée par le consortium R3, auquel participent des banques françaises, est gérée conjointement par un nombre limité de participants (avec des « validateurs » désignés). Elle rassemble 22 banques dans le double objectif de développer et de tester ses possibilités de paiements transfrontières en temps réel (*real time settlements*) et ce, grâce à l'interopérabilité des réseaux blockchains.

Ces évolutions ont poussé SWIFT, le système mondial de messagerie pour paiements interbancaires à développer son propre système le « *Global Payments Innovation Initiative* » (GPI). En cours de test avancé et de commercialisation auprès de 73 banques participantes, cette initiative propose une utilisation des fonds le jour même, une transparence et prévisibilité des frais, le suivi des paiements de bout en bout et un transfert d'informations de paiement plus riches. Le 24 mai 2018, SWIFT a annoncé qu'un quart des paiements transfrontières qui lui étaient confiés étaient désormais réalisés par l'intermédiaire de GPI, soit un peu plus de 100 milliards de dollars par jour et une moitié des paiements réalisés en moins de trente minutes. C'est un exemple extrêmement significatif des progrès qui peuvent être réalisés quand la technologie, se développant dans un environnement concurrentiel, suscite et impose l'innovation.

Là où la résilience aux cyber-attaques est importante

Le grand avantage des registres distribués est leur redondance naturelle. L'ensemble des données est disponible en plusieurs points du réseau. Ils permettent à un système de continuer à fonctionner quand certains de ses éléments sont compromis. Tous les systèmes de paiement et de règlements de gros montants ont besoin de cette robustesse. Elle est aujourd'hui assurée, pour les registres centralisés, par la duplication de tous les éléments essentiels. Une technologie DLT peut apporter des économies substantielles à cet égard.

Là où apparaissent des points de congestion opérationnelle

Les processus industriels et financiers sont des systèmes complexes, dont les acteurs sont nombreux et doivent se coordonner en permanence. Chaque étape peut nécessiter le recueil et la réconciliation de données avant de passer à l'étape suivante. Si des délais de transmission apparaissent, la congestion s'installe et les coûts augmentent. Disposer d'une base de données distribuée permettant de partager en temps réel une information constamment mise à jour procure des gains d'efficacité.

Toutes les opérations de règlement et de livraison de titres nécessitent de telles réconciliations, mobilisant séquentiellement plusieurs intervenants et s'avérant ainsi très coûteuses en ressources et en temps. Ces réconciliations peuvent durer plusieurs jours – retardant d'autant la certitude de la finalité de la transaction et générant un risque de contrepartie. Un registre distribué, actualisé en temps réel, permet aux acteurs de partager à tout instant une vue commune de l'état du système, ce qui accélère le processus et réduit les risques d'erreur⁵⁰.

Un champ d'application plus complexe, mais prometteur, paraît être la gestion des prêts aux entreprises ainsi que l'émission de titres par celles-ci. La documentation juridique, les flux d'intérêt, les procédures d'amendement et de réconciliation sont parfois encore opérées manuellement sur la base d'échanges d'informations par e-mail, avec de nombreuses réconciliations préalablement à tout paiement (Genève).

Le financement du commerce international (*trade finance*) sera significativement transformé par la blockchain. Il repose sur la coordination de nombreux intervenants (armateurs, autorités portuaires, compagnies d'assurances, banques, autorités douanières) qui, tous, jouent un rôle dans la chaîne de traitement et d'exécution d'une transaction transfrontière (import-export). Pour que la chaîne fonctionne, il faut que tous les acteurs puissent tout à la fois localiser les biens couverts et suivre leur évolution. Le partage en temps réel d'un même registre distribué entraînera d'immenses gains d'efficacité.

La même logique s'applique aux « *supply chains* » autour desquelles s'organisent l'internationalisation et la division de la production industrielle. Dans ces véritables « usines transfrontières » (Baldwin), la capacité (procurée par la blockchain) à suivre en temps réel les flux de produits et à coordonner par la même information l'action de centaines de sous-traitants est source de gains majeurs de productivité.

Un enregistrement daté et immuable des données et événements, notamment pour des raisons juridiques et de sécurité

Les progrès de la cryptographie permettent, dans ce cas, de préserver la confidentialité des données ainsi authentifiées, d'en réserver l'accès aux personnes autorisées et, surtout, de vérifier l'authenticité des informations sans prendre connaissance de leur contenu.

Des institutions financières s'apprêtent ainsi à rationaliser la gestion de leurs obligations administratives au regard de la lutte contre le blanchiment et le financement du terrorisme (*know your client* ou KYC). Les données individuelles et attestations certifiées stockées sur une blockchain pourront ainsi être « exportées » par leur titulaire à destination d'autres institutions, selon un processus assurant la confidentialité tout en préservant la certification. D'importantes simplifications et économies sont à attendre.

La même possibilité (partager en toute confidentialité des informations certifiées) peut permettre des améliorations majeures dans la gestion des dossiers individuels de santé. Chaque patient, pourrait conserver et actualiser, sous sa responsabilité, son dossier individuel sur un blockchain, avec les informations certifiées par les médecins ordonnateurs. Ce dossier pourrait être communiqué aisément, au moyen de clés cryptographiques, en totalité ou en partie, à ceux des professionnels de santé pour lesquels il serait nécessaire dans le respect du secret médical, garanti par la cryptographie.

D'autres usages émergent pour tirer parti du double avantage de la confidentialité et de l'authenticité des données qu'offre un registre distribué. En effet, alors que l'usurpation d'identité – numérique ou bancaire – est un mal endémique, la blockchain permet de :

- se prémunir contre la falsification de l'état civil, des titres de propriété (cadastre), des droits d'auteurs et de certificats divers ;
- suivre les transactions liés au transfert de ces droits, afin d'en établir la propriété en temps réel ;
- s'assurer de la parfaite identification des auteurs à l'origine de ces transactions.

Enfin, les blockchains les plus récentes supportent l'exécution de « smart contracts »

On désigne par « *smart contracts* » la version « blockchain » d'applications déjà anciennes, dans lesquelles un algorithme exécute automatiquement des opérations entre personnes différentes à la réception d'informations spécifiées (les « oracles »). Dans les blockchains associées à des monnaies, ces *smart contracts* opèrent des transferts d'unités de valeur entre les participants.

Les *smart contracts* ne sont généralement pas des contrats, au sens juridique du terme, mais l'application par protocole et par algorithmes de conventions conclues entre les participants.

L'intérêt des *smart contracts* vient de ce qu'ils ne nécessitent l'intervention d'aucune tierce partie. L'exécution s'opère sur la blockchain dès que les conditions sont réalisées. Il faut toutefois qu'il n'existe aucune ambiguïté sur l'interprétation de ces conditions et qu'aucun jugement humain ne soit nécessaire préalablement à l'exécution du contrat.

Sous ces limites, les *smart contracts* peuvent connaître des applications nombreuses, notamment dans le secteur financier (gestion du collatéral, appels de marges, paiements d'intérêts, etc.). Il est possible que les clauses d'exécution de nombreux contrats dérivés (en tout cas les plus standardisés) soient insérées, à l'avenir, dans des *smart contracts*.

2. La digitalisation de la valeur

Au-delà de la blockchain, les crypto-monnaies annoncent une autre innovation, moins publiquement soulignée, mais plus importante encore : la digitalisation de la valeur et des actifs. La technologie offre la capacité de représenter numériquement de la valeur et à la transférer en toute sécurité entre individus sans aucun intermédiaire – constituant ainsi une sorte de « billet de banque » digital. Les représentations digitales de valeur sont couramment appelées des « jetons » ou plus fréquemment encore, par leur nom anglais, des « *tokens* ». La cryptographie moderne permet, le cas échéant, de faire cette opération de manière anonyme. On peut donc créer des monnaies et des actifs financiers digitaux « au porteur ».

⁵⁰ Lael Brainard, « *Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?* », 15 mai 2018.

Les potentialités et les risques de la digitalisation de la valeur

Les applications sont multiples. Les crypto-monnaies, qui sont des « tokens » monétaires, sont l'exemple le plus connu. Mais tout actif, réel ou financier, peut potentiellement être digitalisé. La *tokenisation* pourrait s'avérer particulièrement prometteuse pour les actifs rares et peu liquides, dont la valorisation est pénalisée par la faible profondeur de marché dans des proportions importantes. Sont notamment concernés l'immobilier commercial et résidentiel, le *private equity* ou bien encore les œuvres d'art. Dans ce cas d'espèce, des particuliers seront en mesure d'acquérir collectivement un tableau de valeur grâce à l'achat de *tokens*, bien qu'aucun d'entre eux ne soit individuellement en mesure d'acheter seul ce tableau.

Selon une étude du Nasdaq⁵¹, la digitalisation s'appliquerait particulièrement bien à deux grandes catégories d'actifs :

- les actifs incorporels, que sont notamment les brevets, les droits carbone ou bien encore les droits d'auteur. Compte tenu de leur absence d'existence physique, ces actifs apparaissent plus faciles à convertir en *tokens*, bien que les différences de juridictions puissent rendre leurs transferts ultérieurs difficiles ;
- les actifs fongibles, susceptibles de se prêter plus facilement au processus de tokenisation, dans la double mesure où ils peuvent le plus souvent être divisés en plusieurs unités et où l'ensemble des *tokens* peuvent ensuite être associés à un ensemble général de composants d'actifs interchangeables (par exemple, dix kilos d'or).

En convertissant en tokens des actifs rares ou faiblement liquides, la digitalisation ouvrira les marchés correspondants à davantage d'investisseurs et accroîtra le volume global d'échanges. Le développement de la « *tokenisation* » est parfois présenté comme inéluctable, un mouvement dans lequel Internet a vocation à devenir à terme le plus grand marché d'actifs du monde, aussi sûrement qu'Internet est devenu la plus grande bibliothèque du monde. La digitalisation des actifs sous forme de jetons ne fait que prolonger la digitalisation de l'information permise par Internet.

Les risques, bien évidemment, sont à la hauteur des opportunités que présentent ces formes de « titrisation digitale ». Ils apparaissent à deux niveaux :

- Celui de la gouvernance et de la sécurité juridique : attacher (et faire respecter) des droits définis dans des législations nationales à des actifs immatériels circulant sur Internet est un défi non résolu. Ceci d'autant plus que, théoriquement, plusieurs types de droits peuvent être attachés et transférés aux jetons : droits d'usage et non de propriété, comme dans le cas des baux, droits incorporels, comme les droits musicaux. L'exercice des droits inscrits sur un jeton suppose d'en connaître le détenteur effectif, de manière formelle et inconstable. C'est possible sur une blockchain mais plus complexe dans d'autres cas. En l'absence de cadre juridique et de règles de gouvernance, tous les abus sont aujourd'hui possibles et probables ;
- Celui de la stabilité financière : en émettant des jetons échangeables en contrepartie d'actifs illiquides, on procède en fait à une activité de transformation, dont les risques sont bien identifiés et connus. En particulier, les jetons liquides sont exposés à des « *runs* », dans lesquels la perte subite de confiance conduit à un afflux de demandes de conversion en actifs sous-jacents illiquides qui ne peut être satisfait. Les crypto monnaies adossées à des actifs physiques ou financiers, dont la création est envisagée par de nombreux entrepreneurs, sont particulièrement exposées à ce risque.

⁵¹ Addison Cameron-Huff, *How Tokenization Is Putting Real-World Assets on Blockchains*, 30 mars 2017.

Les ICO, reflet des ambiguïtés de la digitalisation de la valeur

Les ICO (*Initial Coin Offerings*) reflètent parfaitement les opportunités et les ambiguïtés de la digitalisation des actifs. Cette pratique de levée de fonds sur Internet – apparue en 2016- est en développement rapide dans un environnement de liquidité abondante. Elle cumule deux grandes novations par rapport aux émissions traditionnelles :

- la procédure d'appel à l'épargne : La procédure des ICO reproduit, dans ses principales étapes, celle des émissions d'actions, mais sans aucune des formalités et garanties dont s'accompagne celle-ci. Il n'y a pas de prospectus visé par les autorités boursières, mais simplement un document (le « *White Paper* ») posté sur Internet, qui n'engage pas juridiquement l'émetteur – lequel parfois n'est même pas établi en tant que société – et n'est pas standardisé. Ce mode d'émission préfigure sans doute l'avenir mais n'offre aujourd'hui aucune garantie réelle aux souscripteurs ;
- la nature très variée des droits que confèrent les « jetons » émis : beaucoup d'acteurs privés et publics tentent aujourd'hui de promouvoir une classification entre jetons dits « financiers » et jetons dits « d'utilité ». En réalité, ces jetons d'utilité sont très ambigus. Il est probable que dans plus de trois-quarts des cas, l'émission de tels jetons est en réalité celle d'une nouvelle crypto-monnaie destinée au paiement de services qui n'existent pas encore, dont l'apparition est subordonnée au succès du projet et dont le prix futur est inconnu. Ce sont donc des produits particulièrement risqués, qui cumulent plusieurs niveaux d'aléas, mais dont la plupart sont néanmoins « cotés » sur des plateformes d'échange.

Les ICO ont connu un succès croissant à compter de l'été 2017 : le montant total des levées de fonds par ICO dans le monde a représenté entre 4 et 6 milliards de dollars en 2017 (les sommes levées se concentrant principalement sur les derniers mois de l'année), contre 100 millions de dollars en 2016. Par comparaison, l'investissement réalisé par les fonds de capital-risque dans le premier tour de financement de start-ups a représenté, à l'échelle mondiale, 13 milliards de dollars en 2017.

Tableau 1 : Baromètre des ICO en France et dans le monde au 31 décembre 2017

ICO	Monde ⁵²	France ⁵³	France (en % du monde)
Nombre	372	16	4,30
Montants levés à l'émission (en milliards de dollars)	4,00	0,13	3,25

Source : Mission.

Les volumes émis par ICO ont continué d'augmenter depuis le début de l'année 2018, le total des fonds levés entre le 1^{er} janvier et le 1^{er} juin s'élevant à 9,5 milliards de dollars⁵⁴, soit près de 2 milliards de dollars par mois.

Au total, les émissions de *tokens* se répartissent assez également entre l'Amérique du Nord, l'Europe et l'Asie⁵⁵, avec toutefois un pays dominant : la Suisse, où 25 % des ICO mondiales ont été réalisées. Le canton de Zoug, a été surnommé la « *Crypto Valley* » par sa position de « *hub* » de référence dans le monde sur les crypto-monnaies. De son côté, l'Asie compte plusieurs pays particulièrement dynamiques, tels que la Corée du Sud, Singapour, le Japon, la Chine et Hong-Kong.

⁵² EY research, *Initial coin offerings (ICOs)*, décembre 2017.

⁵³ Avolta Partners, *Baromètre des ICO en France*, juin 2018.

⁵⁴ Chain Tech et France digitale, *Towards a regulatory framework on crypto-assets*, juin 2018.

⁵⁵ Voir visuellement la répartition géographique des montants levés en ICO : <https://elementus.io/blog/token-sales-visualization>.

Encadré 3 : Panorama des ICO réalisées en France entre 2014 et 2018

On estime aujourd'hui à 16 le nombre d'ICO domiciliées en France et possédant une équipe française, à la date du 1er juin 2016. Le montant total des fonds levés à l'émission s'élève à 130 millions de dollars, aujourd'hui valorisés à 340 millions de dollars sur le marché. Le montant moyen d'une ICO française s'établit ainsi à 8,1 millions de dollars à l'émission et à 21,4 millions de dollars une fois prise en compte la valorisation de marché. Par comparaison, la plus grosse ICO réalisée et connue à ce jour à l'étranger, en l'espèce Telegram, a permis de lever 850 millions de dollars.

Sur ces 16 ICO domiciliées en France, la détention des jetons émis est très concentrée, puisque deux tiers des jetons offerts sont détenus par dix souscripteurs seulement. Il convient à cet égard de souligner qu'en moyenne seuls deux tiers des jetons sont offerts à l'émission, le reste demeurant en réserve.

Les jetons émis sont à 70 % des jetons d'utilité ou « *utility tokens* », contre 25 % pour des jetons de titre ou « *security tokens* ». Les jetons émis le sont également dans plus de la moitié des cas (56 %) sur une blockchain hybride, contre un quart sur une blockchain publique et un peu plus de 6 % sur une blockchain privée.

La liquidité des jetons émis par ICO est aujourd'hui relativement faible, puisque le volume de *tokens* échangés sur le mois de mai 2018 ne représente, en moyenne quotidienne pondérée, que 0,6 % du nombre total de *tokens* en circulation. Le ratio de liquidité varie toutefois très fortement d'un jeton à l'autre, puisqu'il va de 0,1 % à 8,91 %.

Peu liquides, les jetons émis voient également leur prix être particulièrement volatiles. En effet, le multiple de volatilité, mesuré par le rapport entre le prix maximal et le prix minimal, s'établit en moyenne à 6,6 et varie très fortement (allant de 0,2 à 285), attestant de la non-maturité du marché.

Source : Mission, d'après une étude réalisée par Avolta Partners.

Les technologies qui sous-tendent les ICO sont encore dans une phase d'apprentissage, et les acteurs et projets sont souvent éphémères. Selon une étude de l'Académie chinoise des technologies de l'information et de la communication (CAICT) rendue publique le 28 mai 2018, sur les 80 000 projets « blockchain » lancés dans le monde, seuls 8 % d'entre eux sont encore actifs à ce jour, les start-ups développant de tels projets ayant une durée de vie moyenne de 450 jours, soit 1,25 année. Sur les 902 start-ups ayant lancé une ICO en 2017, 46 % d'entre elles ont d'ores et déjà disparu, selon une étude réalisée par le site Bitcoin.com. Le fondateur d'Ethereum, M. Vitalik Buterin, a publiquement reconnu que neuf start-ups sur dix émettant des *tokens* sont vouées à l'échec.

Les Jeux olympiques de 2024, terrain d'expérimentation de la digitalisation de la valeur

Si la digitalisation de la valeur pose des défis importants aux régulateurs, elle est avant tout porteuse d'opportunités majeures pour la sphère économique, mais également pour la sphère publique. Mieux appréhender et, le cas échéant, réguler les applications dont les crypto-monnaies sont porteuses, exigent des entités publiques qu'elles soient elles-mêmes en capacité d'anticiper et de s'approprier les développements technologiques à venir. Si les administrations et les régulateurs ont d'ores et déjà investi dans les technologies liées la blockchain (notamment la Caisse des dépôts et consignations ainsi que la Banque de France), elles peinent à en appréhender toutes les potentialités, en particulier celles liées à la digitalisation de la valeur.

De simples investisseurs dans la blockchain, les autorités publiques doivent prendre le leadership et se muer en véritables développeurs de nouvelles applications permises par la blockchain, telles que la digitalisation de l'accès à un service donné. En effet, développer de telles applications offrira aux acteurs publics la possibilité d'incuber les évolutions technologiques les plus récentes et de mieux en appréhender les risques et les opportunités.

Des expérimentations peuvent, à cet égard, être envisagées à brève échéance. Ainsi, sous réserve de leur engagement ou de leur participation à la réalisation d'un service public, les usagers pourraient se voir distribuer en retour des *tokens* qu'ils pourraient échanger contre l'accès à un autre service. Parce que l'amélioration de la propreté dans les grandes villes passe par l'engagement de ses habitants, ceux-ci pourraient par exemple, en contrepartie de la réalisation d'opérations volontaires de nettoyage, se voir rétribuer par l'octroi de *tokens* qu'ils pourraient ensuite convertir pour accéder à une offre de vélos ou de voitures en libre-service.

Afin de toucher un public plus large, les autorités publiques pourraient s'engager à digitaliser une partie de la billetterie des Jeux olympiques organisés par la France en 2024. Les *tokens* donnant accès à cette cérémonie seraient émis sur une blockchain au bénéfice des personnes ayant contribué à la préparation et à l'organisation d'événements populaires autour des jeux. Ces *tokens* pourraient être ensuite échangés de manière transparente sur cette même blockchain, sécurisant ainsi les transactions et réduisant d'autant les risques liés à la revente au marché noir, à la contrefaçon ainsi qu'à la fraude.

C. Des risques circonscrits qui doivent le rester

Un faible risque pour la stabilité financière globale

À ce stade, les risques pour la stabilité financière ne paraissent pas avérés, ainsi que l'a confirmé le rapport du FMI sur la stabilité financière dans le monde, publié le 9 avril 2018. Le FMI note toutefois que « *si leur utilisation des monnaies virtuelles devait se généraliser en l'absence de garde-fous satisfaisants, la donne pourrait changer* ». Plusieurs facteurs permettent d'affirmer que le risque que les crypto-monnaies font peser sur la stabilité financière globale est aujourd'hui faible.

Les sommes en cause restent peu importantes

La valeur de capitalisation des crypto-monnaies est actuellement relativement faible comparativement au poids du système financier global : avec 432 milliards de dollars au 22 février 2018, ces instruments représentent 1,5 % seulement de la capitalisation de marché de l'indice S&P500 et 5,5 % de la valeur total du marché de l'or. Les crypto-monnaies ont également une taille de marché bien inférieure à celles des récentes bulles spéculatives⁷².

L'exposition du secteur financier traditionnel reste limitée à ce stade

Les crypto-monnaies ne présentent pas de risque systématique du point de vue de la stabilité financière globale, compte tenu de leur intégration encore limitée à ce jour au système financier traditionnel ainsi que dans les produits financiers existants (ETF, dérivés, *futures*).

L'exposition des institutions et acteurs financiers traditionnels aux risques liés aux crypto-monnaies pourrait prendre plusieurs formes :

- la détention directe de crypto-monnaies par les institutions financières, soit au titre d'opérations en comptes propres, soit dans le cadre de la conservation de crypto-actifs pour comptes de tiers ;
- l'octroi de crédit et de facilités financières aux plateformes d'échanges et aux *wallet providers* pour financer la croissance de leurs activités ;
- l'octroi de crédits aux entreprises acceptant les crypto-monnaies comme moyen de paiement ainsi qu'aux particuliers investissant dans ses instruments, exposant les établissements prêteurs à un risque de crédit ;

Selon le *Financial Security Board* (FSB), il n'existe aujourd'hui aucune indication attestant d'une éventuelle exposition des banques et des acteurs financiers traditionnels aux crypto-monnaies. Il n'en demeure pas moins important de préserver cette étanchéité à l'avenir.

Les vulnérabilités se développant au sein de la sphère des crypto-monnaies y restent circonscrites

⁷² Ainsi, lors de la bulle spéculative dite « Dotcom » (1997-2001), les valeurs technologiques ont atteint jusqu'à 3 000 milliards de dollars. Dans la période précédant l'éclatement de la crise des *subprimes*, le volume total de prêts hypothécaires titrisés était de 7 300 milliards de dollars.

Le système des crypto-monnaies a vu apparaître en son sein des vulnérabilités qui, si elles y restent aujourd'hui circonscrites, n'en méritent pas d'être soulignées et surveillées par les régulateurs :

- la volatilité, vingt-cinq fois plus élevée que celle du marché américain des actions, cinq fois plus forte que celle des matières premières et douze fois supérieure à celle du yen. Cette volatilité à laquelle les investisseurs sont exposés rend particulièrement difficile l'utilisation des crypto-monnaies en tant que moyen de paiement et menace la viabilité des plateformes d'échange (« *flash crashes* ») ;
- le recours au prêt pour l'achat de crypto-monnaies : on estime ainsi à 20 % la part des utilisateurs ayant recours à la dette pour financer leurs achats de crypto-monnaies soit au moyen de cartes de crédit ou de prêts hypothécaires⁷³, soit au moyen de prêts ayant des crypto-actifs pour collatéral⁷⁴ ;
- les effets de levier, qui amplifient la transmission des risques à l'économie réelle, car les investisseurs disposent alors de moins de capital pour absorber les pertes en cas de fluctuations de marché. Ainsi, les opérations sur marge (ou « *margin trading* ») avec effet de levier sont actuellement autorisées sur les crypto-monnaies dans un certain nombre de pays⁷⁵.

Encadré 6 : Effets de leviers sur les principales plateformes d'échange de crypto-monnaies

La plateforme d'échange américaine, Poloniex, offre à ses clients des opérations sur marge avec un effet de levier de 2,5, effet de levier qui peut s'élever à 100 fois la mise initiale sur la plateforme Bitmex basée aux Seychelles. La plateforme japonaise, Bitflyer, offre pour sa part un effet de levier atteignant jusqu'à 15 fois le dépôt en cash de ses clients.

Le montant total des contrats bénéficiant de cet effet de levier sur les plateformes n'est pas connu. Les entités susceptibles de financer ce levier ne sont pas davantage connues. Certains régulateurs ont toutefois fait état de plateformes offrant des prêts aux investisseurs.

Source : Financial Stability Board (FSB).

- le développement produits dérivés et d'instruments d'échange à terme (swaps) portant sur des crypto-monnaies : contrairement aux premiers, les seconds impliquent la livraison effective de crypto-actifs et, par voie de conséquence, leur détention et leur comptabilisation au bilan, avec le risque sous-jacent d'une transmission plus facile de la volatilité de ces actifs et du risque afférent à l'économie réelle.

Un risque de perte de confiance en cas d'effondrement rapide et général

Un choc négatif au sein de la sphère des crypto-monnaies pourrait affaiblir durablement la confiance que le public place aujourd'hui dans le système financier et ses infrastructures de marché. En effet, si les institutions financières traditionnelles venaient à être davantage exposées aux crypto-monnaies et si les craintes sur la viabilité de celles-ci venaient à se matérialiser, la confiance placée par les épargnants et les investisseurs dans le système financier en serait durablement amoindrie.

Ainsi, une brutale perte de valeur des crypto-monnaies, sous l'effet des fluctuations de marché, de la fraude ou de l'action des régulateurs, ferait peser sur l'ensemble du système financier un fort risque réputationnel. Par conséquent, il est essentiel pour les régulateurs – dont la crédibilité ne manquerait pas d'être mise à l'épreuve en cas d'effondrement rapide et général – d'avoir un discours ferme et clair sur la nécessité de limiter l'exposition des acteurs financiers traditionnels aux crypto-monnaies.

⁷³ Michelle Fox, "People are taking out mortgages to buy bitcoin, says securities regulator," CNBC, 11 décembre 2017.

⁷⁴ Olga Kharif, "These Guys Want to Lend You Money Against Your Bitcoin," Bloomberg, 14 décembre 2017.

⁷⁵ Yuval Gov (2018), "Bitcoin and Altcoins margin trading for beginners," January.

Les risques liés à l'anonymat et à la lutte anti-blanchiment

Les crypto-monnaies peuvent être utilisées, dans certains cas, pour dissimuler l'origine ou la destination des fonds. En effet, les mécanismes anonymes et décentralisés d'émission et de transfert de la plupart des crypto-monnaies peuvent favoriser l'utilisation de ces instruments à des fins criminelles (vente sur Internet de biens ou services illicites) ou à des fins de blanchiment ou de financement du terrorisme.

Les risques d'usage des crypto actifs à de telles fins sont liés au fait que les détenteurs de monnaies virtuelles ne sont pas identifiés, les clés privées de détention des crypto actifs étant en effet anonymes. Par analogie, cela revient à une situation dans laquelle aucun nom ne correspondrait à un IBAN, mais que toutes les opérations réalisées avec cet IBAN seraient visibles par tous.

En France, l'organisme de traitement du renseignement et d'action contre les circuits financiers clandestins (Tracfin) identifie l'utilisation de crypto-monnaies, comme étant à l'origine d'un risque spécifique en matière de blanchiment des capitaux et de financement du terrorisme. Cet organisme a ainsi reçu des banques, en 2017, quelques 351 déclarations de soupçon liées à l'utilisation des crypto-monnaies, contre 28 seulement en 2014.

Encadré 7 : L'activité de Tracfin en matière de crypto-monnaies

En 2016, Tracfin a reçu 178 déclarations de soupçon directement liées à des transactions en monnaie virtuelle pour un total de près de 5 M€.

Dans plus de la moitié des cas, l'utilisation de monnaies virtuelles (achat ou vente) est l'élément à l'origine de la déclaration de soupçon. La majorité des déclarations ont pour motif un doute sur l'origine ou la destination de fonds sans caractérisation précise du soupçon.

Les phénomènes les plus régulièrement recensés par les déclarants sont des cas d'intermédiation ou d'exercice illégal d'une profession réglementée. Ces dossiers font état d'individus collectant des fonds en provenance de nombreux particuliers dans le but de procéder à des opérations d'achat/revente de monnaies virtuelles sur des plateformes d'échange européennes pour le compte de tiers.

Source : Rapport annuel d'activité de Tracfin pour 2016.

À ce jour, si les cas de blanchiment d'argent au moyen de crypto-monnaies demeurent peu documentés et les cas répertoriés de financement du terrorisme par le biais de ces instruments demeurent relativement anecdotiques, le groupe d'action financière (GAFI) a récemment souligné l'utilisation croissante de ces produits à des fins criminelles. Outre le trafic de drogue à petite échelle et la fraude, le lien entre les crypto-monnaies et d'autres crimes semblent, en effet, se développer selon les conclusions du GAFI⁷⁶.

Les risques associés à l'usage du cash sont sans commune mesure avec ceux associés aux crypto-monnaies. Comme l'a indiqué Europol, « *bien que tous les usages du cash ne soient pas criminels, tous les criminels utilisent du cash à un moment donné dans le processus de blanchiment d'argent* »⁷⁷, ce qui n'est pas le cas avec les crypto-monnaies. Europol a également précisé que l'utilisation à des fins criminelles des crypto-monnaies exige toujours le recours au cash, soit pour l'encaissement, soit pour le décaissement des sommes en jeu.

Dans ce prolongement, le GAFI considère que les risques les plus significatifs en matière de lutte anti-blanchiment et de financement du terrorisme sont concentrés aux interfaces de conversion entre crypto-monnaies et monnaies ayant cours légal, soulignant ainsi la nécessité de réguler notamment les plateformes d'échange et autres intermédiaires de conversion.

⁷⁶ GAFI, *Rapport au G20*, juillet 2018.

⁷⁷ Europol, *Why is cash still a king? A strategic Report on the use of cash by Criminal groups as a facilitator for money laundering*, 2015.

L'Union européenne, dans sa dernière analyse supranationale des risques liés au blanchiment de capitaux et au financement du terrorisme en date de juin 2017⁷⁸, estime qu'en matière de lutte contre le blanchiment et de financement du terrorisme, les risques liés au cash sont « très significatifs », alors que ceux liés aux crypto-monnaies sont « modérément significatifs ». De ce point de vue et même du point de vue de la lutte contre la criminalité en général, l'analogie entre crypto-monnaies et cash n'est pas parfaite.

De fait, les rares études réalisées en la matière montrent que les activités illicites représentent une fraction limitée des échanges de bitcoins. Le *think tank* américain « Fondation pour la défense de la démocratie » a publié en janvier 2018 une étude détaillée sur le réseau Bitcoin de 2013 à 2016. Ses résultats montrent que les fonds d'origine illicite représentent moins de 1 % du volume des transactions du réseau Bitcoin, et qu'ils n'ont fait que diminuer au fil des années pour atteindre 0,1 % sur la dernière année considérée⁷⁹. Une étude d'Europol corrobore pour partie ce constat : l'agence européenne estime ainsi que la part des transactions en bitcoins liées à un commerce illégal représentent 3 % à 6 % de l'ensemble des transactions.

L'intégrité des marchés et la protection des épargnants

Bien qu'assez peu souligné, le risque d'intégrité des marchés est un risque essentiel. L'enthousiasme pour la technologie des registres distribués et de la blockchain n'incite, en effet, pas au discernement et à la discrimination entre les produits. Il s'agit en cela d'un phénomène similaire à celui observé lors de la bulle dite « dot.com » dans les années 2000.

Aggravé par les conditions monétaires et financières accommodantes, le risque d'intégrité des marchés tient également pour une large part à l'écosystème des crypto-monnaies, à la fois opaque et très évolutif, avec des acteurs souvent mal identifiés et particulièrement mobiles.

En outre, la cyber-sécurité reste pour les investisseurs et les épargnants une préoccupation majeure. En effet, la conservation des crypto-actifs est confrontée à des cyber-risques importants, comme en attestent les risques avérés de piratage des portefeuilles électroniques assurant le stockage des crypto-actifs.

Dans ce contexte, les détenteurs n'ont aucun recours en cas de vol de leurs avoirs par des pirates informatiques. Les épisodes répétés de fraudes importantes (piratage de Coincheck en janvier 2018 pour 534 millions de dollars américains, faillite retentissante en 2015 de la première plate-forme mondiale d'échange de bitcoin, MtGox⁸⁰), illustrent la vulnérabilité de l'écosystème des crypto-actifs et le niveau élevé des risques associés, en l'absence de mécanismes de garantie.

Le phénomène des ICO n'échappe pas à cette préoccupation de cyber-sécurité. Dans une étude de janvier 2018, le cabinet Ernst & Young a estimé que plus de 10 % des fonds levés par ICO avaient été soit perdus, soit volés à la faveur d'attaques de pirates informatiques. Ainsi, sur 372 ICO étudiées pour un total de 3,7 milliards de dollars levés, 400 millions de dollars ont disparu.

Le contournement des contrôles de capitaux et de changes

Si les crypto-monnaies facilitent les paiements transfrontières, en particulier dans les pays émergents, elles offrent, en contrepartie, la possibilité de contourner les règles nationales en matière de contrôle de capitaux et de changes.

(...)

⁷⁸ http://ec.europa.eu/newsroom/document.cfm?doc_id=45653

⁷⁹ <http://www.defenddemocracy.org/media-hit/yaya-j-fanusic-bitcoin-laundering/>

⁸⁰ À la suite d'une fraude interne ayant entraîné le détournement de 650 000 bitcoins pour une contrepartie d'environ 360 millions de dollars américains.

Benoît Cœuré and Jacqueline Loh: Bitcoin not the answer to a cashless society

Op-ed by Mr Benoît Cœuré, Chair of the Committee on Payments and Market Infrastructures (CPMI), and Ms Jacqueline Loh, Chair of the Markets Committee, published in the Financial Times under the title "Bitcoin not the answer to a cashless society", 13 March 2018.

* * *

Digital token reveals the weakness of our current payment systems

Next week, finance ministers and central bankers from the group of G20 countries will discuss bitcoin and other blockchain-based digital tokens. Such cryptocurrencies are poor imitations of money. Almost nobody prices goods in bitcoin, few use them for payments, and, as a store of value, they are no better than gambling in a casino. Policymakers are rightly worried about consumer and investor abuses, as well as illicit use.

Yet, while bitcoin and its cousins are something of a mirage, they might be an early sign of change, just as Palm Pilots paved the way for today's smartphones. Cash will not be king forever, even though it still rules in many parts of the world. New research from the Bank for International Settlements (BIS) shows non-cash payments have roughly doubled in size, as a share of GDP, since the turn of the century. Some Nordic countries are already cutting back on cash. And the iGeneration is more likely to reach for a payment app than a purse. To their children, banknotes and coins may look like museum exhibits.

These trends have sparked a discussion about whether central banks should issue their own digital coinage. A new report on central bank digital currencies (CBDC), released by the two committees we chair at the BIS, sets the scene for this important debate.

What is a CBDC? The answer goes to the heart of money and payments. Today, banknotes and coins are the only way consumers can access central bank money. The money in your bank account is actually provided by a commercial bank. Your bank promises to exchange that money for cash when you go to the ATM. But when you pay bills online or swipe your credit card, you are using commercial bank money.

Under the current system, only financial institutions have direct access to digital central bank money via accounts at their national central bank. A consumer-oriented CBDC would extend that access to everyone. Although this might not seem like a big step to digitally savvy consumers, it could have far-reaching ramifications for the role of money, the financial system and the economy.

For example, a CBDC for all would challenge the current model of banks taking customer deposits and using that money to fund the lending that helps drive the economy. The consequences for bank business models and financial stability would need to be carefully parsed. More fundamentally, do we need a CBDC? Existing payment arrangements – based on commercial money – are already digitally provided and increasingly convenient, instantaneous and available 24/7. Nevertheless, if cash disappeared, there would be a stronger case to consider a CBDC. Otherwise, the public would be wholly dependent on commercial money, and trust in the currency, a key public good, would be reliant on the creditworthiness of commercial entities and on specific payment technologies. However, despite the growing popularity of electronic payments, the cashless society is not here yet. Demand for bank notes is still growing in many countries.

If it were to come, a CBDC would have to be as convenient for consumers and businesses to use as the commercial equivalent. It would have to be hacker-proof. If we want to stop illegal use,

it should not grant the same anonymity of cash to users. But giving central banks unprecedented amounts of information about individuals is equally controversial. There is no one-size-fits-all solution.

In sum, thinking carefully about the future of money is timely in view of new technologies and increasing use of electronic payments. Still, it is not yet clear whether CBDCs for consumers and businesses are necessary or desirable. The jury is still out, and the answer will clearly differ country by country.

Away from the public eye, change may also be happening and perhaps sooner. The BIS report canvasses a second, complementary, model of CBDCs aimed at financial institutions that would build on the blockchain technologies underlying bitcoin. Such tokenised forms of digital central bank money could potentially help streamline many of the cumbersome clearing and settlement processes that are currently needed to complete securities and foreign exchange trades. So far, however, central bank experiments with such forms of CBDCs have not shown conclusive benefits for wholesale payments and beyond, but technology and design are evolving quickly.

Despite its many faults, bitcoin has put the spotlight on an old failing of our current system: cross-border retail payments. Such payments not only permit shoppers to easily buy goods online from overseas, but also allow foreign workers to send money home, supporting financial inclusion and development. However, these payment channels are generally much slower, less transparent and way more expensive than domestic ones. Improvements here are the best way of rising to the bitcoin challenge.

Michel Aglietta : « Une monnaie mondiale et privée, c'est absurde et dangereux »

Pas de monnaie sans confiance, et pas d'économie sans monnaie. L'économiste décrypte les ressorts de ce lien essentiel et livre ses réflexions sur le bitcoin, le libra de Facebook et les monnaies digitales de banques centrales.

« *La confiance est la matière première dans laquelle toutes les catégories de monnaie sont frappées* », relève l'universitaire Yuval Noah Harari dans son best-seller *Sapiens*. Qu'il s'agisse du grain d'orge, la première monnaie connue de l'histoire, apparue à Sumer autour de 3 000 ans avant Jésus-Christ, des cauris, les coquillages des sociétés primitives, des dollars ou euros d'aujourd'hui circulant essentiellement sous la forme d'écritures électroniques, ces instruments servant de monnaie « n'ont de valeur que dans notre imagination commune » et reposent sur une convention collective, « une révolution purement mentale ». L'apparition de la monnaie a libéré les échanges de la condition dite de « double coïncidence des désirs » imposée par le troc, et ainsi marqué le passage à l'économie de marché. « La monnaie est le système de confiance mutuelle le plus universel et le plus efficace qui ait jamais été imaginé », estime même l'historien israélien. La parant de mille vertus, il lui attribue un rôle pacificateur : « La monnaie est l'apogée de la tolérance », affirme-t-il.

« Grâce à l'argent, même des gens qui ne se connaissent pas et ne se font pas confiance peuvent tout de même coopérer efficacement. »

Dès l'Antiquité, Aristote avait défini ses trois fonctions, qui restent d'actualité : unité de compte (permettant d'établir les prix), réserve de valeur et intermédiaire des échanges (moyen de paiement ayant une valeur fiable aux yeux de tous). « La monnaie [nomisma en grec, de nomos la norme, ndlr] est pour nous une sorte de gage donnant l'assurance que l'échange sera possible si jamais le besoin s'en fait sentir », écrit le philosophe dans *L'Éthique à Nicomaque*. Une sorte de contrat, de garantie. La fin de la convertibilité en or de la monnaie (en 1936 pour le franc, en 1971 pour le dollar), a montré ce lien essentiel entre monnaie et confiance de façon plus évidente. Nos économies modernes sont fondées sur la monnaie fiduciaire (du latin fides, la confiance), c'est-à-dire émise par une banque centrale, sans valeur intrinsèque ni possibilité de la convertir en un poids fixe en or, et à 90 % sous forme scripturale (le reste en pièces et billets). Cette monnaie fiduciaire est « acceptée en échange de biens et de services, car la population fait confiance à la banque centrale en ce qui concerne le maintien de la stabilité de la monnaie sur la durée », explique la Banque centrale européenne (BCE) sur son site. L'économiste Michel Aglietta a travaillé plusieurs décennies sur ce lien entre monnaie et confiance, relevant qu'il n'y a « pas de monnaie sans confiance », même l'or étant à ses yeux une monnaie fiduciaire. « La monnaie n'a pas d'utilité intrinsèque mais elle a une utilité sociale formidable, parce qu'on postule qu'elle est acceptée par tous. Elle fait lien social », nous confie l'auteur de *La Monnaie entre violence et confiance*.

« Le paiement n'est pas un acte individuel mais un système. Pour qu'il y ait finalité des règlements, il faut une entité supérieure, ultime, qui ne peut être privée, qui est reconnue légitime par la loi. Ce qui ne veut pas dire que cette institution doit être dépendante de l'État. Elle peut même avoir du capital privé et a intérêt à être autonome. La monnaie est un bien public par nature, mais elle n'est pas une créature de l'État : elle est un processus d'unification de la société, légitimée par la puissance publique », analyse l'universitaire, conseiller scientifique au CEPII et à France Stratégie.

La crise financière a engendré le bitcoin

La grave crise financière mondiale de 2007-2008 a ébranlé cette confiance dans l'ensemble du système, dans les banques centrales et commerciales, et dans les monnaies. C'est dans ce contexte qu'un certain Satoshi Nakamoto (le pseudonyme d'un collectif, probablement) a créé le bitcoin. Son livre blanc du

31 octobre 2008 n'est pas un brûlot libertarien mais un texte technique proposant la création d'un « système de pair à pair de cash électronique », pour pouvoir échanger de la valeur sur Internet « sans le besoin d'un tiers de confiance » : le nouveau système se fonde sur « une preuve cryptographique au lieu de la confiance ». La foi dans le code informatique plutôt que dans l'État et son bras armé, la banque centrale.

« La croyance qu'un code informatique à lui seul puisse remplacer la nécessité d'une instance d'autorité légitimée par la loi et qui représente le lien collectif, et ce pour le monde entier, soit plus de 7 milliards d'habitants, cela n'a aucun sens ! C'est une croyance d'informaticiens. Elle repose sur une idée politique, l'anarchisme, selon lequel la société peut faire ordre social de manière organique », argumente Michel Aglietta. Il se montre critique sur le bitcoin, son absence d'instance légitime centrale, ses délais de traitement de transactions, ses coûts de pollution, sa limitation en quantité, mais il reconnaît que « la technologie blockchain a le potentiel de réduire considérablement les coûts des paiements ». Très au fait du projet de cryptomonnaie de Facebook, le libra, il ne cache pas ses réserves. « Le projet libra est extrêmement dangereux. Si le bien public est approprié privativement, il n'y aura plus de démocratie. La monnaie doit rester publique. C'est une plaisanterie quand Facebook parle d'une association à but non lucratif. Une constitution ne va pas déléguer à un ensemble d'acteurs privés, qu'ils soient cent ou un seul, ce qui est la cohésion de l'ordre social. En outre, Facebook a la prétention d'en faire une monnaie mondiale. C'est absurde !! Il n'y a pas d'ordre social mondial, or la monnaie est la représentation d'un ordre social. Il n'est pas possible que des acteurs privés non bancaires participent à un système de paiement sans être régulés comme des entités spéciales. Ce n'est pas par hasard si les banques ont des licences et sont régulées. Les gouvernements vont s'apercevoir du danger. Une des solutions est la monnaie digitale de banque centrale », fait-il valoir. En Suède, la Riksbank a un projet très avancé, l'e-krona, ou couronne digitale.

« Il n'y a pas de raison que Facebook soit le seul à proclamer "Je suis la monnaie ultime" !! Pour l'instant, Google et Amazon continuent de coopérer avec des acteurs bancaires pour le paiement, mais Google ne peut accepter que Facebook soit le seul à créer sa monnaie digitale. On se dirige donc vers une pagaille formidable !! Le danger est que le pouvoir monétaire glisse de l'autorité légitime à des monopoles privés », met en garde l'économiste. « Le système monétaire international ne se change pas en fonction des lubies d'untel », insiste-t-il. Si le géant des réseaux sociaux a assuré qu'il mettrait en place un remboursement en cas de perte des libras (smartphone volatilisé ou mot de passe oublié), il ne devrait pas bénéficier de la garantie réglementaire existant dans de nombreux pays sur les dépôts bancaires à hauteur de 100 000 euros par personne en France par le biais du Fonds de garantie des dépôts et résolution (FGDR), tandis que les sommes déposées sur les livrets d'épargne (livret A, LDDS, LEP) sont garanties en totalité par l'État. Sauf à être officiellement régulé comme une banque.

14 % des sondés prêts à utiliser le libra

Gouvernements et banques centrales ont exprimé leurs réserves, voire leur défiance, à l'égard du libra, et le G7 va mettre en place une taskforce sur les stablecoins (cryptomonnaies indexées sur une devise ou un panier d'actifs pour stabiliser leur valeur). Mais Facebook inspire-t-il assez confiance à ses membres pour que ces derniers aient envie d'utiliser sa monnaie privée ? En France, selon un sondage de YouGov pour 20 Minutes, seuls 14 % des sondés ont déclaré qu'ils envisageaient d'utiliser le libra, et 12 % ont déclaré lui faire confiance, la proportion étant plus élevée chez les 18-24 ans (20 %). Le libra dépassera-t-il le stade de projet et pourra-t-il vraiment concurrencer les monnaies légales ? D'autres monnaies privées pourraient-elles émerger dans les années à venir ? Jusqu'ici, la forte volatilité des « monnaies virtuelles » (les banques centrales préfèrent dire « cryptoactifs » car elles leur refusent le statut de monnaie) comme le bitcoin les a empêchées de remplir le rôle de valeur de réserve.

Delphine Cuny



L'objectif de Nakamoto était de permettre la création et la circulation d'une monnaie sans aucune intervention d'une banque centrale ou d'institutions financières. Pour ce faire, il a créé le protocole de la chaîne de blocs et la crypto-monnaie bitcoin. Comme l'écrit Nakamoto dans le résumé au début de son article de 2008 :

"Une monnaie électronique gérée par un réseau de pairs ("peer to peer network") permettrait d'effectuer des paiements en ligne sans recourir à un intermédiaire financier. Les signatures digitales joueraient un rôle dans ce réseau, mais ne seraient pas suffisantes pour éviter le recours à un tiers de confiance. Nous proposons une solution à ce problème."

Un bitcoin ne valait pas plus de 50 cents en 2010, aujourd'hui il vaut près de 10 mille dollars. Belle performance ! Et pourtant, le bitcoin fait l'objet de doutes et même de critiques sévères. Ainsi, en 2018, à l'université de Francfort, le président de la Banque des Règlements Internationaux disait (voir son allocution sur <https://www.bis.org/speeches/sp180206.htm>)

"Une monnaie est une indispensable convention sociale, bénéficiant du soutien d'une institution publique responsable en laquelle on a confiance. La meilleure institution de ce type étant une banque centrale... Les jetons digitaux privés qui se prétendent des devises, comme bitcoin, ne doivent pas mettre en danger la confiance en la valeur fondamentale et la nature de la monnaie."

De sérieux avertissements ont aussi été prononcés par les plus grands économistes, au rang desquels Joseph Stiglitz ou Jean Tirole, lequel écrivait dans une lettre ouverte au Financial Times le 30 Novembre 2017.

"Nous devons être prudent face à la hausse du bitcoin : les investisseurs doivent être protégés, et les banques régulées, les compagnies d'assurance et les fonds de pension ne devraient pas être autorisés à s'exposer au risque de ces instruments... Les gouvernements qui considèrent avec sympathie le bitcoin et les ICO devraient protéger leurs citoyens et leurs institutions financières contre le risque d'évolutions couteuses pour la société."

Deux visions s'opposent donc : d'un côté la vision libertarienne et technologique, selon laquelle la monnaie est créée et échangée dans un réseau de pairs, grâce à un protocole informatique, sans aucune intervention extérieure ; de l'autre côté la vision institutionnelle et politique, selon laquelle la monnaie ne peut être digne de confiance que si son émission est encadrée par une institution publique fiable, telle qu'une banque centrale indépendante.

Le développement des crypto-monnaies s'inscrit donc dans le contexte de deux tendances lourdes de nos sociétés : remise en cause de l'establishment et des institutions, essor et influence révolutionnaire des nouvelles technologies de l'information. Plutôt qu'un pouvoir central, arbitre en dernier ressort de l'allocation et de la valorisation de la monnaie, les partisans des crypto-monnaies défendent l'idée

d'une démocratie directe des internautes, se déployant dans le cadre d'une chaîne de blocs publique, ouverte et transparente¹.

Comment se situer face à ces deux visions contradictoires ? Faut-il souscrire à la vision libertarienne ou à la vision institutionnelle ? La chaîne de blocs et les crypto-monnaies vont-elles révolutionner nos sociétés et nos économies, ou bien ne sont-elles que de dangereuses illusions ?

Pour apporter un éclairage sur ces questions, Bruno Biais, chercheur TSE, utilise les outils de la théorie économique, afin d'analyser le fonctionnement de la chaîne de blocs, dans la première partie, de ce cahier puis la valeur des crypto-monnaies, dans la seconde partie.

1/ Des institutions financières, des banques centrales et des entreprises développent actuellement des chaînes de blocs privées. Ces initiatives sont très intéressantes, mais radicalement différentes des chaînes de blocs publiques, qui sont décentralisées, transparentes et ouvertes à tous, alors qu'une chaîne de blocs privée est gérée par une autorité centrale qui décide qui a accès à la chaîne, qui peut intervenir et comment. Nous ne traiterons ici que des chaînes de blocs publiques.



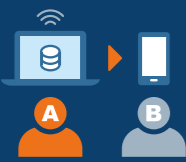
BRUNO BIAIS

Professeur à la Toulouse School of Economics, Bruno Biais est également chercheur senior au Centre de Recherche en Management (CNRS). Son travail a été publié dans *Econometrica*, le *JPE*, l'*ARE*, la *Review of Economic Studies*, le *Journal of Finance* et le *RFS*. Il a enseigné à HEC, CMU, LBS, Oxford et LSE. Il a été conseiller scientifique d'Euronext et du NYSE. Il a reçu la médaille de bronze du CNRS et est membre de la Société économétrique. Il a été rédacteur en chef de la *Review of Economic Studies* et co-éditeur du *Journal of Finance*.

DOMAINES DE RECHERCHE

- Microstructure du marché
- Finance d'entreprise
- Contrats financiers
- Économie politique
- Psychologie et économie
- Économie expérimentale





Le fonctionnement d'une chaîne de blocs

Le résumé au début de l'article de Nakamoto (2008), dont nous avons plus haut cité les premières phrases, continue de la manière suivante :

"Le réseau date les transactions en les incluant dans une chaîne de "hash-based proof of work", donnant ainsi lieu à un enregistrement qui ne peut être changé sans refaire la "proof of work". La chaîne la plus longue sert non seulement de preuve de la séquence d'événements enregistrés, mais aussi de preuve que ces enregistrements ont été effectués par la capacité de calcul agrégée la plus puissante. Tant que la majorité de la capacité de calcul est contrôlée par des nœuds qui ne s'allient pas pour attaquer le réseau, elle donnera lieu à la chaîne la plus longue et dépassera les attaques. La structure du réseau est minimale : les messages sont diffusés dans la mesure du possible, les nœuds peuvent quitter le réseau quand ils le veulent, et, quand ils reviennent au réseau, acceptent la plus longue chaîne de blocs."

Ces phrases ne sont pas évidentes à comprendre au premier abord. En particulier elles utilisent des expressions mystérieuses, comme "proof of work", "hash" et "chaîne la plus longue". Pour essayer de clarifier tout cela, nous allons dans un premier temps expliquer l'objectif et le mécanisme de la chaîne de blocs. Dans un deuxième temps nous présenterons les prédictions de la théorie économique pour le fonctionnement de cette chaîne.

La vision de Nakamoto (2008)

Rappelons d'abord les trois caractéristiques essentielles de la chaîne de blocs :

- 1) C'est un registre indiquant à qui (en fait à quelle identification informatique) appartiennent des objets ou des actifs, par exemple des bitcoins. Chaque bloc dans la chaîne décrit les modifications du registre.
- 2) C'est un registre distribué car il est accessible à tous ceux qui se connectent au réseau, et qui peuvent ainsi le consulter, et aussi le modifier. La chaîne de blocs est une "distributed ledger technology".
- 3) Dans ce registre distribué les décisions sont prises par les internautes membres du réseau. Le protocole de la chaîne de blocs organise ainsi une sorte de « vote informatisé » par les membres du réseau. L'objectif est que nul ne puisse décider à lui seul (au contraire de ce qui se passe avec une autorité centrale). En fait, plutôt qu'un vote stricto sensu, le protocole de la chaîne de blocs permet une sorte de tirage au hasard, parmi tous les membres du réseau. Pour chaque bloc, c'est-à-dire pour chaque modification de la chaîne de blocs, on tire au sort un membre du réseau, qui décide ou non de valider la modification.

La première chaîne de blocs, et la plus importante aujourd'hui encore, est le registre indiquant à qui appartient chaque bitcoin. Lorsqu'un détenteur de bitcoin l'échange contre un bien, un service, ou une autre monnaie, il en informe le réseau. La tâche du réseau est alors de valider cette transaction, de l'inclure dans un bloc avec d'autres transactions, et de rattacher ce bloc à un bloc précédent. Cette chaîne révisée par l'ajout d'un bloc supplémentaire donne le nouvel état du registre.

Les membres du réseau procédant à cette validation des transactions et ce rattachement des blocs sont les mineurs. Nakamoto (2008) décrit la façon dont il propose que les mineurs travaillent (illustrée dans la Figure 1):

- I) Le mineur reçoit sur le réseau les messages indiquant les transactions ;
- II) il regroupe un ensemble de messages dans un bloc ;

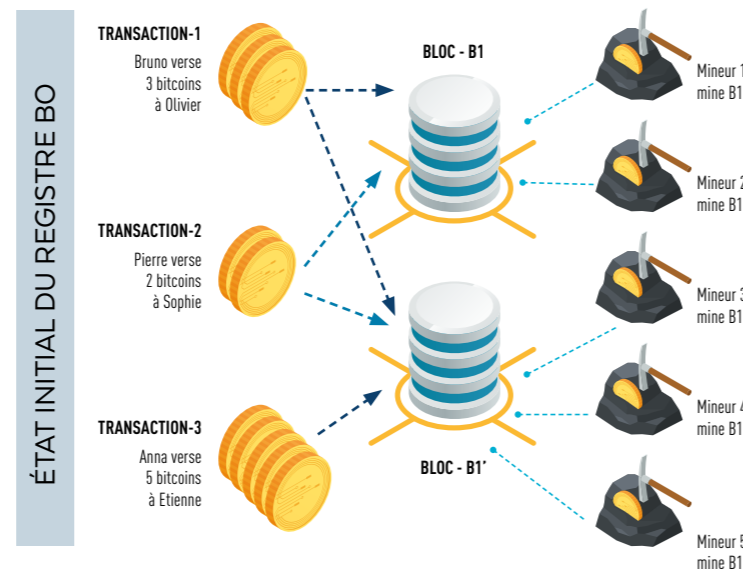


Figure 1A : mineurs, transactions et blocs

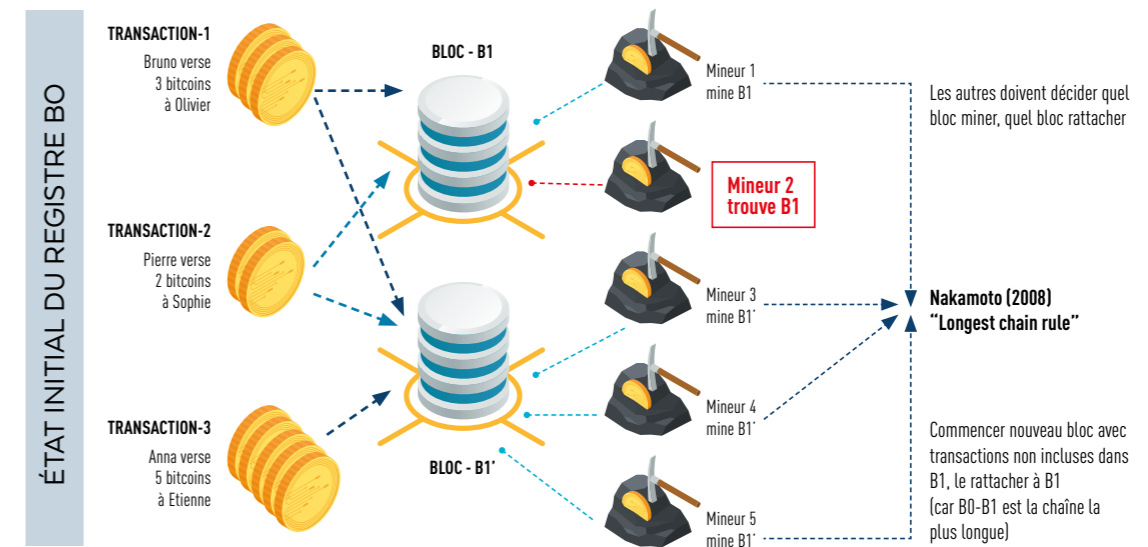


Figure 1B : règle de la chaîne la plus longue

III) il vérifie que ces messages sont valides (par exemple que ceux qui disent qu'ils ont transféré un bitcoin le possédait bien) - cette étape est très rapide ;

IV) il travaille à résoudre un problème numérique très compliqué, sans aucun intérêt intrinsèque, et sans aucune relation avec le nombre ou la nature des transactions contenues dans le bloc.

Dès qu'un mineur a résolu son problème numérique, il annonce au réseau qu'il vient de résoudre un bloc donné, et à quel bloc précédent il le rattache. Les autres mineurs reçoivent cette information. Ils pourraient choisir de l'ignorer, et continuer à chercher la solution du problème correspondant à leur bloc. Cependant, Nakamoto (2008) recommande aux mineurs d'abandonner leur propre bloc, commencer à en miner un nouveau, et l'enchaîner au bloc qui vient d'être résolu. Suivre cette recommandation c'est suivre la règle de la chaîne la plus longue, qui stipule qu'à tout moment le bloc qu'un mineur cherche à résoudre doit s'enchaîner à la chaîne la plus longue à ce moment-là.

Supposons donc que les mineurs suivent la règle de la chaîne la plus longue. Après qu'un bloc a été résolu, ils vérifient que la solution proposée par le mineur est la bonne. Cette vérification est rapide car si les problèmes numériques proposés aux mineurs sont difficiles à résoudre, leur solution est facile à vérifier. En effectuant cette vérification, les participants au réseau obtiennent la preuve que le mineur a bien fait son travail : c'est la "proof of work". Après avoir vérifié la "proof of work", les mineurs décident d'accepter le nouveau bloc ou non. S'ils l'acceptent, ils enchaînent à ce bloc les blocs qu'ils résoudront eux-mêmes par la suite.

Qu'est-ce qui pourrait amener un mineur à suivre la règle de la chaîne la plus longue et abandonner le minage de son propre bloc pour se concentrer sur le bloc qui vient d'être résolu par un autre mineur ?

Un premier élément de réponse est fourni par la nature du processus de résolution des blocs. Pour résoudre le problème numérique correspondant à son bloc, le mineur tire des solutions au hasard et à chaque tirage teste si c'est la bonne solution. Pour ce faire, le mineur utilise des ordinateurs. Plus la capacité de calcul de ces ordinateurs est grande, plus le nombre de solutions possibles que le mineur tire chaque seconde (hash rate) est grand, et plus il résout vite son problème en moyenne. Cependant, à capacité de calcul et difficulté du problème constantes, le nombre de tirage au hasard que le mineur devra faire avant de trouver la solution est une variable aléatoire. Par conséquent, le temps de résolution d'un problème est variable. Une propriété très importante de cette variable aléatoire est que le temps qui reste avant la résolution d'un problème est indépendant du temps déjà passé à tenter de résoudre ce problème. On peut avoir l'intuition de cette propriété en imaginant que le mineur effectue des tirages avec remise dans une urne contenant de nombreuses boules, dont l'une contient la solution



alors que les autres ne contiennent aucune information. Dès lors, un mineur qui a travaillé une seconde sur son problème a autant de chances de le résoudre pendant la seconde suivante qu'un mineur qui a déjà travaillé un quart d'heure sur son problème. De ce point de vue, un mineur n'a pas plus intérêt à s'obstiner sur le problème qu'il a commencé à chercher à résoudre qu'à s'attaquer à un problème nouveau.

Mais pourquoi les mineurs consacrent ils leur capacité de calcul, leur temps et leur électricité à la résolution des blocs ? C'est parce que, pour chaque bloc résolu, le mineur reçoit une récompense. Ainsi, dans le protocole bitcoin il est prévu que le mineur qui résout un bloc reçoit un certain nombre de bitcoins, actuellement 12,5. En pratique, le mineur inscrit dans son bloc une transaction qui attribue ces bitcoins à lui-même. Si les autres mineurs expriment leur accord avec le bloc qu'il a miné, en y enchaînant les leurs, ils expriment leur accord à l'attribution de cette récompense. Ces 12,5 bitcoins sont créés ex nihilo. Ce sont ces récompenses qui alimentent la création de la crypto-monnaie. Cette création monétaire est prédéterminée par le protocole Bitcoin, qui prévoit que le montant gagné par un mineur baissera progressivement. Il était initialement égal à 50 bitcoins, et est divisé par 2 tous les 4 ans. Ainsi il s'établira à 6,25 en 2020. En 2140, 21 millions de bitcoins auront été minés, et il est prévu que la création monétaire de bitcoin s'arrête alors.

Comment les mineurs seront-ils rémunérés lorsque la création de bitcoin cessera? En plus de la création monétaire, les mineurs bénéficient du paiement de commissions par les agents économiques à l'origine des transactions. Si je veux transférer 1 bitcoin à un de mes enfants, et désire que cette transaction soit rapidement minée, je promets une commission élevée, par exemple 0,01 bitcoin, au mineur qui résoudra le bloc incluant ma transaction. Quand il n'y aura plus de création monétaire, les mineurs seront rémunérés seulement par ces commissions.

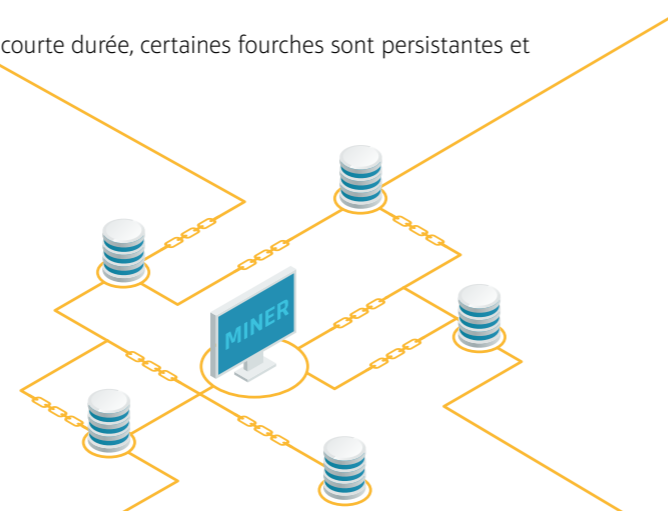
Selon la vision de Nakamoto (2008), le protocole décrit ci-dessus, et le respect de la règle de la chaîne la plus longue, doivent permettre l'émergence d'une chaîne unique, transparente et ouverte à tous, proposant un registre faisant l'objet d'un consensus fiable et durable. Cette vision est-elle réaliste ? Qu'a-t-on observé en pratique, et quel éclairage apporte la théorie sur ce qui s'est produit dans le passé et sur ce qui peut se produire dans l'avenir ?

L'épreuve des faits et de la théorie

Le constat premier est que le bitcoin connaît un immense succès. Beaucoup de personnes en achètent et en vendent, ce qui donne lieu à de nombreuses transactions, qui sont validées par les mineurs. De manière correspondante, on observe un nombre croissant de mineurs, utilisant une capacité de calcul et une quantité d'électricité croissantes (10 térawatt-heure il y a un an, 44 il y a 3 mois, 62 aujourd'hui, voir <https://digiconomist.net/bitcoin-energy-consumption>). Cette consommation d'électricité correspond actuellement à celle de la Suisse. D'autres crypto-monnaies, elles aussi utilisatrices de capacité de calcul et d'électricité, connaissent un grand succès, au premier rang desquelles l'ether, basée sur la chaîne de blocs Ethereum.

En fait on observe la création de très nombreuses nouvelles crypto-monnaies, créant souvent des fourches depuis les crypto-monnaies initiales. Ainsi, durant l'été 2016, une fourche s'est produite sur Ethereum, donnant lieu à une crypto-monnaie concurrente, ether classic. En août 2017, une fourche s'est produite dans Bitcoin, donnant lieu à la création de Bitcoin Cash, et à l'automne 2017, une nouvelle fourche est apparue avec Bitcoin Gold. En décembre 2017, alors que le cours du bitcoin s'envolait, le rythme d'apparition des fourches a connu une forte accélération, avec Super Bitcoin, Bitcoin X, Oil Bitcoin, Bitcoin World, Lightning Bitcoin, etc.

Même si la plupart des fourches récentes seront vraisemblablement de courte durée, certaines fourches sont persistantes et attirent mineurs et investisseurs. C'est le cas, par exemple, de Bitcoin Cash. Le nombre de tirage de solutions par seconde (hash rate) sur le réseau bitcoin s'élève actuellement à 30 exahash par seconde (30 fois 10 puissance 18). Ce n'est que 8 fois plus élevé que celui de Bitcoin Cash. D'ailleurs un bitcoin cash vaut à peu près 0,16 bitcoins. Or chaque fourche I) correspond à une déviation de la règle de la plus longue chaîne proposée par Nakamoto, II) éloigne du consensus en créant des chaînes de blocs proposant des registres différents, et III) risque d'éroder la valeur des crypto-monnaies.



Pourquoi cette multiplication des fourches ? Comment est-elle possible, alors que Nakamoto annonçait l'émergence d'une chaîne de blocs unique ?

À l'origine des principales fourches mentionnées ci-dessus il y a des désaccords au sein de la communauté des mineurs et développeurs. Dans le cas d'Ethereum Classic, des ethers avaient été détournés d'un fonds de placement (TheDAO, acronyme de Decentralized Autonomous Organization). Des membres de la communauté avaient proposé de revenir en arrière dans la chaîne des blocs, pour annuler le détournement de fonds. On crut d'abord que toute la communauté se rangeait à cette solution, mais on s'aperçut rapidement qu'une minorité s'y opposait, car elle était attachée au principe de l'immutabilité de la chaîne de blocs. Un an et demi plus tard, cette fourche subsiste : l'ether classic vaut environ 20 dollars, alors que l'ether vaut environ 700 dollars. Dans le cas de Bitcoin Cash, il s'agissait d'un désaccord sur la manière de modifier le protocole pour accroître la taille des blocs, et dans le cas de Bitcoin Gold le désaccord portait sur l'utilisation d'ASIC, des circuits intégrés spécifiques, qui ne peuvent être utilisés que pour le protocole Bitcoin, et dont la production est dominée par une puissante entreprise chinoise.

Par-delà ces désaccords, il y a une raison profonde à l'apparition de ces fourches : le minage est un jeu de coordination, qui admet des équilibres multiples, et des fourches sur le sentier d'équilibre. Pour comprendre ce phénomène, rappelons-nous que les mineurs sont récompensés par des bitcoins nouvellement créés, inscrits dans le bloc qu'ils résolvent. Or ces bitcoins ne seront reconnus comme valables par les autres agents économiques que si le bloc lui-même est reconnu comme valable. Ce sera le cas si les autres mineurs décident d'enchaîner leurs propres blocs à ce bloc. Et ils le feront s'ils pensent que la chaîne dans laquelle est incluse ce bloc est la chaîne faisant l'objet d'un consensus. Ainsi, de multiples équilibres peuvent émerger. Dans un équilibre, les mineurs anticipent que la chaîne A va faire l'objet d'un consensus, ils décident alors de rattacher leurs blocs à cette chaîne, par conséquent la chaîne attire de nombreux blocs, faisant ainsi l'objet d'un consensus, conformément à l'anticipation initiale, qui s'avère rationnelle. Mais dans un autre équilibre la grande majorité des mineurs pensent que A n'est pas valable, ils décident donc de rattacher leurs blocs à d'autres chaînes, A est abandonnée, s'avérant ainsi non valable, conformément à l'anticipation initiale. Dans notre article de recherche en commun avec Christophe Bisière, Matthieu Bouvard et Catherine Casamatta ("The blockchain folk theorem") nous montrons l'existence de ces équilibres multiples, et que plusieurs fourches concurrentes coexistent à long terme à l'équilibre, voir :

https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2017/wp_tse_817.pdf

Pour conclure cette première partie, rappelons que, conformément à la vision de Nakamoto, la chaîne de blocs fonctionne, attire des mineurs et sert de registre pour des crypto-monnaies qui sont valorisées par les investisseurs. Cependant, en contradiction avec la vision de Nakamoto, les mineurs ne suivent pas toujours la règle de la chaîne la plus longue, il n'y a pas de chaîne unique faisant l'objet d'un consensus complet, mais des fourches proposant différentes versions du registre. L'apparition et la persistance de ces fourches est liée au fait que le minage est un jeu de coordination, qui admet de multiples équilibres.

La valeur économique d'une cryptomonnaie

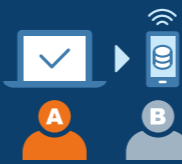
Étant données les promesses et les difficultés de la technologie de la chaîne de blocs sur laquelle elles sont fondées, quelle est la valeur économique des crypto-monnaies ? Pourraient-elles un jour concurrencer les monnaies supervisées par les banques centrales ? Pour apporter un éclairage sur cette question, nous commencerons par préciser la fonction économique de la monnaie, puis nous nous interrogerons sur la capacité des crypto-monnaies à remplir cette fonction.

Qu'est-ce qu'une monnaie, en général, et quels sont les déterminants de sa valeur ?

Une monnaie est quelque chose que j'accepte en paiement car j'anticipe qu'elle sera acceptée en paiement par les autres quand je voudrai à mon tour acheter. Dès cette définition, notre attention est attirée sur la notion d'anticipation, de croyance. Nous verrons qu'en ce qui concerne la monnaie tout est affaire de croyances.

Pour réfléchir au rôle économique de la monnaie, on peut commencer par considérer une économie de troc, et ensuite analyser comment la situation s'améliore quand on introduit la monnaie.

Dans une économie de troc, où seulement des échanges bilatéraux de biens et services prévalent, se pose le problème de la double coïncidence des besoins. Supposons qu'Alain a des abricots mais aime les carottes, alors que Bernard aime les abricots



mais a des bananes. Lorsqu'Alain rencontre Bernard, Bernard voudrait les abricots d'Alain, mais Alain n'a pas envie des bananes de Bernard. Il n'y a pas double coïncidence des besoins, l'échange ne peut avoir lieu.

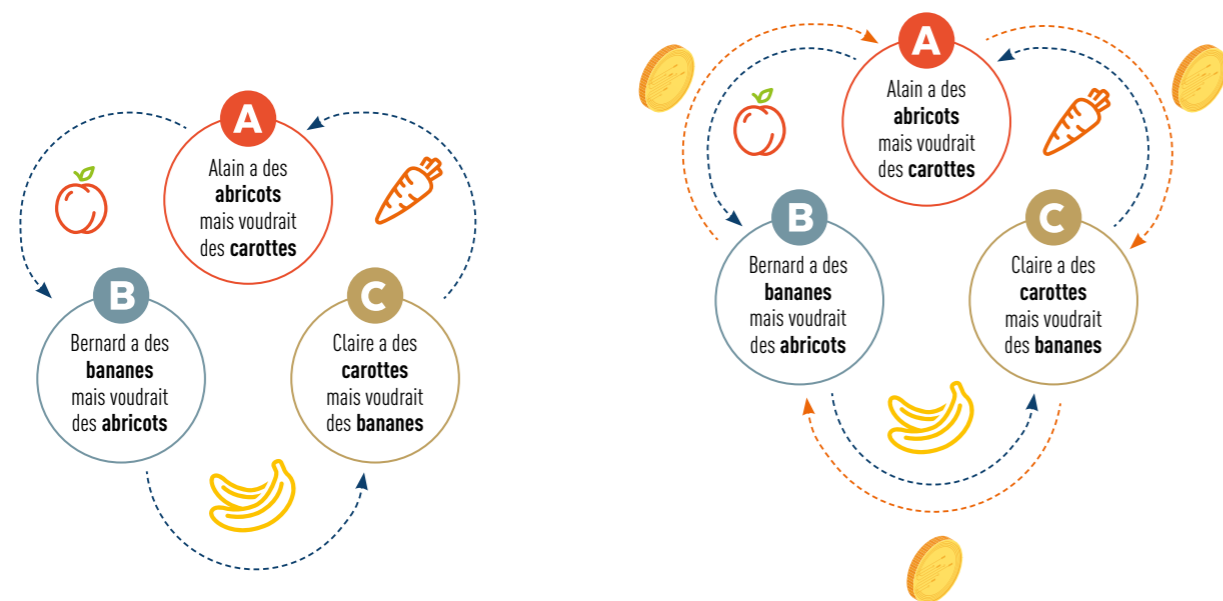
Pour permettre des échanges, on a besoin d'une relation sociale plus sophistiquée, comme celle analysée par le Triangle de Wicksell, grand économiste suédois né en 1851 et mort en 1926 (voir Figure 2). Supposons qu'en plus d'Alain et Bernard, il existe un troisième agent économique, Claire, qui a des carottes mais aime les bananes. Gardons l'hypothèse que les transactions sont bilatérales et supposons de plus que les fruits ou légumes ne peuvent être achetés, stockés puis revendus.

Pour que chacun puisse manger le fruit qu'il aime, il faudrait les échanges suivants :

- Alain donne ses abricots à Bernard
- Bernard donne ses bananes à Claire
- Claire donne ses carottes à Alain

Comment parvenir à cette allocation ? Il suffit d'introduire une pièce de monnaie, jeton, ou "coin", créée, par exemple, par une autorité centrale, roi Crésus ou banque centrale, qui accepte de la prêter, mais exige qu'on la lui rende à la fin des échanges. Dans ce contexte on peut parvenir à l'allocation optimale de la façon suivante :

- Bernard emprunte un jeton à la banque centrale et donne ce jeton à Alain en échange de ses abricots.
- Alain donne alors un jeton à Claire en échange de ses carottes.
- Finalement Claire donne un jeton à Bernard en échange de ses bananes, et Bernard peut rendre le jeton à la banque centrale.



Dans ce modèle, alors qu'elle n'a aucune valeur intrinsèque, la monnaie permet de réaliser des échanges, et ainsi d'améliorer la satisfaction de tous les agents économiques. On peut généraliser ce type de modélisation de la monnaie à de nombreux agents, interagissant pendant de nombreuses périodes. Une telle généralisation est proposée par le modèle à générations imbriquées, initialement proposé par Maurice Allais en 1947 dans son ouvrage *Économie et Intérêt*.

Le Triangle de Wicksell illustre bien le rôle crucial joué par les croyances dans le fonctionnement des échanges monétaires : Alain accepte le jeton que lui propose Bernard en échange de ses abricots, car il anticipe que Claire, à son tour, acceptera le jeton qu'il lui proposera en échange de ses carottes. Quant à Claire, si elle accepte le jeton d'Alain, c'est parce qu'elle anticipe que Bernard, à son tour, acceptera le jeton qu'elle lui proposera en échange de ses bananes. C'est donc bien un équilibre en anticipations rationnelles que tous acceptent la monnaie, car ils pensent qu'elle sera acceptée. Mais cette hiérarchie de croyances (croyances, croyances sur les croyances, etc.) n'est pas la seule possible à l'équilibre. Il existe aussi un équilibre de la défiance : chacun croit que les autres n'accepteront pas le jeton qu'il proposera, donc chacun refuse d'accepter le jeton qu'on lui propose. La défiance est ainsi une anticipation rationnelle. Nous retrouvons, ici encore, la multiplicité des équilibres que nous avons rencontrée dans notre analyse de la chaîne de blocs.

Dans l'analyse ci-dessus, tous les fruits et légumes avaient le même prix : un jeton. Dans un environnement plus complexe, de nombreux prix vont intervenir : prix variés des différents biens et services relativement à une monnaie (par exemple prix de la baguette en euros) mais aussi prix des différentes monnaies les unes par rapport aux autres (par exemple cours de l'euro vis-à-vis du dollar). Que nous apprend la théorie économique sur ces prix ?

Comme le montre Jean Tirole dans son article publié en 1985 dans *Econometrica* "Asset bubbles and overlapping generations", les monnaies sont un actif bien particulier, tout à fait différent d'actifs comme les actions : la valeur fondamentale de ces dernières reflète la valeur actuelle des biens réels et services qu'elles produiront dans le futur. C'est donc le fondamental à venir qui détermine le prix aujourd'hui. À l'inverse, les monnaies ne créent pas de bien réel, mais procurent un service de transaction : on pourra les utiliser dans le futur pour acheter des biens ou services. Or la valeur de ce service croît avec le prix qu'aura la monnaie dans le futur. Plus le cours de l'euro sera élevé dans un mois, plus le service de transaction que me procurera dans un mois l'euro que j'achète aujourd'hui sera élevé. Ainsi, au contraire des actions, c'est le prix futur qui détermine la valeur fondamentale aujourd'hui. Dès lors le prix aujourd'hui reflète les croyances au sujet du prix de demain.

Et, à nouveau, l'importance des croyances entraîne l'existence de nombreux équilibres en anticipations rationnelles : certains dans lesquels le cours de la monnaie est faible aujourd'hui car on anticipe qu'il sera faible demain, et d'autres dans lesquels il est élevé aujourd'hui car on anticipe qu'il sera élevé demain ! De plus, au cours du temps, les croyances peuvent changer, même si rien ne change dans l'économie réelle, entraînant des fluctuations, de la volatilité, dans le cours des monnaies.

Comment stabiliser la valeur de la monnaie ? En coordonnant les anticipations. C'est le rôle de l'autorité centrale. Rôle qu'elle peut exercer si elle est fiable, comme peut l'être, par exemple, une banque centrale indépendante et dont les objectifs et la détermination sont clairs. Un instrument supplémentaire pour ancrer les anticipations est de s'engager à accepter la monnaie en paiement, comme le fait l'état d'un pays en s'engageant à accepter la devise nationale pour le paiement des impôts.

Mais, si l'intervention d'une autorité centrale peut stabiliser les cours, en coordonnant les anticipations, elle peut aussi déstabiliser la monnaie. C'est le cas lorsque l'état est prédateur. Il peut alors spolier la valeur des avoirs monétaires en créant de l'inflation ou bien en empêchant les agents économiques d'utiliser leurs avoirs, par exemple en instaurant un contrôle des capitaux. En amont, la défiance par rapport à l'autorité centrale, état ou banque centrale, peut entraîner des croyances pessimistes, et une baisse de la valeur de la monnaie.

Comment situer les crypto-monnaies par rapport à ce cadre d'analyse ?

Dans la logique de l'inspiration libertaire qui a présidé à sa création, le bitcoin peut s'avérer très utile lorsque la situation politique empêche les agents d'utiliser la monnaie émise par la banque centrale et le système bancaire pour satisfaire pleinement leurs besoins. Ainsi, la faillite politique du Zimbabwe est telle que sa monnaie a perdu toute crédibilité, et son système bancaire est devenu extrêmement fragile et risqué.

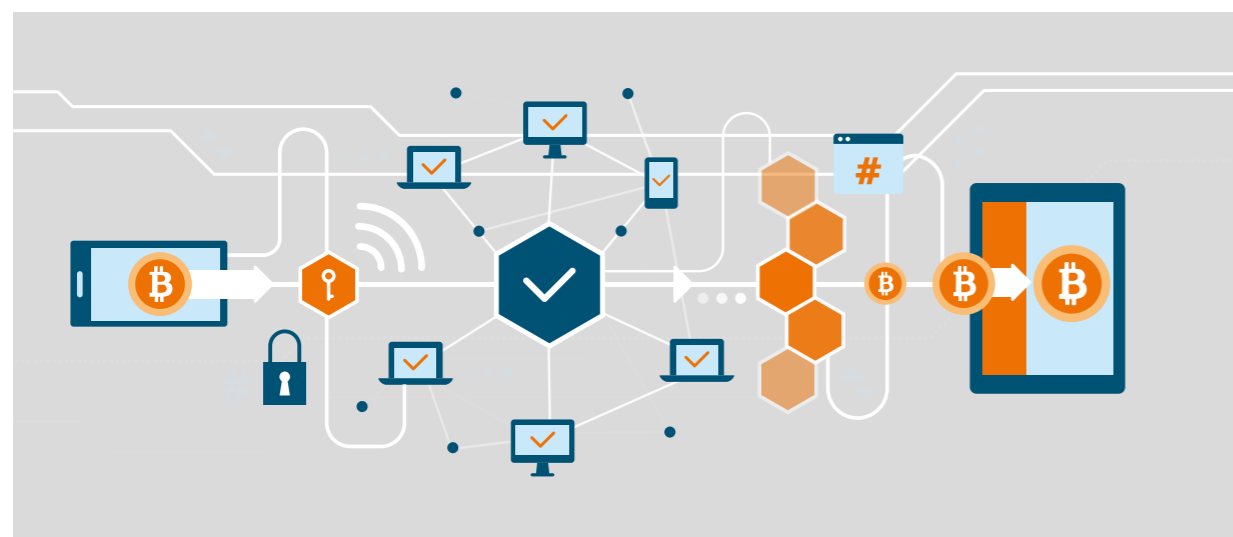
Pour régler leurs transactions les agents économiques se sont donc tournés vers le bitcoin, qui ne peut être confisqué par le pouvoir politique. De même, au Venezuela, l'inflation galopante et la crise politique ont presque annulé la valeur et la crédibilité de la monnaie nationale. Les agents économiques se sont donc tournés vers les crypto-monnaies, en particulier le bitcoin ou l'éther. En fait, comme l'électricité est peu coûteuse au Venezuela, les agents économiques se sont même lancés dans le minage de crypto-devises. En Chine, le gouvernement contrôle les banques et les mouvements de capitaux hors du pays. Pour contourner ces contrôles, les chinois ont eu, de plus en plus, recours aux crypto-monnaies. C'est ce qui explique la réaction très négative du gouvernement chinois par rapport à ces monnaies, et les régulations visant à restreindre leur utilisation.

CONCLUSION

Même si la situation politique d'un pays est relativement stable, il est possible que son système bancaire soit peu développé et peu efficace, rendant les paiements difficiles et coûteux. Le règlement de transactions par crypto-monnaies sur internet pourrait alors s'avérer utile. Les crypto-monnaies pourraient aussi être utiles pour effectuer des transferts de fonds internationaux quand les méthodes traditionnelles de transfert sont inefficaces et coûteuses.

Le développement de l'utilisation des crypto-monnaies se heurte cependant à de nombreux inconvénients, parmi lesquels figurent les suivants :

- a) Comme on l'a rappelé plus haut, la valeur d'une monnaie à un moment donné dépend des anticipations quant à sa valeur future. Or ces anticipations peuvent fluctuer considérablement, rendant le cours de la monnaie volatil. C'est probablement ce phénomène qui est à l'origine de la grande volatilité du bitcoin. De plus, par définition, nulle autorité centrale ne peut intervenir pour stabiliser le cours de la crypto-monnaie. Une conséquence de la grande volatilité des crypto-monnaies est qu'elles ne peuvent remplir une des trois fonctions essentielles de la monnaie qui est de servir d'unité de compte.
- b) L'utilisation d'une crypto-monnaie pour payer un bien ou un service expose à un risque de contrepartie difficile à gérer : soit le vendeur ne livre son bien qu'après que la chaîne de bloc a validé le transfert de la crypto-monnaie, et dans ce cas l'acheteur est exposé au risque que le vendeur ne livre pas le bien, soit le vendeur livre le bien immédiatement, auquel cas il est exposé au risque que la transaction ne soit finalement pas validée par la chaîne de blocs.
- c) L'essor des échanges de crypto-monnaies (alimenté par celui de la spéculation) a conduit à une congestion des chaînes de blocs. Par exemple la chaîne de blocs Bitcoin ne valide qu'un bloc toutes les dix minutes, et chaque bloc a une taille maximale d'un mégaoctet. Cela ralentit la vitesse avec laquelle les transactions sont validées. Pour que leur transaction soit incluse plus rapidement dans un bloc, et ainsi validée plus rapidement, les agents économiques peuvent promettre des commissions aux mineurs (comme cela a été expliqué plus haut). La commission moyenne pour une transaction sur Bitcoin est aujourd'hui proche de 30 dollars. Congestion et commissions rendent donc la validation des transactions en bitcoins lente et coûteuse, ce qui réduit la capacité de la crypto-monnaie de remplir une autre des trois fonctions essentielles de la monnaie, celle de moyen de paiement.
- d) Pour résoudre le problème de la congestion, il faudrait modifier le protocole, par exemple pour augmenter la taille des blocs. La communauté des mineurs et développeurs a cherché à résoudre ce problème depuis au moins un an, mais n'a pas encore réussi à se mettre d'accord sur une solution acceptée par tous. C'est que la coordination est difficile dans un contexte décentralisé.
- e) Les crypto-monnaies ne jouent aujourd'hui qu'un rôle minime en tant que moyen de paiement, relativement aux monnaies émises par les banques et les banques centrales. Pour qu'elles puissent jouer un rôle significatif, il faudrait pouvoir augmenter le nombre de transactions validées, et, pour ce faire augmenter la taille des blocs. On vient de voir que cela s'avérerait difficile.



8

Au début de notre réflexion nous avons noté que le développement des crypto-monnaies s'inscrit dans le cadre de deux tendances lourdes de nos sociétés. L'une est de nature technologique : le recours croissant aux nouvelles technologies de l'information et de la communication. L'autre est de nature sociale et politique : la remise en cause des élites et le désir de redonner le pouvoir à la base. Que nous ont appris nos analyses sur les perspectives des crypto-monnaies au regard de ces deux dimensions, technologique et socio-politique ?

Du point de vue technologique, pour que les crypto-devises, qui actuellement ne jouent qu'un rôle très marginal dans les paiements, parviennent à jouer un rôle significatif, il faut qu'elles puissent valider un volume de transactions plus importants. Une solution pour augmenter ce volume serait de multiplier le nombre des crypto-monnaies et des chaînes de blocs correspondantes. Cette solution ne serait guère satisfaisante, car la multiplication des crypto-monnaies réduirait leur fiabilité, alors que la multiplication des chaînes de blocs (utilisant la "proof of work") accroîtrait de manière non soutenable la consommation d'électricité. L'autre solution serait d'augmenter la taille de chaque bloc. On a vu plus haut que cette augmentation n'allait pas de soi. Supposons tout de même que la communauté des développeurs et mineurs finisse par mettre au point et adopter une modification du protocole augmentant la taille des blocs. Cette approche permettrait-elle d'augmenter le nombre de transactions validées sans une consommation d'électricité non soutenable ?

Dans un protocole reposant sur la "proof of work", plus la rémunération de la validation des blocs est élevée, plus les mineurs lui consacrent une grande capacité de calcul, plus la consommation d'électricité est grande. Pour limiter la consommation d'électricité, il faut donc limiter la rémunération de la résolution d'un bloc. On a vu plus haut que la récompense pour la résolution d'un bloc tend à décroître : actuellement égale à 12,5 bitcoins, elle passera à 6,25 en 2020, puis 3,125 en 2024, etc. Cette tendance va dans le bon sens, mais pour qu'elle baisse la rémunération des mineurs il faut aussi que le cours du bitcoin ne soit pas trop élevé. Il est possible, et même probable que ce sera le cas, mais on ne peut en être sûr. De plus, il faut aussi que la valeur totale des commissions offertes par les agents économiques pour la validation de leurs transactions reste basse. Or s'il y a une augmentation du nombre des transactions (incluses dans des blocs plus larges) cela tendra à faire monter le niveau total des commissions. Pour contrer ce phénomène il faut que la valeur individuelle de chaque commission reste faible. Pour atteindre cet objectif, il est nécessaire que le réseau ne soit pas congestionné, mais plutôt en surcapacité. Cela nous ramène à la nécessité de l'augmentation de la taille des blocs, qui est vraiment une condition indispensable au développement des chaînes de blocs et des cryptomonnaies.

Du point de vue politique et social, un des thèmes communs aux réflexions que nous avons proposées est la difficulté de coordonner les anticipations et les croyances d'agents économiques dispersés. Des croyances mal coordonnées et instables peuvent conduire à des mouvements de cours excessifs, et ainsi à des monnaies fragiles et volatiles. Des croyances mal coordonnées peuvent aussi conduire à une multiplication des fourches, empêchant la chaîne de blocs de fonctionner correctement. C'est un problème important, qui pourrait grever l'avenir des chaînes de blocs publiques et des crypto-monnaies. En effet, l'inspiration libertarienne de ces technologies interdit l'intervention d'une autorité centrale et exige que la coordination provienne de la base, ce qui est difficile à réaliser en pratique. En cela les crypto-monnaies diffèrent significativement des monnaies traditionnelles, pour lesquelles la banque centrale peut aider les agents à coordonner leurs croyances, comme le montrent Isabel Schnabel et Hyun Shin, dans un récent document de travail de la Banque des Règlements Internationaux, intitulé "Money and Trust: Lessons from the 1620s for money in the digital age." (Voir <https://www.bis.org/publ/work698.htm>)

Pour conclure cet exposé, rappelons un épisode d'histoire monétaire qui illustre bien les dangers créés par des croyances trop volatiles et mal ajustées. En 1707, John Law arrive en France. Il propose de remplacer les monnaies existantes (pièces en métal précieux) par des billets de papiers gagés sur les actions de la Compagnie des Indes Occidentales. Voilà bien une innovation, on pourrait même dire une disruption. En 1719, le cours des actions de la Compagnie est passé de 500 livres à 10000 livres. La monnaie nouvelle créée par John Law connaît un succès retentissant. On se bouscule pour l'acheter. Certains la revendent à profit. Des nobles, des ecclésiastiques, des domestiques et des aubergistes amassent très rapidement des fortunes impressionnantes. En 1720, les cours s'effondrent, les billets du Mississippi ne valent plus rien, de nombreuses personnes sont ruinées.

III. Central banks and payments in the digital era

(...)

Introduction

A vital function of the financial sector is to provide efficient ways for households and businesses to make and receive payments. A sound and well functioning payment system facilitates economic activity and supports long-run economic growth.¹

Payment systems today build upon a two-tier structure provided by the central bank together with commercial banks. The central bank plays a pivotal role by ensuring trust in money, a core public good for the economy at large, while the private sector leads on innovation in serving the public. The central bank supplies the ultimate safe medium to settle both wholesale and retail transactions, while commercial banks supply the bulk of retail payment instruments.

Over the past few decades, payment systems have undergone a radical transformation. New payment methods and interfaces have taken shape, and many more innovations are under way.² While these developments raise new challenges, the core role of the central bank in payment systems remains. The private sector can provide the innovation, ingenuity and creativity to serve customers better, but history illustrates that private sector services thrive on a solid central bank foundation. Whether promoting interoperability, setting standards or levelling the competitive playing field, there are strong arguments for the public sector to play a role. In fact, today the central banks' role is as important as ever, if not more so.

Central banks are actively pursuing a range of policies to tackle existing shortcomings. The objective is to ensure that households and businesses have access to safe and efficient payment options. Central banks can choose to stand at the cutting edge of innovation themselves, not least in their direct provision of services to the public at large. One option at the frontier of policy opportunities is the issuance of CBDCs, which could amount to a sea change. CBDCs could offer a new, safe, trusted and widely accessible digital means of payment. But the impact could go much further, as they could foster competition among private sector intermediaries, set high standards for safety, and act as a catalyst for continued innovation in payments, finance and commerce at large.

This chapter discusses the foundations of money and payment systems, payment trends and policies. It concludes with a short discussion of the future of payments.

Money and payment systems: the foundation

While we use money every day, its theoretical definition can be elusive.³ Still, we all recognise it when we see it. Money has taken different forms through the ages, but one of its defining features has been serving as a medium of exchange, accepted as payment for goods and services (Box III.A).⁴ In addition, money serves as a store of value and a unit of account. This chapter focuses primarily on the medium of exchange function, also called means of payment, and on the supporting system.⁵

A payment system is a set of instruments, procedures and rules for the transfer of funds among participants.⁶ Payment systems are generally classified as either retail or wholesale. A retail payment system handles a large volume of relatively low-value payments, in such forms as credit transfers, direct debits, cheques, card payments and e-money transactions. A wholesale payment system executes transactions between financial institutions. These payments are typically large-value and need to settle on a particular day and sometimes by a particular time.

As money has evolved through the centuries, so have the means of payment. The pace of change is especially rapid today. Indeed, payments continue to be the financial service most affected by shifts in demand, technology and new entrants.⁷ Despite improvements, households and businesses demand safer and ever faster payments. They increasingly expect payments to be mobile-first, fully digital and near instant, whether online or at the point of sale. Moreover, the current pandemic could accelerate the shift to digital payments.

At the same time, some new entrants have tried to capitalise on the existing shortcomings. Three such attempts stand out: the rise (and fall) of Bitcoin and its cryptocurrency cousins;⁸ Facebook's proposal to develop Libra – a private global stablecoin arrangement;⁹ and the foray of big tech and fintech firms into financial services.¹⁰ Some of these have failed to gain much traction; others are perceived as a threat to jurisdictions' monetary sovereignty; while many have yet to address a host of regulatory and competition issues. Nevertheless, all have propelled payment issues to the top of the policy agenda.

The foundation of a safe and efficient payment system is trust in money.¹¹ In a fiat money system, where money is not backed by a physical asset, such as gold, trust ultimately depends on the general acceptance of pieces of paper that cannot be redeemed in anything but themselves. General acceptance is what ultimately makes them valuable, alongside confidence that payments made with them can irrevocably extinguish obligations ("finality"). In countries around the world, central banks have become the designated institution to pursue this public interest.¹²

In pursuit of this objective, the central bank issues two types of liabilities. One is physical cash (banknotes and coins) for use by the general public, the most common form of money over the centuries and across countries. Physical cash is accepted (ie exchanged for goods and services) by virtue of a combination of its legal tender status (which makes payments with physical cash final) and central banks upholding their commitment to safeguard its value. The other type of liability – commercial banks' deposits with the central bank (ie reserves) – is for use in wholesale transactions. Like cash, central bank money is safe and, with legal support, underpins payment finality. Payments are further supported by central bank credit – essential to oil the payments machine. What makes both forms of

money special is not just that they have no (or very low) credit risk but also that they represent, by construction, the most liquid asset in the system.

History indicates that the most effective and efficient payment system is a two-tier one. In it, banks compete with each other at the interface with ultimate users while the central bank provides the foundation. Commercial banks offer accounts to households and businesses which, in turn, have accounts with the central bank to settle payments among themselves.¹³ In a two-tier system, maintaining confidence in commercial bank money is essential. To do so, several institutional mechanisms have been put in place, with the central bank playing pivotal roles. Ultimately, commercial bank money derives its value from the promise of being convertible into central bank money at par and on demand. In order to buttress that promise, the central bank also acts as the ultimate source of liquidity (ie as lender of last resort). Prudential regulation and supervision – often performed by the central bank – limit the risk of banks’ failure while deposit insurance schemes can help prevent runs and ensure that holders of transaction deposits are reimbursed should a failure occur.

Payment systems are complex markets with multiple participant types. They involve not only banks but also non-bank payment service providers (PSPs) offering payment services to end users. Generally, banks and other PSPs offer consumer-facing or retail services at the “front end”. This can include providing so-called “digital wallets” and mobile interfaces that give users access to their bank account or store credit card details. Some banks and other PSPs play key roles in clearing, settlement and processing at the “back end” (Box III.B).

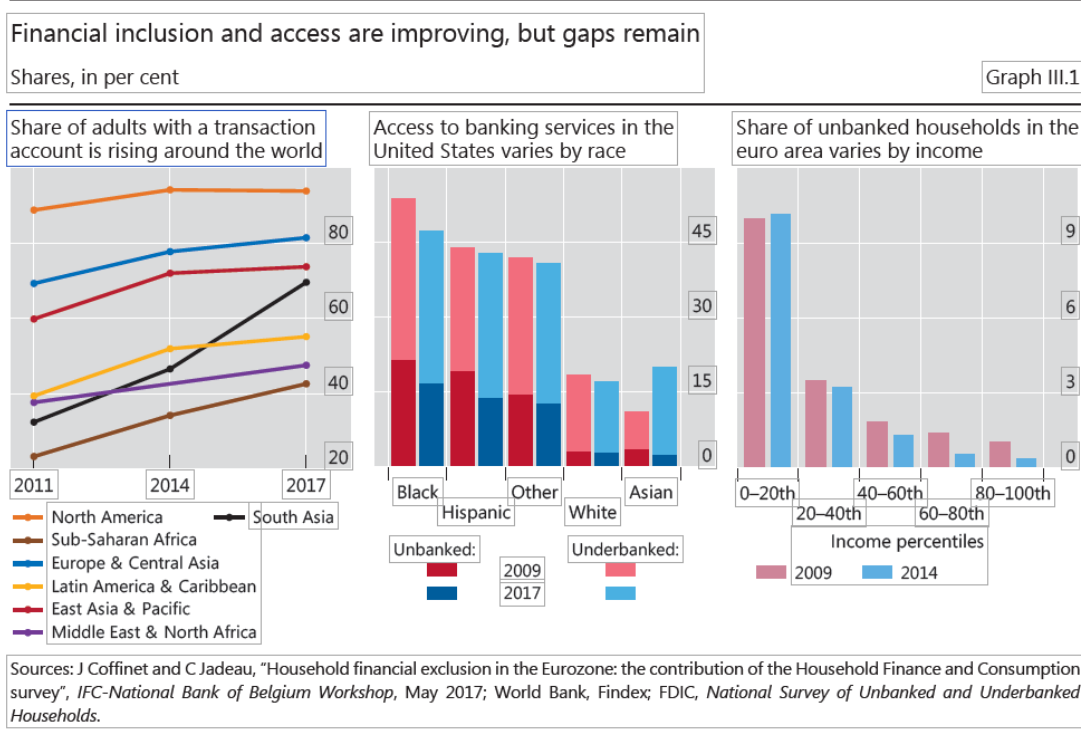
This complexity has some similarity to a town market that brings together different types of buyers and sellers. It may appear complex, but it can be an efficient form of exchange once strong institutional backing is in place. Central banks help organise the payments marketplace by playing the three key roles of operator, catalyst and overseer (Box III.A).¹⁴ They can provide the critical institutional infrastructure, set and oversee implementation of standards, and encourage the provision of a high-quality range of services, thereby promoting innovation and competition.

Central banks can also improve the services they supply directly to ultimate users by staying at the technological frontier. To that end, a number of central banks are considering issuance of CBDCs. CBDCs can serve both as a complementary means of payment that addresses specific use cases and as a catalyst for continued innovation in payments, finance and commerce.

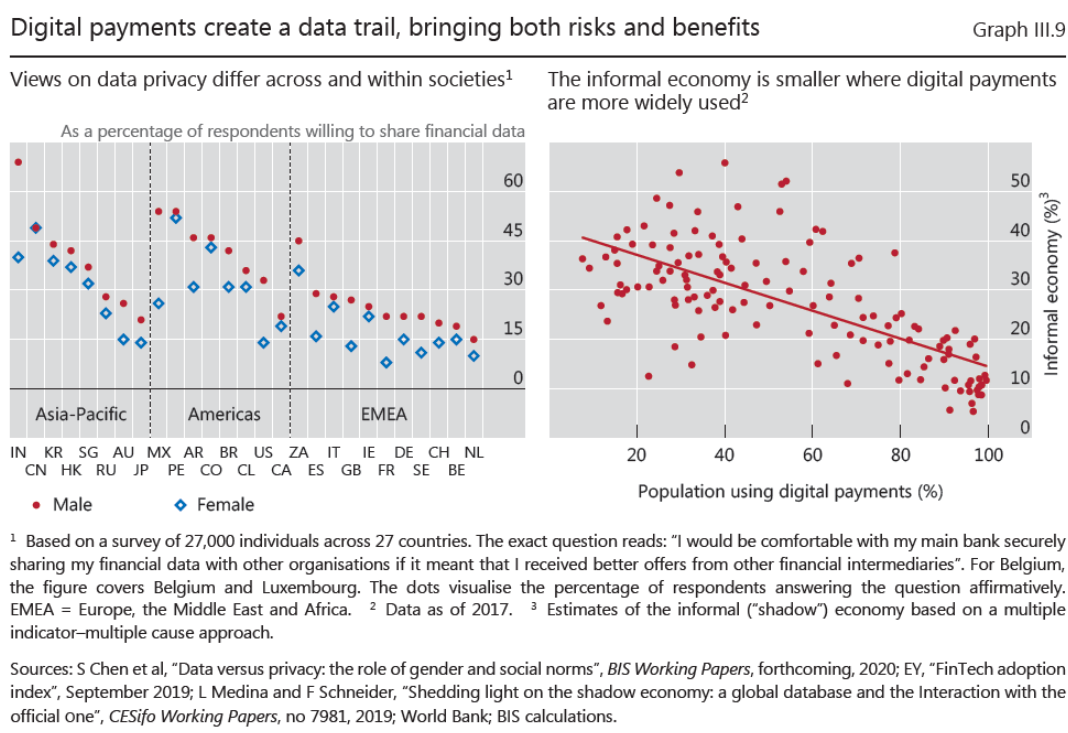
Supporting the payments marketplace also requires preserving its safety and integrity. Just as a sound and smooth functioning payment system underpins economic growth, so can disruptions to a payment system cause major economic damage. Economic activity can grind to a halt if payments do not function. And compromised integrity can lead to a loss of confidence. Localised distress can spread across domestic and international financial markets, extending the damage.

To maintain the safety and integrity of payment systems, the central bank must mitigate various threats. A first threat is systemic risk, which can arise in an interconnected payment system when the inability of a system participant to perform as expected causes other participants to be unable to meet their obligations when due; this can propagate credit or liquidity risks throughout the system. Central banks have expended considerable effort in recent decades to mitigate such risks.¹⁵ A second threat is fraud; wholesale payments, given that they are large-value and complex, are a primary target. A third and related threat is counterfeiting, which applies to cash, and possibly also to CBDCs. A fourth threat is illicit financing and money laundering – the process of disguising the illegal origin of criminal proceeds. In this general context, cyber threats have grown in importance. More than ever, there is a broad range of entry points through which to compromise a payment system. The international community has been actively engaged in mitigating these and other threats, including through work conducted in international organisations and standard-setting bodies.

(...)



(...)



CBDC: designing safe and open payments for the digital economy

CBDCs are a prime example of how central banks can stand at the cutting edge of innovation themselves. Technology – in particular, in the field of digital currency – opens up opportunities for payment systems. CBDCs combine this innovative technology with the tried and trusted foundation of the central bank. It is central banks' choice to harness these forces for the common good. They can combine their role as catalyst, overseer and operator, and develop an entirely new set of payment arrangements that run on digital currencies.

CBDCs have the potential to be the next step in the evolution of money, but a thoughtful approach is warranted. CBDC issuance is not so much a reaction to cryptocurrencies and private sector “stablecoin” proposals, but rather a focused technological effort by central banks to pursue several public policy objectives at once. These objectives include financial inclusion; guaranteeing safety and integrity in digital payments; establishing resilient, fast and inexpensive payments; and encouraging continued innovation in payments.

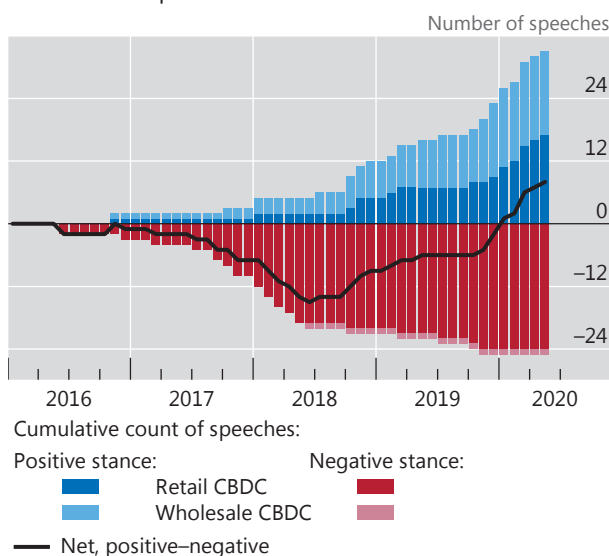
Wholesale digital money is not new – the financial sector has had direct access to such central bank money for decades. However, a wholesale CBDC, if well designed, has the potential to increase efficiency. For example, “programmability” could enable the automatic and near instant delivery of a traded security once a payment is received and verified. In this way, a wholesale CBDC can enhance safety and speed and potentially simplify the post-trade clearing and settlement cycle.⁶¹ A wholesale CBDC could also help mitigate the risk of fraud and cyber attacks; in particular, its technology could improve the irrevocability of digital record-keeping.

The implications of a retail CBDC would be more far-reaching. Such an innovation would provide general users with direct access to central bank money, and potentially offer a safe, reliable and universally accessible settlement instrument – just as cash does now. The benefits would have to be carefully weighed against the implications for the functioning of the financial system, such as the risk of disintermediation, including accelerating bank runs at times of stress, and a potentially larger central bank footprint in the financial system.⁶² The monetary policy implications would also warrant attention. In contrast to cash, retail CBDCs could be interest-bearing, influencing monetary policy transmission, including by reducing the effective lower bound on nominal policy rates.

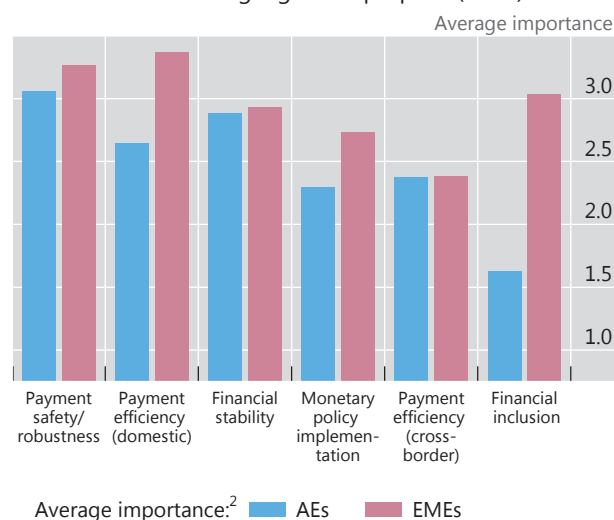
Over the last several years, central banks and policymakers have become more favourably disposed towards issuance of wholesale and retail CBDCs.⁶³ They have featured more positively in central bank communications since late 2019 (Graph III.10, left-hand panel). The motivations for retail CBDCs are numerous and vary across jurisdictions. A 2019 survey of 66 central banks revealed that safety and efficiency of domestic payments are most important, while inclusion is a key motive among emerging market and developing economies (right-hand panel).⁶⁴ Recently, the need to address the declining use of cash has received increasing attention. As consumers migrate to electronic payments, for online transactions as well as in-person purchases, cash usage is declining precipitously in some jurisdictions.⁶⁵ The Covid-19 crisis, and the attendant rise of electronic payments, are likely to boost CBDC development across the globe (Box III.D).

CBDC: an increasingly likely option

Graph III.10

Central bank speeches on CBDC¹

Motivations for issuing a general purpose (retail) CBDC



¹ Search on keywords “CBDC”, “digital currency” and “digital money”. The classification is based on authors’ judgment. The score takes a value of –1 if the speech stance was clearly negative or in case it was explicitly stated that there was no specific plan at present to issue digital currencies. It takes a value of +1 if the speech stance was clearly positive or a project/pilot was launched or was in the pipeline. Other speeches (not displayed) have been classified as neutral. ² 1 = not so important; 2 = somewhat important; 3 = important; and 4 = very important.

Sources: R Auer, G Cornelli and J Frost, “The rise of central bank digital currencies: drivers, approaches and technologies”, forthcoming, 2020; C Boar, H Holden and A Wadsworth, “Impending arrival – a sequel to the survey on central bank digital currency”, *BIS Working Papers*, no 107, January 2020.

Technically, a successful retail CBDC would need to provide a resilient and inclusive digital complement to physical cash. As such, a CBDC must have all the features and more that make cash so attractive. The basic elements are trust in the issuing entity, legal tender status, guaranteed real-time finality and wide availability. But a CBDC must also be equivalent to cash in other dimensions. First, CBDCs need to be user-friendly. Schoolchildren, seniors, and every age group in between handle banknotes and coins with ease; some central banks have even designed features to make banknotes accessible for the blind.⁶⁶ Second, CBDCs must be highly resilient to infrastructure outages and cyber attacks. Such events could wreak havoc if there was a disruption to electronic payments and cash was no longer generally used. Third, CBDCs need to guarantee the safety and integrity of payments. Just like cash, they need to be counterfeit-proof. And just like other digital means of payment, they need to safeguard the user’s privacy while allowing for effective law enforcement. There are opportunities with CBDCs to improve tracing and potentially improve anti-money laundering compliance. But societies’ preference may differ regarding how to balance better tracing with privacy protection.

More generally, CBDCs can coexist with both cash and current electronic payment options. They could be made fully consistent with the two-tiered payment system, allowing the public and private sectors to focus on their respective comparative advantages. Central banks can focus on ensuring trust, stability and integrity in payments. For their part, the private sector is best placed to undertake the consumer-facing activity of CBDCs. Designs would need to mitigate the risk of funds flowing out of banks and into the CBDC, in particular in times of stress. One possibility that is worth exploring is remunerating CBDC holdings at a lower interest rate than the rate paid on commercial bank reserves at the central bank.⁶⁷

Alternatively, central banks could restrict the amount of CBDC that households and businesses can hold, eg through caps.⁶⁸

A substantial role for the private sector raises the need to guarantee compliance with regulatory standards, ensure open competition and allow innovation to flourish. The central bank may grant private sector intermediaries the privilege to distribute CBDC to retail clients, but new entrants and new technologies will be subject to existing regulatory standards. A level playing field is necessary for the sake of incumbents, but also for newcomers. And the technical design and accompanying legal framework should ensure open competition among the various private sector intermediaries, including by avoiding the creation of closed-loop payment systems or introducing frictions when consumers want to switch providers. Guaranteeing open competition also pertains to the collection, use and sharing of data. In particular, starting with a clean slate, the CBDC design should find a new balance between allowing for data portability, safeguarding privacy and mitigating the risks of money laundering and illicit financing.

Ensuring that the retail CBDC allows for ongoing competition requires not only open competition, but also that the central bank operate an infrastructure that fosters innovation. This calls for a flexible and adaptable central bank-operated infrastructure. PSPs must be able to access the CBDC via multiple channels, including back-end interfaces and APIs. A level playing field in terms of access combined with adaptability should foster private sector innovation.

If the CBDC design succeeds in taking these various considerations into account, central banks could harness technological progress in the field of digital currencies and offer a stable and trusted digital unit of account, with guaranteed finality of payments. In this way, CBDCs could become a complementary means of payment that addresses both specific use cases and market failures as well as a catalyst for continued innovation in payments, finance and commerce at large.

That said, research on CBDCs is still in its early stages, and development efforts will take some time. Given their transformative nature, central banks are carefully considering all design options and determining which ones are the best fit for the specific circumstances of each jurisdiction. As insights advance, the exchange of information among central banks is critical. Through tight cooperation, central banks can benefit from peer learning and develop common approaches.

The BIS is closely supporting central banks in their CBDC research and design efforts (Box III.E). The institution is part of an international group of central banks assessing the potential case for CBDC issuance. The BIS Innovation Hub is developing a wholesale CBDC, which will allow for new forms of tokenised trading and settlements.⁶⁹ The BIS-based CPI surveys global CBDC research and development efforts on an annual basis.⁷⁰ In its analytical publications, the BIS continues to shed light on the underlying economic and technological design challenges.

Conclusion

Central banks provide the solid foundation for payment systems, underpinning trust in money while supporting private sector innovation. Over centuries, in their roles as operator, catalyst and overseer, central banks have encouraged the private sector to provide payments that are safe, efficient and widely accessible. The innovations in money and payments that central banks have spurred have promoted increasingly efficient and convenient payments.

While the fundamental roles of central banks in payment systems will endure, payments will continue to evolve. Today, the digitalisation of the economy and

greater access to communication have hastened the replacement of cheques and cash with card and mobile payments. In many parts of the world, cash will continue to decline as a means of payment. Many technologies aim to improve payment access and security, including the use of biometrics. If anything, the demand for faster, more convenient and safer payments is likely to accelerate with the Covid-19 crisis.

Rapid technological progress presents central banks and other authorities with both options and challenges regarding how best to enhance efficiency and adapt payment systems. Across policy options, some general principles apply. First, competition and innovation, notably supported by interoperability, best encourage progress on access, cost and quality. When properly channelled, they can also improve safety. Second, to be successful, private sector innovation should be guided by the public sector with a view to improving efficiency and ensuring safety, integrity and trust. Third, cooperation between the public and private sectors, domestically and internationally, is paramount.

While authorities will foremost need to support competitive private sector markets that harness new digital technologies, new public payment instruments may gain traction. Central banks too can naturally play a key role. In particular, CBDCs, if properly designed, have the potential to give rise to a new payment mechanism that is interoperable by default, fosters competition among private sector intermediaries, and sets high standards for safety and risk management.

The current crisis may accelerate changes in payments – yet it also harbours new risks. Even though the pandemic has underscored the interdependence of countries, policy responses have been primarily national. As authorities have limited cross-border movement and implemented social distancing measures, international economic activity has come to an abrupt halt. Going forward, enhancing coordination and taking steps to prevent or reduce fragmentation in cross-border payment systems are public sector priorities. This is particularly important given that issues of competition policy and data privacy have so far been addressed primarily at the national level and in the light of the rising tide of economic nationalism.⁷¹

Here, too, central banks can be a force promoting international policy coordination, supporting not just domestic payment systems but, above all, their cross-border integration. In international committees such as the FSB and the CPMI, central banks can benefit from peer learning and develop common approaches. In international forums like the G20, central banks and governments can agree on mutually beneficial stances on payment policy. International coordination ensures that advancements in payments support greater efficiency and cross-border integration. International collaboration on innovative financial technology within the central banking community, such as through the newly established BIS Innovation Hub, is accelerating progress on these policy goals.

The rise of digital currency

New entrants are vying to occupy the space once used by paper bills. This column, part of the VoxEU debate on the future of digital money, proposes a simple framework to make sense of who is attempting to pry our wallets open. It argues that the adoption of new digital means of payment could be rapid and bring significant benefits to customers and society, but that the risks must be tackled with innovative approaches and heightened collaboration across borders and sectors. One approach is for central banks to engage in a public–private partnership with fintech firms to provide a safe, liquid, and digital alternative to cash: synthetic central bank digital currency.

A battle is raging...for your wallet. With sharp elbows, new entrants are vying to occupy the space once used by paper bills, or that reserved for your debit card.

Alipay, Libra, M-Pesa, stablecoins – we first need to make sense of just who is attempting to pry our wallets open. We propose a simple framework to do so.

We then argue that the adoption of new, digital means of payment could be rapid. It could bring significant benefits to customers and society, including efficiency gains in payments, greater competition, financial inclusion, and innovation in related sectors. But risks are also paramount to financial stability and integrity, monetary policy transmission, and anti-trust. These must be tackled with innovative approaches and heightened collaboration across borders and sectors.

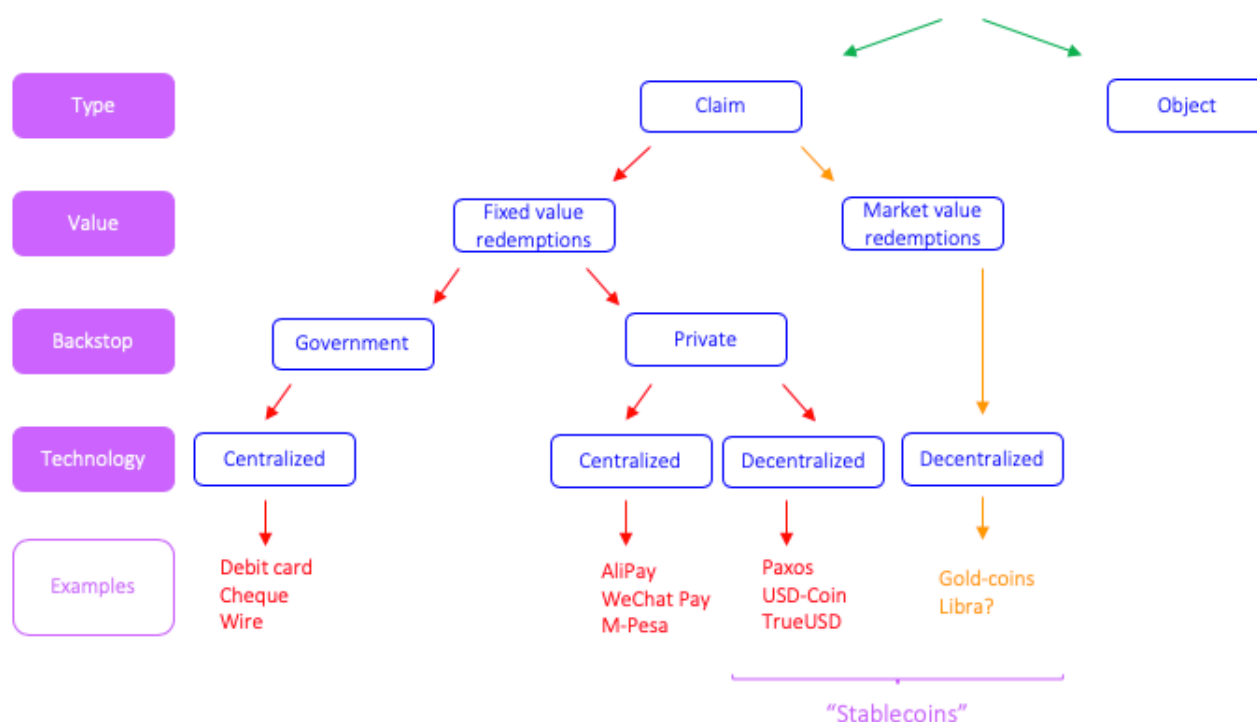
Policymakers will not be able to remain bystanders. In fact, their actions will influence the adoption of new means of payment, and their design. One approach is for central banks to engage in a public–private partnership with fintech firms to provide a safe, liquid, and digital alternative to cash – synthetic central bank digital currency, or sCBDC for short – which comes with its own benefits and risks.

The literature is quickly picking up on the potential disruption caused by new means of payment (e.g. Duffie 2019, BIS 2019).

A framework of analysis

To help make sense of the plethora of new entrants in the payments space, we offer a simple classification scheme that we call the ‘Money Tree’ (Adrian and Mancini-Griffoli 2019). At its heart are four key features that help distinguish different forms of money: type, value, backstop, and technology. We illustrate this scheme in Figure 1 by contrasting bank deposits and stablecoins. Further details and discussions of other forms of money are in Adrian and Mancini-Griffoli (2019).

Figure 1 Simplified money tree to classify different forms of money



Bank deposits are the most popular means of payment in many countries. These are claims on banks, as opposed to objects with intrinsic value. Bank deposits have fixed value to the extent they can be redeemed into currency – or cash – at face value. Ten euros deposited in a bank can be redeemed against a ten-euro note with reasonable certainty in many countries. That is an incredibly useful feature, allowing payments in bank deposits to be made without concern for exchange rate risk.

Trust in the redemption guarantee rests on government backstops: deposit insurance, lender of last resort and emergency liquidity facilities, as well as careful supervision and oversight of banks. And finally, the settlement technology is usually centralised, as banks and central banks collaborate to maintain a shared ledger of account balances.

New means of payment such as stablecoins differ in important ways. Most stablecoins continue to be claims on the issuing institution. Many also offer redemption guarantees at face value – a coin bought for ten euros can be exchanged back for a ten-euro note (a sort of money-back guarantee).

However, trust in this pledge does not rest on government backstops. It must be generated privately by fully backing coin issuance with safe and liquid assets. Finally, the settlement technology is usually decentralised, based on the blockchain model.

Some stablecoins do not offer redemptions at fixed prices, but at market prices instead. We say their value is variable relative to the domestic unit of account. This is the case of commodity tokens, such as gold coins, and of coins that are exchanged or redeemed for the going value of the assets backing them. One example is mutual fund shares written to digital tokens that can be readily exchanged. Libra may fit this model.

Stablecoin adoption

Adoption of new forms of money will depend on their attractiveness as a store of value and means of payment. Cash fares well on the first count, and bank deposits on both. So why hold stablecoins? Why are stablecoins taking off? Why did USD Coin recently launch in 85 countries, Facebook invest heavily in Libra, and centralised variants of the stablecoin business model become so widespread? Consider that 90% of Kenyans over the age of 14 use M-Pesa and the value of Alipay and WeChat Pay transactions in China surpasses that of Visa and Mastercard worldwide combined.

The question is all the more intriguing as stablecoins are not an especially stable store of value. As discussed, they are a claim on a private institution whose viability could prevent it from honouring its pledge to redeem coins at face value. Stablecoin providers must generate trust through the prudent and transparent management of safe and liquid assets, as well as sound legal structures. In a way, this class of stablecoins is akin to constant net asset value funds which can break the buck – i.e. pay out less than their face value – as we found out during the global financial crisis.

However, the strength of stablecoins is their attractiveness as a means of payment. Low costs, global reach, and speed are all huge potential benefits. Also, stablecoins could allow seamless payments of blockchain-based assets and can be embedded into digital applications by an active developer community given their open architecture, as opposed to the proprietary legacy systems of banks.

And, in many countries, stablecoins may be issued by firms benefitting from greater public trust than banks. Several of these advantages exist even when compared to cutting-edge payment solutions offered by banks called fast-payments.

But the real enticement comes from the networks that promise to make transacting as easy as using social media. Economists beware: payments are not the mere act of extinguishing a debt. They are a fundamentally social experience tying people together. Stablecoins are better integrated into our digital lives and designed by firms that live and breathe user-centric design.

And they may be issued by large technology firms that already benefit from enormous global user bases over which new payment services could spread like wildfire. Network effects – the gains to a new user growing exponentially with the number of users – can be staggering. Take WhatsApp, for instance, which grew to nearly 2 billion users in ten years without any advertisement, based only on word of mouth!

Risks of stablecoins

Risks are multiple, though that is not an excuse for policymakers to throw in the towel. On the contrary, they must create an environment in which the benefits of technology can be reaped while minimising risks, as discussed in Lipton (2019). Policymakers will need to be innovative themselves and to collaborate – across countries, but also across sectors. Central bankers, regulators, ministries of finance, antitrust authorities, currency issuers, and technology experts will need to speak a common language for a common purpose.

The first risk is to the disintermediation of banks, which could lose deposits to stablecoin providers. However, banks will try to compete by offering their own innovative solutions and higher interest on deposits. And stablecoin providers could recycle their funds back into the

banking system or decide to engage themselves in maturity transformation by turning themselves into banks.

Second, we could face new monopolies. Tech giants could use their networks to shut out competitors and monetise information. At the heart of this power is proprietary access to data on customer transactions. We need new standards for data protection, control, and ownership.

Third, there is a threat to weaker currencies. In countries with high inflation and weak institutions, people might give up local currencies for stablecoins in foreign currency. This would be a new form of ‘dollarisation’ and might undermine monetary policy, financial development, and economic growth. To avoid this, countries must improve their monetary and fiscal policies. The question is whether they can or should restrict foreign currency stablecoins in the interim.

Fourth, stablecoins could foster illicit activities. Providers must show how they will prevent the use of their networks for activities like money laundering and terrorist financing. This means complying with international standards. New technologies offer opportunities to improve monitoring. So, supervisors will need to adapt to the more fragmented value chain of stablecoins, including wallet providers, crypto exchanges, validation nodes, and investment vehicles.

The fifth risk is loss of ‘seigniorage’. Central banks have long captured, on behalf of taxpayers, the profits stemming from the difference between a currency’s face value and its cost of manufacture. Issuers could siphon off profits if their stablecoins do not carry interest but the hard currency backing them is invested at a return. One way to address this issue is to promote competition so issuers would eventually pay interest on coins.

Sixth, we must ensure consumer protection and financial stability. Customer funds need to be safe and protected from runs like the one that took down Lehman Brothers investment bank. In part, this calls for legal clarity on what kind of financial instruments stablecoins represent.

One approach would be to regulate stablecoins like money market funds that guarantee fixed nominal returns, requiring providers to maintain sufficient liquidity and capital. We could call this the ‘shadow banking’ approach, which attempts to extend prudential regulation beyond the classic banking perimeter.

Synthetic central bank digital currency (sCBDC)

Another option is the ‘narrow banking’ approach. In this case, the central bank could require stablecoin providers to back coins with central bank reserves. The approach is not unheard of. The People’s Bank of China requires giant payment providers AliPay and WeChat Pay to abide by these standards, and central banks around the world are considering giving fintech companies access to their reserves – though only after satisfying a number of requirements related to financial integrity, interoperability, security, and data protection, among others.

Clearly, doing so would enhance the attractiveness of stablecoins as a store of value. Competition with banks would only grow stronger. The social price tag is up for debate.

But there are also clearer-cut advantages of offering stablecoin providers access to central bank reserves:

1. stability, given the backing in perfectly safe and liquid assets;
2. regulatory clarity as narrow banks would fit neatly into existing regulatory frameworks;
3. interoperability among stablecoins (as client funds would be exchanged between reserve accounts) and thus greater competition;
4. support for domestic payment solutions rivalling foreign currency stablecoins offered by monopolies that are hard to regulate; and
5. better monetary policy transmission, thanks to lower pressure on currency substitution, and more immediate transmission of interest rates if reserves held by stablecoin providers were remunerated.

A final consideration jumps out: if stablecoin providers held client assets in reserves at the central bank, clients would essentially be able to hold, and transact in, central bank liabilities. That, after all, is the essence of CBDC.

Bingo! We have thus manufactured what we call synthetic CBDC (sCBDC). We remain, however, fully aware that the stablecoins are the liability of private-sector firms despite the public determining the size of central bank liabilities.

sCBDC offers significant advantages over its full-fledged cousin. The latter, discussed widely in the literature and envisioned by central banks, requires getting involved in many of the steps of the payments value chain. This can be costly and risky for central banks. Steps include interfacing with users and managing brand reputation; complying with integrity standards; offering clients an interface to hold and trade the payment instrument; picking, managing, and evolving technology; offering a settlement system; and managing data and monitoring transactions.

In the sCBDC model – which is a public–private partnership – central banks would go back to focusing on their core function: providing trust and efficiency by means of state-of-the-art settlement systems. The private sector – stablecoin providers – would be left to satisfy the remaining steps under appropriate supervision and oversight, and focus on their own competitive advantage – innovating and interacting with customers.

Whether central banks adopt CBDC at all is another matter and will result from carefully weighing pros and cons. But to the extent central banks wish to offer a digital alternative to cash, they should consider sCBDC as a potentially attractive option.

That is only one of the incarnations of stablecoins. Others will no doubt materialise and colour the future of payments and the financial industry. If anything, existing players will be induced to offer new and more attractive services in the payments – and especially cross-border payments – space. From desktop publishing, the digital revolution has finally reached the shores of consumer finance too.

Editor's Note: The views expressed are those of the author(s) and do not necessarily represent the views of the IMF and its Executive Board

Tobias Adrian
Tommaso Mancini-Griffoli

The Riksbank proposes a review of the concept of legal tender

The Riksbank proposes that a committee with broad-ranging expertise shall be tasked with performing a review of the concept of legal tender and of the role of central bank money in a digitalised economy. The committee should also review the role and responsibility of both the state and the private sector on the payment market. The digitalisation of payment may lead to cash not being generally accepted in the future. This, in turn, may lead to the general public no longer having access to central bank money, which can affect the function and efficiency of the entire payment system. The proposal is being put forward in a petition to the Swedish Riksdag.

The Riksbank has supplied different forms of money to the general public for 350 years. Furthermore, banknotes issued by the Riksbank were given constitutional status as legal tender as a result of the 1809 Instrument of Government[1]. Cash use has decreased rapidly in Sweden and a scenario within the not-too-distant future, in which cash is not generally accepted, cannot be ruled out. This would be tantamount to a cashless society. The general public no longer having access to any form of central bank money can make it more difficult for the Riksbank to promote a safe and efficient payment system in Sweden, not just in times of crisis and war but also in peacetime. The Riksbank has previously expressed concern over this development and has therefore analysed the scope for introducing a Central Bank Digital Currency (CBDC), an “e-krona”, to which the general public has access.

“We think that the concept of legal tender should be technically neutral so that it fulfils a function even in a digital future”, says Stefan Ingves.

The Riksbank therefore proposes that a committee with all-round expertise be tasked with performing a review of the concept of legal tender, the state’s role with regard to means of payment in a digitalised economy and the role and responsibility of both the state and the private sector on the payment market. The committee should propose the legislative amendments needed so that Sweden continues to have a stable and efficient payment market. As time is of the essence regarding this issue, the time-frame for the assignment should not be too long.

[1] An earlier version referred to the constitutional status being adopted in the 1850s, but the decision was actually taken in connection with the 1809 Instrument of Government. This correction has also been made in the petition.

La Chine mise sur les devises 2.0 après le lancement du Libra

La version digitale du renminbi, peut-être lancée dès cette année, présentera des similarités avec la devise de Facebook. Dans un contexte tendu avec l'administration Trump, ce lancement est une réponse à la domination du dollar et mainmise redoutée de Washington sur les devises 2.0.

La deuxième économie mondiale veut être la première à se lancer dans l'aventure des devises 2.0, et l'initiative de Facebook n'est pas étrangère à cette ambition. « *La Chine voit dans le Libra une menace économique et géopolitique. Elle est mécontente depuis longtemps de la domination du dollar dans le système financier mondial et s'inquiète à l'idée de voir un groupe américain dominer le monde futur de la monnaie digitale* », souligne Martin Chorzempa économiste au Piie.

La future monnaie digitale chinoise, peut-être lancée avant la fin de l'année, aura des similarités avec le Libra dans sa conception, a déclaré Mu Changchun, directeur adjoint du département paiements de la banque centrale chinoise, sans en être une simple copie. En juillet, il avait déclaré que l'adoption du Libra dans certains pays pourrait inciter leurs populations à abandonner leurs propres monnaies. « *Nous devons faire en sorte d'éviter que des monnaies comme celle-ci deviennent des monopoles.* »

Wang Xin, directeur de la recherche de la Banque populaire de Chine, avait été encore plus explicite dans un contexte de tensions et guerre commerciale avec les États-Unis. Le succès de la devise de Facebook aboutirait à un monde « *avec un seul patron, le dollar et les États-Unis* ». Derrière le géant américain, c'est la mainmise de Washington sur les devises 2.0 qui est redoutée par Pékin.

Politique monétaire

La banque centrale de Chine travaillait sur ce projet depuis 2014, et a créé trois ans plus tard un département spécifique qui a déposé un certain nombre de brevets relatifs aux technologies des devises 2.0. Après le lancement du Libra en juin, elle a accéléré la cadence et a commencé à dévoiler son projet le mois dernier.

La devise digitale pourra être utilisée sur WeChat et Alipay, a confirmé la Banque populaire de Chine. C'est au travers des banques, et notamment des grandes banques publiques, que les particuliers auront accès à ces renminbis dématérialisés. Ils assureront un certain anonymat, assurent les autorités. « *[Celles-ci] pourraient décider que cette monnaie délivre des taux d'intérêt à leurs détenteurs. Une baisse des taux inciterait les particuliers à l'utiliser pour consommer et à ne pas la thésauriser. Cette possibilité d'agir sur les taux renforcerait l'efficacité de la politique monétaire* » explique Takahide Kiuchi, économiste chez Nomura.

Cette nouvelle initiative doit aussi permettre d'accélérer l'internationalisation du renminbi, un projet de long terme de Pékin, et l'accroissement de son influence hors des frontières. Les chinois émigrés à l'étranger pourront envoyer de l'argent à leur famille par ce biais et éviter de payer les frais des sociétés de transfert d'argent. Garantie infalsifiable et sûre, cette devise digitale est aussi une réponse au fléau de la contrefaçon de billets en Chine.

Nessim Aït-Kacimi

Could Facebook's Libra Affect National Economies and Interest Rates?

Facebook's proposed "simple global currency," known as Libra, has drawn skepticism, scrutiny, and debate since it was announced in 2019. European and US regulators are concerned about an American corporate behemoth harnessing blockchain cryptocurrency technology to dominate an important range of financial services. Nevertheless, on August 23, Bank of England governor Mark Carney delivered a speech that referred to Libra and highlighted some potential benefits of a coordinated move toward a global standard based on a basket of existing currencies, which he labeled a "synthetic hegemonic currency." Concerns that Libra might replace national currencies and pose significant challenges for macroeconomic policymakers are overblown, however, at least in advanced economies.

Even if Libra gains traction, local currencies are likely to continue to be used for most transactions, with Libra limited to the most globally tradable goods and services. National central banks would retain the power to set domestic monetary conditions. There could be some impact on the average level of interest rates, however: Libra is backed by a basket of safe bonds and bank deposits, much like a mutual fund. As these are bought, interest rates in countries whose currencies are in the basket may decline. Interest rates in countries with currencies outside the basket may rise modestly.

As Martin Chorzempa discusses in a previous post, the basket of currencies is intended to give Libra coins a more stable value than bitcoin and other cryptocurrencies. Transactions using Libra could become cheaper and faster than conventional payments. The global reach of Facebook and other companies sponsoring Libra has led to predictions that it will be used extensively as payment for goods and services and to advertise or invoice prices. Libra could conceivably become an alternative to local currency bonds and bank deposits as an investment for households and firms.

But for advanced economies, which have sound monetary policy frameworks, salaries, rents, and local services will continue to be invoiced and paid for in national currency. Taxes, after all, need to be filed and paid in local currency, and government spending (a large share of GDP) is conducted in local currency too. The ability of even very small and open economies to avoid using the currencies of their neighbors reflects the sticking power of national currencies. With most prices and wages set in local currency, national central banks will continue to control the monetary conditions that matter for macroeconomic stabilization.

The Libra Association says that it does not plan to pay interest on Libra balances, making them less attractive as an investment. However, given the current low, and even negative, level of interest rates in many advanced economies, zero interest on Libra balances may not look so bad. Moreover, it is possible that Libra will pay interest in the future, making it fully competitive as a safe and liquid investment. By giving ordinary households a ready alternative to local currency deposits, Libra may increase the sensitivity of a country's exchange rate to changes in its policy interest rate. But this effect would be relatively minor because firms and wealthier households, which control the bulk of all financial assets, already have easy access to foreign exchange.

The primary macroeconomic effect of Libra is likely to be on the level of interest rates and the market for sovereign debt. Widespread adoption of Libra would increase the demand for the securities that back Libra coins, pushing up their prices and reducing their rates of return. Economies with currencies in the Libra basket will experience upward pressure on exchange rates and downward pressure on interest rates. Conversely, economies with currencies outside the Libra basket will experience downward pressure on exchange rates and upward pressure on interest rates as their residents sell local assets for Libra tokens, thereby reducing overall demand for local assets.

These effects will depend critically on the choice of currencies and weights in the Libra Reserve basket as well as the size of the Libra Reserve, which in turn depends on the extent to which Libra is viewed as a safe and convenient investment, including in developing economies with a history of unstable and inflationary local currencies.

Some studies imply that holdings of US assets as foreign exchange reserves, which exceed \$6 trillion, may have depressed US interest rates by several percentage points. However, the fact that US interest rates are among the highest in advanced economies, despite the massive holdings of dollars as reserve assets, suggests that cross-border investment in dollars has only a modest effect on US interest rates, probably less than one percentage point. It seems unlikely that Libra would move rates by more than a percentage point. Nevertheless, even modest downward pressure on interest rates in Japan and the euro area would be unwelcome as long as interest rates are below zero. In these economies, Libra may intensify the need for an enhanced role for fiscal policy in moderating economic downturns. Investing in assets with a negative rate of return could also make it harder for the Libra Association to meet its expenses.

Facebook announced that the Libra Reserve basket will “include the US dollar, the British pound, the euro, and the Japanese yen,” but no indication was given on whether other currencies are also being considered. It is surely no coincidence that these four currencies, along with the Chinese yuan, comprise the special drawing right (SDR) of the International Monetary Fund (IMF). IMF members (which include nearly every country in the world) have pledged to make the SDR the world’s premier reserve asset. Libra offers a chance to make good on this pledge. However, Facebook is not allowed to operate in China, which probably explains its reluctance to include the Chinese yuan in the basket.

If Libra is to become a widespread vehicle for international trade and investment, the composition of the Libra basket should be determined by the international community through an appropriate forum such as the IMF. The SDR basket is an obvious reference point. However, there is also a case to be made for a broader basket in order to spread the costs and benefits more widely and to make the global trading system more symmetric and less subject to the dominance of a single currency or small group of currencies. One way to reconcile these competing considerations is for Facebook to set the Libra basket equal to the SDR basket and for the IMF to broaden the SDR to include the currencies of all economies with sound monetary and fiscal policy frameworks, as discussed on page 28 of this symposium.

**Joseph E. Gagnon
Gonzalo Huertas**

Vers la fin du paiement cash ?



DEEPOL/PLAINPICTURE

DOSSIER

Dans la boulangerie Bo&Mie, à deux pas de la porte Saint-Martin, à Paris, une affiche demande aux clients de « privilégier s'il vous plaît la carte, et notamment le sans-contact », pour plus de rapidité lors du paiement « et par mesure d'hygiène sanitaire ». Depuis que l'épidémie de coronavirus s'est répandue en France, de tels écriteaux pour dissuader l'usage des espèces fleurissent devant les caisses des petits commerces et des supérettes. « C'est à prendre en photo, c'est un moment d'histoire », commente Gilles Grapinet, PDG de Worldline, premier groupe de services de paiement en Europe.

Pour la première fois, au plus fort d'une crise, les Français ne se sont pas rués vers les guichets de leur banque pour retirer des billets et les conserver sous le matelas. Bien au contraire, les retraits de cash aux distributeurs automatiques se sont effondrés. « Entre le début et la fin de la période de confinement, les retraits de billets ont chuté de 50 % en volume, et de 40 % en valeur, du jamais-vu au cours des quinze dernières années », témoigne Erick Lacourrière, directeur général des services à l'économie et du réseau à la Banque de France. Depuis la réouverture des commer-

ces de proximité, le nombre de retraits aux automates bancaires reste encore en retrait de 10 % en valeur et 20 % en volume par rapport à l'an dernier.

« La pandémie de Covid-19 a suscité des inquiétudes sans précédent de la part du public concernant la transmission du virus par le cash », explique la Banque des règlements internationaux (BRI), la banque des banques centrales, dans une étude publiée en avril. Elle précise que le nombre de recherches sur Internet concernant à la fois les mots « billets » et « virus » a atteint des « niveaux records », en particulier en France. Pour rassurer les populations et augmenter la confiance dans les espèces, certaines banques centrales, celle de Corée du Sud, celle de Hongrie et celle du Koweït notamment, ont activement com-

La possible transmission du coronavirus par l'intermédiaire des pièces et billets a favorisé l'accélération des **paiements digitaux**. Même si changer les habitudes prendra du temps, cela pourrait faciliter la transition déjà bien engagée vers une société sans argent liquide

ALORS QUE L'USAGE DES ESPÈCES DÉCLINE, LES BANQUES CENTRALES DE LA ZONE EURO N'ONT JAMAIS ÉMIS AUTANT DE BILLETS

munié sur la stérilisation ou la mise en quarantaine des billets de banque. Pas en France. « Les billets sont, par leur fréquence d'utilisation, les produits les plus échangés par les hommes. Mais ils n'offrent pas un environnement favorable à la survie du Covid, justifie Erick Lacourrière. A la Banque de France, nous avons regardé de près, avec plusieurs laboratoires, le risque de survie des bactéries et des virus sur un billet. Cette durée est plus faible que sur d'autres supports, comme le plastique ou les surfaces métalliques. La charge virale s'affaiblit fortement au-delà de trois heures. »

La méfiance envers les espèces a été nourrie, dès le début de la pandémie, par l'Organisation mondiale de la santé (OMS), dont les recommandations en faveur des moyens de paiement sans contact (en approchant sa

carte bancaire ou son téléphone sur le terminal de paiement du commerçant) ont ensuite été relayées par l'Autorité bancaire européenne (ABE). Le 25 mars, quelques jours après le début du confinement, le régulateur européen des banques a encouragé le relèvement du plafond des paiements par carte sans contact de 30 à 50 euros sur le continent, pour limiter l'usage des billets ou des pièces.

Pendant le confinement, les boutiques ayant baissé le rideau, l'ensemble des flux de paiement ont reculé. Mais la stigmatisation de l'argent liquide a profité aux paiements électroniques, et avant tout au « sans-contact ». Chez les clients de BPCE (Banque populaire Caisse d'épargne), en avril, plus de 60 % des transactions de moins de 30 euros ont été effectuées en mode sans contact, contre 41 % en avril 2019. « De nombreux consommateurs éprouvaient des réticences à passer au sans-contact, par peur de la fraude. Cette période de confinement leur a fait sauter le pas, et il n'y aura pas de retour en arrière », analyse Pierre-Antoine Vacheron, directeur général de Natixis Payments, au sein du groupe BPCE.

NOUVELLES HABITUDES

Toutes les banques ont connu la même accélération. Le Groupement des cartes bancaires, qui centralise les données, note que les paiements de proximité compris entre 0 et 30 euros étaient réalisés à 58 % en sans contact avant le confinement, puis à 66 % dans la semaine qui a suivi le déconfinement. Lorsque, le 11 mai, le plafond des transactions sans contact a été relevé à 50 euros en France, près d'un tiers des paiements par carte CB sur la tranche 30-50 euros est passé en mode sans contact en quelques jours.

« C'est du jamais-vu, l'adoption avait été beaucoup plus lente lorsque le plafond était passé de 20 à 30 euros. Les commerçants ont fait de réels efforts pour mettre à jour leurs terminaux de paiement », constate Julien Lalle, secrétaire général de l'Observatoire de la sécurité des moyens de paiement à la Banque de France. « Nous avons été surpris de ces chiffres très importants, qui vont encore progresser, enchérit Loÿs Moulin, directeur du développement auprès du Groupement des cartes bancaires CB. De nouveaux commerçants vont vouloir s'équiper du mode sans contact, par exemple dans le secteur de l'habillement, parce que le panier moyen est adapté au nouveau plafond de 50 euros, et par intérêt pour les gestes barrières. »

Pièces et billets ont également fait les frais de nouvelles habitudes de consommation prises pendant le confinement, comme le « click & collect », que certaines chaînes de magasins ont proposé au débotté à leurs clients. « Nous l'avons développé très rapidement, pour une enseigne de boulangeries où pour Le Slip français, indique Pierre-Antoine Vacheron. Le consommateur commande et paie en ligne, puis va retirer ses achats. Les Français s'y habituent. » Des soignants convertis à la télémedecine ou des libraires de quartier se sont équipés de solutions de paiement électronique comme Paylib, ou l'application Lydia. Est-ce pour autant le grand soir

David Marcus : « Les crises renforcent les tendances déjà en cours »

Pour le cofondateur de Libra, le projet de monnaie numérique lancé par Facebook, l'essor des transactions électroniques va s'accélérer

ENTRETIEN

David Marcus est actif dans les paiements en ligne depuis l'an 2000. Ex-PDG de l'entreprise de transfert d'argent Paypal, il a cofondé Libra, le projet de monnaie numérique lancé par Facebook avec une vingtaine de partenaires. Il est directeur de Novi (ex-Calibra), le porte-monnaie virtuel que l'entreprise de Mark Zuckerberg veut créer pour populariser Libra et l'intégrer à ses réseaux Facebook, WhatsApp, Messenger et Instagram.

La pandémie liée au coronavirus peut-elle être un point de bascule dans le recul des paiements en liquide ?

Les crises renforcent les tendances déjà en cours. L'essor des transactions électroniques va fortement s'accélérer. Certains disent qu'il n'y aura plus de cash dans cinq ans : je pense que ça va mettre plus longtemps que ça. Mais à un

horizon de vingt ans, l'utilisation des espèces sera vraiment très limitée. Dans les pays où la population aura accès à un smartphone et à des services sur l'Internet mobile, la grosse majorité des transactions sera numérique.

Les obstacles au déploiement des paiements en ligne sont-ils réglementaires, culturels ?

Le problème, c'est la fragmentation des réseaux utilisés pour déplacer de l'argent dans le monde, et c'est ce que nous essayons de résoudre avec Libra. En Europe, les systèmes opèrent en quasi-temps réel et à bas coût, mais ils sont limités aux banques et à l'Europe. On voit en Inde ou en Chine des systèmes de paiement qui marchent très bien localement, mais pas en dehors. Aux Etats-Unis, on a un système antédiluvien qui met trois jours à transférer de l'argent de banque à banque... Cela rappelle le temps où on payait un euro par minute pour appeler les Etats-

Unis depuis la France, 20 centimes d'euros par texto – et ces derniers n'étaient pas interoperables avec certains pays. Internet est arrivé et on a pu bâtir des applications de communication comme WhatsApp, qui permettent d'échanger avec n'importe qui dans le monde, de façon illimitée. Ce que nous essayons de faire avec Libra, c'est un système de transfert d'argent efficace et accessible, concurrentiel et pas contrôlé par une entreprise. Et sur ce réseau seront développés des services, comme Novi, le porte-monnaie de Facebook.

A quoi pourra servir Novi, à payer son pain ?

Aujourd'hui, on ne rencontre pas de problème pour payer son pain à la boulangerie : c'est facile, efficace, pas cher... Libra ou Novi n'apporteront rien de plus. Mais dans des pays qui utilisent principalement des espèces, où des familles dépendent financièrement de proches qui leur envoient de

l'argent depuis l'étranger, une vraie révolution peut se produire. Nous allons pouvoir réduire les coûts et faciliter l'utilisation de services. On espère faciliter les paiements transfrontaliers.

Le cœur de cible de Novi, c'est une famille indienne sans compte bancaire qui reçoit de l'argent d'un proche installé en Californie comme ingénieur ?

Dans un premier temps, oui. Mais, à terme, si une plate-forme et un porte-monnaie vous permettent d'envoyer et de recevoir de l'argent du monde entier, à un coût quasi nul, et sont intégrés avec les services que vous utilisez tous les jours, vous allez l'utiliser de façon plus régulière, pour des paiements domestiques de personne à personne ou pour des paiements en ligne.

Est-ce que, derrière les monnaies numériques, se profile une autre couche de services

comme l'identité numérique, les permis de conduire, etc. ?

Cela va même au-delà : disposer d'une identité numérique et pouvoir la contrôler pour ouvrir de nouveaux comptes, par exemple. Mais d'autres services vont se développer autour de l'argent programmable : sur Libra, nous avons un langage de programmation baptisé Move, qui permet de faire des « smart contracts » [des contrats codés dans la blockchain, un protocole informatique fondé sur la cryptographie et permettant de valider et de répertorier des transactions]. Le contrat s'exécute automatiquement, donc vous n'avez pas besoin d'une tierce partie à laquelle faire confiance.

Par exemple, vous me prêtez 100 euros et je vous rembourse chaque mois cinq euros, avec des intérêts : je suis sûr que des start-up vont proposer un contrat numérique pour automatiser tout cela. Sur une block-

chain, vous pouvez aussi imaginer des prêts à très long terme, des contrats d'assurance. Toute une série de choses pourront être faites sur un réseau comme Libra, pas forcément par Facebook, mais par la communauté qui va y développer des services.

Quand et comment Novi va-t-il se lancer ?

A Novi, nous sommes dépendants du lancement du réseau Libra. Ce dernier est lié à l'obtention d'une licence de paiement auprès de la Finma, l'autorité des marchés financiers de Suisse, où l'association Libra est basée. Nous espérons lancer une première phase du produit Novi avant fin 2020. Nous sommes en cours d'obtention de licences pour pouvoir opérer en tant que porte-monnaie électronique, dans les régions et pays où nous aimerions opérer. Le lancement sera graduel. ■

PROPOS RECUEILLIS PAR VÉ. CH. ET AL. P.

Covid-19, un nouveau coup dur pour le cash ?

Durant l'épidémie, les modes d'achat et la réglementation ont été **défavorables aux pièces et aux billets**

• Retraits

La baisse du nombre de retraits (-40% en valeur au plus fort du confinement) a été plus importante que la baisse de l'activité, signe que la situation était défavorable au cash.

• Refus de paiement

Du fait de l'épidémie, de nombreux refus de paiement en espèces ont été enregistrés. La Banque de France a dû rappeler que ce mode de paiement ne pouvait pas être refusé et que le risque de contamination était faible.



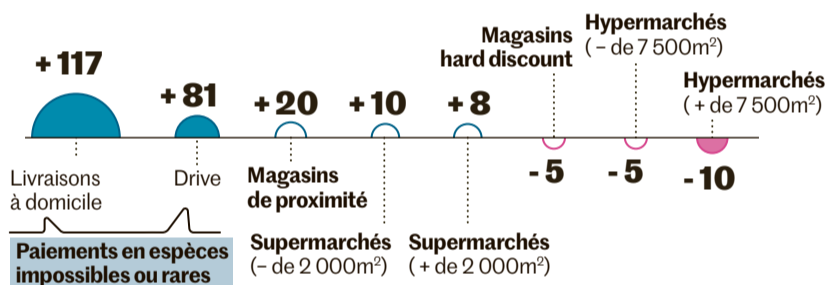
• Panier moyen

Les Français ont fait moins souvent leurs courses mais ont acheté plus à chaque fois, ce qui a grossi leur panier moyen et a ainsi pu décourager le paiement en cash, souvent réservé aux petits achats.

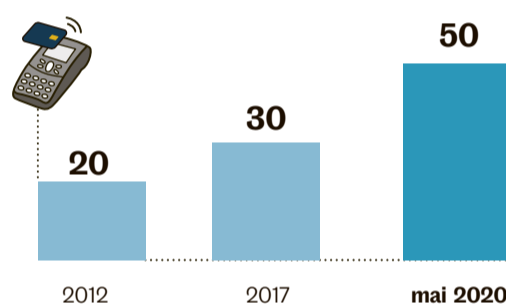
• Sans contact

Le paiement sans contact a été présenté comme un geste barrière par de nombreux acteurs du monde bancaire, ce qui a favorisé son usage.

Evolution des ventes de produits alimentaires en France entre la semaine du 20 au 26 avril 2020 et la semaine correspondante en 2019, en %

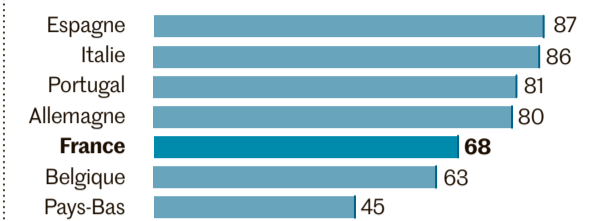


Plafond de paiement sans contact en France, en euros

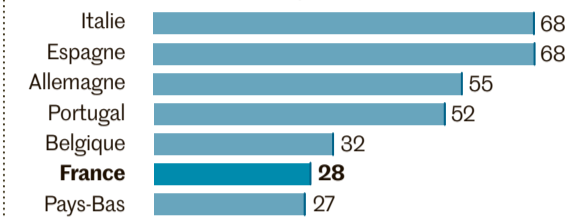


Avant le Covid-19, le cash déjà moins répandu en France qu'ailleurs en Europe

Part du paiement en espèces en point de vente en 2016, en %
...du nombre total des transactions

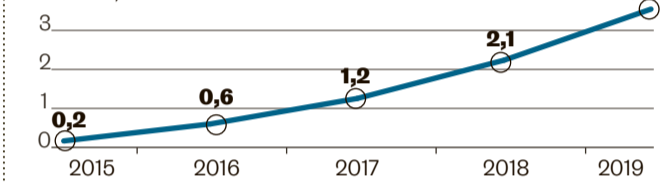


...du total des sommes échangées

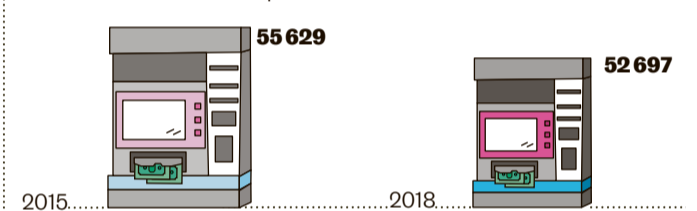


Hausse du sans-contact et raréfaction des distributeurs : symboles d'un cash déclinant

Nombre de paiements sans contact en France, en milliards



Nombre de distributeurs automatiques de billets en France métropolitaine



En 2015, il y avait

107 distributeurs automatiques de billets en France pour 100 000 adultes.

En 2018, ce ratio tombe à **98,3**

Infographie Le Monde : Camille Bressange, Maxime Mainguet • Source : Banque de France, BCE, Banque mondiale, Nielsen, GIE CB

des paiements digitaux ? Le cash, si apprécié des Français, puisqu'il restait jusqu'à la crise sanitaire le moyen de paiement le plus utilisé pour les petits montants, appartiendra-t-il bientôt au passé ? « Je ne crois pas beaucoup aux crises qui retournent les tables, mais à une accélération puissante d'un mouvement déjà engagé », affirme M. Grapinet. Le cash était déjà sur une pente descendante. Au milieu des années 2000, les paiements en espèces soutenaient un cinquième du PIB, l'an prochain ce sera un septième. »

C'est un paradoxe. Alors que l'usage des espèces décline, les banques centrales de la zone euro n'ont jamais émis autant de billets. Actuellement, 1400 milliards d'euros circulent en cash, soit une hausse de 5 % par rapport à 2019 pour la zone euro, et même de 9 % pour la France. « L'appétence des citoyens pour le cash perdure, mais davantage pour constituer un bas de laine et moins pour payer », explique M. Lacourrière. Selon cet expert de la Banque de France, un tiers environ des billets en euros « partent à l'exportation », parce que l'euro, comme le dollar, constitue, en tant que monnaie stable, un instrument de thésaurisation, notamment en Afrique, en Russie, en Europe orientale ou au Moyen-Orient. Un autre tiers des billets imprimés est conservé sous le matelas en Europe. Enfin le dernier tiers sert à payer, mais cette part « évolue à la baisse », constate M. Lacourrière.

Tous les spécialistes du paiement sont d'accord sur un point : les habitudes changent très lentement. La laborieuse progression du paiement mobile (avec un smartphone en sans-contact chez les commerçants) l'illustre bien. Selon la Banque de France, ils ont représenté moins de 1 % des paiements par carte au point de vente en 2019. Le fabricant de l'iPhone croit à l'essor futur de sa solution Apple Pay, dont les transactions ont doublé en un an au niveau mondial et qui est acceptée par 90 % des cartes bancaires et 60 % des points de vente en France. Mais chez BPCE, pionnier d'Apple Pay en France dès 2016, pas l'ombre d'un frémissement n'a été enregistré pendant le confinement.

L'argent liquide ne va donc pas disparaître brutalement. La Banque de France y veille d'ailleurs, « les populations fragiles n'ayant souvent pas d'autres moyens de paiement que le cash », souligne M. Lacourrière. Au cours de la pandémie, l'institution a ainsi dû rappeler

à des commerçants que les espèces bénéficiant du cours légal en France, elles ne pouvaient pas être refusées (sous réserve de certains plafonds), sous peine d'une sanction pénale. « Mais le cash est soumis à des feux croisés », souligne Gilles Grapinet. Le e-commerce est cinq à six fois plus dynamique que le commerce traditionnel, nous achetons de plus en plus de biens virtuels comme des abonnements Spotify ou des jeux en ligne, qu'on ne peut pas payer en espèces. De plus en plus de commerçants proposent de payer avec des "app", comme Uber. »

RÉGLEMENTATIONS ET INNOVATION

Les réglementations ne poussent pas non plus à un développement du cash, « pour des raisons liées à l'économie clandestine, au terrorisme, à la rupture d'égalité face à l'impôt », ajoute-t-il. L'innovation pousse également à l'adoption des paiements électroniques. BNP Paribas teste actuellement une carte bancaire biométrique avec un capteur d'empreintes digitales, qui permet de payer en sans-contact sans être limité par un plafond. Elle sera disponible pour les clients à la fin de l'année. Mais déjà des technologies plus innovantes,

« L'APPÉTENCE DES CITOYENS POUR LE CASH PERDURE, MAIS DAVANTAGE POUR CONSTITUER UN BAS DE LAINE ET MOINS POUR PAYER »

ÉRICK LACOURRIÈRE
directeur général
à la Banque de France

comme les cryptomonnaies, se mettent sur les rangs. Ces devises numériques codées grâce à la blockchain – un protocole informatique fondé sur la cryptographie, permettant de valider des transactions – n'ont pas encore atteint le grand public. Le bitcoin, sa version la plus décentralisée mais aussi la plus volatile, reste cantonné à un public de spécialistes. Libra, le projet commercial lancé en 2019 par Facebook avec 28 partenaires, a connu des revers réglementaires. Mais Bertrand Perez, le président de l'association Libra, reste optimiste : « Le coronavirus est une catastrophe humaine. Mais c'est aussi un catalyseur de tendances : la numérisation des paiements est accélérée. Des gens ont goûté aux achats en ligne et il en restera des traces », croit-il.

Libra espère pouvoir se lancer « avant fin 2020 » après obtention d'une autorisation de l'autorité des marchés financiers suisse, qui travaille en lien avec d'autres régulateurs nationaux. Novi, le porte-monnaie créé par Facebook qui s'appuiera sur l'infrastructure Libra, est « en cours d'obtention d'autorisation » dans plusieurs pays et régions, assure son directeur, David Marcus, le concepteur de Libra. Libra se veut particulièrement attractif pour

les « quatre milliards d'exclus du système financier sur la planète, dont un milliard possède déjà un smartphone », assure M. Perez. Mais les premières devises numérisées seront des versions électroniques des grandes monnaies. Novi espère séduire les amateurs de transferts internationaux, mais aussi les personnes qui voudront échanger de l'argent entre particuliers ou faire des achats sur Facebook et ses filiales WhatsApp et Instagram, auquel il sera intégré. Les géants du numérique croient à l'arrivée de nouveaux usages : la solution de paiement mobile Google Pay numérise déjà des cartes de fidélité (Etam, Mr Bricolage...) ou des billets d'avion (Air France...), comme le fait celle d'Apple. Et le fabricant de l'iPhone imagine gérer un jour des documents d'identité ou des permis de conduire. Libra aussi, explique David Marcus, qui évoque même des contrats numériques de propriété, de prêt ou d'assurance. Les banques françaises se disent sceptiques. « On jugera du succès ou de l'échec de libra dans dix ans », avance dans un sourire le créateur de la cryptomonnaie créée par Facebook.

VÉRONIQUE CHOCRON
ET ALEXANDRE PIQUARD

Les banques centrales réfléchissent aussi sur leur « e-monnaie »

DANS LE SECRET de ses dorures très XIX^e siècle, la vénérable Banque de France travaille sur des innovations de pointe, telle que la blockchain, cette technologie permettant de transmettre des informations de façon sécurisée pour réaliser des paiements. Le 14 mai, elle a ainsi testé l'utilisation d'une « monnaie digitale de banque centrale » – les experts parlent de « MDBC » – pour régler une émission de titres financiers par la Société générale. Dès juillet, elle mènera dix autres expérimentations avec des partenaires choisis par appel à projets. « Il existe deux grands types de MDBC : l'une directement adressée au grand public, offrant un moyen de paiement complémentaire au cash ; l'autre, destinée aux règlements entre les banques », précisent Nathalie Aufaivre, directrice générale de la stabilité financière

et des opérations, et Valérie Fasquelle, directrice des infrastructures, de l'innovation et des paiements. « C'est cette deuxième forme que nous expérimentons, avec la blockchain ».

D'après la Banque des règlements internationaux, 80 % des banques centrales de la planète étudient aujourd'hui la possibilité de créer une monnaie digitale, et 10 % en sont au stade du projet pilote. Avantage pour les particuliers, une monnaie aussi sûre et disponible, sans intermédiaire, qu'un véritable billet. Dans les pays émergents, l'objectif est surtout d'améliorer l'inclusion financière. L'Equateur teste ainsi un « e-peso » permettant les paiements par SMS, depuis un portefeuille numérique.

Dans les économies avancées, il s'agit plutôt de coller à l'évolution des usages, comme la disparition du cash :

la Suède, par exemple, développe une « e-couronne » apte à remplacer pièces et billets. Mais l'enjeu est aussi « de ne pas prendre de retard sur l'innovation et de continuer à la soutenir, tout en assurant la sécurité des règlements », ajoutent M^{mes} Aufaivre et Fasquelle.

Guerre d'influence

En la matière, la montée en puissance du Bitcoin, né en 2008, et le lancement programmé de Libra, la cryptomonnaie de Facebook dévoilée en juin 2019, inquiète les grands régulateurs financiers. « Si leur usage se déploie, ces e-monnaies pourraient perturber le fonctionnement des politiques monétaires traditionnelles », explique Aditi Kumar, spécialiste du sujet à Harvard.

En arrière-plan, une guerre d'influence géopolitique se dessine éga-

lement, ajoute-t-elle. Depuis avril, la Chine expérimente ainsi un yuan digital dans quatre villes, et espère élargir l'expérience en 2022. « Son émergence pourrait défier la suprématie du dollar dans les systèmes de paiement internationaux », détaille M^{me} Kumar. Suprématie que les Etats-Unis utilisent pour imposer des sanctions aux entreprises européennes commerçant avec l'Iran, par exemple.

C'est aussi l'une des raisons pour laquelle les instituts monétaires européens planchent sur le sujet. Car si le projet fonctionne et est généralisé, la MDBC de la Banque de France pour les règlements interbancaires aiderait à renforcer le rôle de l'euro à l'international. Et permettrait à la zone euro de s'affranchir du dollar. ■

MARIE CHARREL

Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud

A Wall Street Journal analysis of 1,450 cryptocurrency offerings reveals

Hundreds of technology firms raising money in the fevered market for cryptocurrencies are using deceptive or even fraudulent tactics to lure investors.

In a review of documents produced for 1,450 digital coin offerings, The Wall Street Journal has found 271 with red flags that include plagiarized investor documents, promises of guaranteed returns and missing or fake executive teams.

“Jeremy Boker” is listed as a co-founder of Denaro, an online-payment project. In investor documents for a public offering in March, which claimed to have raised \$8.3 million, Mr. Boker boasted of his cryptocurrency startup’s “powerhouse” team. In his biography, he noted a “respectable history of happy clients” in consulting before he launched Denaro.

In fact, Mr. Boker’s bio image was a stock photo, there is no evidence he exists and the rest of his team appears to be fictional, except for two freelancers who said they were paid by people unknown to them to market the project, the Journal found.

The principals behind Denaro couldn’t be identified and attempts to reach the company went unanswered. The real person whose image was repurposed as Mr. Boker’s turns out to be Jenish Mirani, a banker in Poland. Mr. Mirani, who had posted the photo on his personal website, said “it was really shocking” to find out about its afterlife.

Investors have poured more than \$1 billion into the 271 coin offerings where the Journal identified red flags, according to a review of company statements and online transaction records—nearly one in five of those reviewed. Some of the firms are still raising funds, while others have shut down. Investors have so far claimed losses of up to \$273 million in these projects, according to lawsuits and regulatory actions.

Companies use coin offerings to raise funds by selling their own digital currency. Led by the bitcoin fever, the 1,450 projects analyzed by the Journal—a number believed to encompass most of those aimed at an English-speaking audience since 2014—say they have raised at least \$5 billion. Since 2017, cryptocoin offerings have generated more than \$9 billion in proceeds globally, according to research and data firm Satis Group.

Recently, the Securities and Exchange Commission issued warnings to investors that many deals in the booming private market for cryptocurrencies could be violating securities laws, and on Wednesday launched a website touting a fake coin offering as an example of what to avoid.

Since December the agency has filed civil charges against companies and individuals in four separate cases involving initial coin offerings, known as ICOs. At least a dozen companies put their offerings on hold after the agency raised questions, an SEC official said in February.

At the heart of most coin offerings is a company’s “white paper,” a document that typically details mission statements, team biographies and the technical specifics of a project.

Of the 1,450 white papers downloaded from three popular websites that track coin offerings, the Journal found 111 that repeated entire sections word-for-word from other white papers. The copied language included descriptions of marketing plans, security issues and even distinct technical features such as how other programmers can interact with their database.

Shane Shifflett
Coulter Jones

Digital Currencies, Stablecoins, and the Evolving Payments Landscape

Governor Lael Brainard

At The Future of Money in the Digital Age, Sponsored by the Peterson Institute for International Economics and Princeton University's Bendheim Center for Finance, Washington, D.C.

Technology is driving rapid change in the way we make payments and in the concept of "money." There is a long history of technological advances challenging the prevailing notions of money, from the trading of coins to the use of paper currency, to the electronic debiting and crediting of funds on the accounts of banks. Today, efforts by global stablecoin networks such as Facebook's Libra to establish the next chapter in the story of money are raising threshold questions about legal and regulatory safeguards, financial stability, and monetary policy. Because of its potential global reach, Facebook's Libra imparts urgency to the debate over what form money can take, who or what can issue it, and how payments can be recorded and settled.

Reassessing Money

Money has traditionally served three functions. Money facilitates payments as a medium of exchange, serves as a store of value that can be relied on for future use, and simplifies transactions by providing a common unit of account to compare the value of goods and services.

A decade ago, Bitcoin was heralded as a new kind of digital money that would address frictions in payments as well as serve as a unit of account and store of value without the need for centralized governance. Bitcoin's emergence created an entirely new payment instrument and asset class exchanged over a set of payment rails supported by distributed ledger technology. Distributed ledger technology may allow for a shared, tamper-resistant ledger that can be updated by anyone with sufficient computing power, in contrast to traditional recordkeeping systems built on a single ledger managed by a trusted central entity. But Bitcoin and some other early iterations of cryptocurrencies have exhibited extreme volatility, limited throughput capacity, unpredictable transaction costs, limited or no governance, and limited transparency, which have limited their utility as a means of payment and unit of account.⁵

Stablecoins were designed specifically to overcome the substantial volatility exhibited by first-generation cryptocurrencies, which limits their reach in payments and their utility as a unit of account. As the name implies, stablecoins aim to maintain stable value by tying the digital currency to an asset or basket of assets, such as commercial bank deposits or government-issued bonds. Stablecoins also differ from the initial set of cryptocurrencies in that they may be issued by a central entity and rely on third-party institutions for some aspects.

Just as any currency's value as a medium of exchange increases with the size of the network using it, so too the power of a stablecoin payment system will depend on its ability to achieve widespread adoption, due to the associated network externalities. In light of the 2.7 billion active monthly users on Facebook's platforms, the Libra stablecoin project stands out for the speed with which its network could reach global scale in a payment system.

To assess the efforts by stablecoin issuers to provide the three functions of money, it is useful first to consider existing arrangements for the issuance, regulation, and transfer of money. Central bank money and commercial bank money are the foundations of the modern financial system. Central bank money is composed of physical cash and money held in deposits at a central bank. Central bank money is important for payment systems because it represents a safe settlement asset, allowing users to exchange central bank liabilities with confidence in their acceptance and reliability. In addition, central banks can play a critical role as providers of liquidity by lending central bank money at moments of stress.

Commercial bank money refers to money held in deposits at commercial banks. It is widely used in part because people are confident that they can convert it on demand to the liability of another commercial bank or the central bank, such as physical cash. This confidence comes in no small part because bank deposits are insured, and commercial banks are subject to supervision, regulation, and deposit insurance requirements. Consumers and businesses also use this money in transactions because of its convenience and availability, which in turn expand with the size of the network using this money.

Nonbank private money or assets can also facilitate transactions among a network of users. In some cases, such as airline miles, such assets may have value only within the network. In other cases, the issuer of an asset within a network may guarantee convertibility to a sovereign currency. Consumers trust that the company issuing such money will be able to honor these liabilities. Many U.S. consumers have experience with nonbank private money in the form of gift cards, loyalty points, and virtual gaming currencies. Although many of these are relatively limited in scale and purpose, some nonbank money networks are sizeable. Starbucks reported that it had \$1.6 billion in stored value card liabilities as of September 2018—more than the deposits held at many depository institutions.

As the scale and scope of such private networks grow, so too do the convenience and benefit of transacting within the network in a self-reinforcing dynamic, called network externalities. These network benefits may be augmented by the active use of network data for a host of purposes, from allocating and pricing credit to sharing reviews to prioritizing information that is pushed to users. In China, consumers and businesses participate in two mobile networks, Alipay and WeChatPay, which by some accounts handled more than \$37 trillion in mobile payments last year. These networks operate within China based on the renminbi as the unit of account, and balances are transferable in and out of bank or credit card accounts.

Stablecoins with Global Scale and Scope

Stablecoins may resemble private nonbank liabilities depending on their design and claim structure. Stablecoins aspire to achieve the functions of traditional money without relying on confidence in an issuer—such as a central bank—to stand behind the money. Indeed, for some potential stablecoins, a close assessment suggests users may have no rights with respect to the underlying assets or the system overall.

We have seen the growth of massive payments networks on existing digital platforms, such as Alibaba and WeChat, and the issuance of stablecoins on a smaller scale, such as Tether, Gemini, and Paxos. What sets Facebook's Libra apart is the combination of an active-user network representing more than a third of the global population with the issuance of a private digital currency opaquely tied to a basket of sovereign currencies. It should be no surprise that Facebook's Libra is attracting a high level of scrutiny from lawmakers and authorities.

Libra, and indeed any stablecoin project with global scale and scope, must address a core set of legal and regulatory challenges before it can facilitate a first payment. I will emphasize a few issues in particular.

First, compliance with know-your-customer rules and regulations are essential to ensure stablecoins are not used for illegal activities and illicit finance. Libra's business model is inherently cross-border, and, as such, each participant in the system deemed to be a financial institution would need to ensure compliance with each national jurisdictions' anti-money-laundering laws. Libra's intended global reach would likely necessitate a consistent global anti-money-laundering framework in order to reduce the risk of illicit transactions.

Second, issuers of stablecoins designed to facilitate consumer payments must clearly demonstrate how consumer protections would be assured. Consumers will need to be educated on how their rights differ with respect to digital wallets compared to bank accounts. In the United States, as elsewhere, statutory and regulatory protections have been implemented with respect to bank accounts so that consumers can reasonably expect their deposits to be insured up to a limit; fraudulent transactions to be the liability of the bank; transfers to be available within specified periods; and clear, standardized disclosures about account fees and interest payments. Not only is it not clear whether comparable protections will be in place with Libra, or what recourse consumers will have, but it is not even clear how much price risk consumers will face since they do not appear to have rights to the stablecoin's underlying assets. Consumers need to be cautioned that stablecoins are likely to be starkly different from sovereign-issued currency in legal terms. It will be important to get clarity on what legal entity can be held responsible for the security of personally identifiable information and transaction data and how personal data will be stored, accessed, and used. The large number of cyber breaches in the last few years highlight the importance of these issues.

Third, it will be necessary to define the financial activities that the various players in the Libra ecosystem are conducting in order for jurisdictions to assess whether existing regulatory and enforcement mechanisms are adequate. As the legal domicile of the Libra Association, Switzerland is of particular interest. Swiss authorities have established three new categories to facilitate their approach of regulating by function: "payment tokens" are cryptocurrencies that are meant for use in payments or value transfers; "utility tokens" are blockchain-based applications; and "asset tokens" are cryptoassets that are analogous to equities, bonds, and

derivatives. To the extent that some innovations do not fit neatly within a single category, these classifications may not be mutually exclusive.

In the United States, regulators are closely examining the specific functions of particular stablecoins and cryptocurrencies more broadly to determine whether and where they fit in the existing regulatory structure and whether additional authorities or guidance is necessary. U.S. market regulators have authorities for products judged to be securities or commodity futures under relevant law. At the state level, the New York State Department of Financial Services has established a BitLicense for entities associated with virtual currencies. The Federal Reserve and the other federal banking agencies have supervisory authority over banks, including, in many cases, the ability to regulate and examine companies that provide services to banks. Neither the Federal Reserve nor any other regulator has plenary authority over payment systems operating in the United States. Although the Financial Stability Oversight Council does have the authority to designate systemically important nonbank financial companies; financial market utilities; or payment, clearing, and settlement activities based on the facts of the specific situation, it is not clear at this time whether any cryptocurrency issuer would meet the statutory requirements for designation.

Stablecoins, and cryptocurrencies more generally, challenge the long-held premise that payments must be recorded in a central ledger managed by a single entity. In fact, banks were established to perform this central ledger function. Distributed ledger technology allows for the direct peer-to-peer transfer of assets, potentially eliminating the need to transact through intermediaries. While distributed ledger technology could offer advantages by enhancing operational resilience, increasing transparency, and simplifying recordkeeping, the public and immutable nature of the transactions ledger also introduces risks, such as data privacy concerns and legal complexity.

Global stablecoin networks also may pose challenges to bank business models. In the extreme, widespread migration to one or more global stablecoin networks could disintermediate the role of banks in payments. If consumers and businesses reduce their deposits at commercial banks in favor of stablecoins held in digital wallets, this could shrink banks' sources of stable funding, as well as their visibility into transactions data, and thereby hinder banks' ability to provide credit to businesses and households. That said, many banks are likely to adapt by offering alternative methods of peer-to-peer settlement and by incorporating stablecoins into their business models, whether by partnering with fintech firms who issue stablecoins or by issuing their own, as some are already doing.

Moreover, widespread adoption of stablecoins could have implications for the role of central banks and monetary policy. Payments are the economy's circulatory system. Large-scale migration into a new stablecoin network for purposes of payments may prove to be the leading edge of a broader migration. If a large share of domestic households and businesses come to rely on a global stablecoin not only as a means of payment but also as a store of value, this could shrink demand for physical cash and affect the size of the central bank's balance sheet. The central bank's approach to implementing monetary policy may be complicated to the extent that banks' participation in short-term funding markets is affected.

These effects are likely to be more significant for small, open economies or those with weak monetary institutions, where the migration away from the sovereign currency to a global stablecoin could weaken the scope for independent monetary policy through a process that is the digital analogue of dollarization. Large-scale stablecoin use could also affect larger, advanced economies with extensive connections to the global financial system, including by increasing market volatility and by transmitting shocks across borders.

Finally, there are likely to be financial stability risks for a stablecoin network with global reach. If not managed effectively, liquidity, credit, market, or operational risks—alone or in combination—could trigger a loss of confidence and a classic run. A global stablecoin network raises complicated issues associated with many legally independent but interdependent operations, and the lack of clarity about the management of reserves and the rights and responsibilities of various market participants in the network. The potential for risks and spillovers could be amplified by potential ambiguity surrounding the ability of official authorities to provide oversight and backstop liquidity and to collaborate across borders.

Central Bank Digital Currencies

Even before the advent of stablecoins, the rapid migration of payments to digital systems prompted interest in the issuance of central bank digital currencies. In some jurisdictions, there has already been a pronounced migration from cash to digital payments, which naturally prompts monetary authorities to explore moving to digital issuance of their own.

The potential for global stablecoin systems has intensified the interest in central bank digital currencies. Proponents argue that central bank digital currencies would be a safer alternative to privately issued stablecoins because they would be a direct liability of the central bank.¹⁶ For instance, Markus Brunnermeier, Harold James, and Jean-Pierre Landau provide important arguments.¹⁷

Of course, the Federal Reserve and other central banks already provide money digitally in the form of central bank deposits in traditional reserve or settlement accounts. However, in the current context, central bank digital currency typically refers to a new type of central bank liability that could be held directly by households and businesses without the involvement of a commercial bank intermediary. Under this definition, central bank digital currency could be a flexible form of central bank money that could differ from traditional reserves along three dimensions: a much broader set of institutions and individuals could access it, some types of balances might not pay interest, and it might entail greater government visibility into end users' transactions.

In the United States, there are compelling advantages to the current system. First, physical cash in circulation for the U.S. dollar continues to rise, suggesting robust demand. Second, the dollar is an important reserve currency globally, and maintaining public trust in the sovereign currency is paramount. Third, we have a robust banking system that meets the needs of consumers: our banks are many in number, diverse in size, and geographically dispersed. Finally, we have a widely available and expanding variety of digital payment options that build on the existing institutional framework and the applicable safeguards.

Moreover, central bank digital currency for general purpose use—that is, for individual consumer use—would raise profound legal, policy, and operational questions. Let's consider the balance between privacy and illicit activity. If it is designed to be financially transparent and provide safeguards against illicit activity, a central bank digital currency for consumer use could conceivably require the central bank to keep a running record of all payment data using the digital currency—a stark difference from cash, for instance. A system in which individual payments information would be recorded by a government entity would mark a dramatic shift. A related question is whether the Federal Reserve has the authority to issue currency in digital form and, if necessary, to establish digital wallets for the public.

There could also be profound monetary policy implications. Some economists have argued that a central bank digital currency could address the problems posed by the zero lower bound by potentially transmitting monetary policy directly to the public. Executing monetary policy in such a manner would effectively imply the elimination of all physical cash and the power to impose a negative rate, or a tax, on households' holdings of digital money. My own strong preference is to address the effective lower bound by using our existing tools vigorously, since I view the cost-benefit assessment of negative rates as unattractive for the current U.S. context.

Financial stability considerations are also important. The ability to convert commercial bank deposits into central bank digital currency with a simple swipe surely has the potential to be a run accelerant. Here, too, the role of banks in providing financial intermediation services could be fundamentally altered.

Finally, there could be operational risks to introducing a central bank digital currency. For starters, this might require the Federal Reserve to develop the operating capacity to access or manage individual accounts, which could number in the hundreds of millions. A myriad of other operational challenges would need to be addressed, including electronic counterfeiting and cyber risks. It is worth noting that the technologies used currently for private-sector digital currencies do not provide the same level of information technology reliability, integrity, and scalability as central bank systems in use today. Many of these technologies do not provide for clear, predictable, and final settlement, which is a core tenet of payment systems.

That said, some jurisdictions may move in this direction faster than others, based on the particular attributes of their payments and currency systems. At the Federal Reserve, we will continue to analyze the potential benefits and costs of central bank digital currencies and look forward to learning from other central banks.

Supporting Payments Innovation

While prudence cautions against rushing into untested approaches to central bank digital currencies, we are actively investing in our payments infrastructure, so that everyone has access to real-time payments. Every day, U.S. payment and securities settlement systems turn over roughly \$12.5 trillion. The Federal Reserve is committed to working closely with the private sector to promote a safer and more efficient payments system.

This summer, we announced that the Federal Reserve will launch the first new payment service in more than 40 years to help make real-time payments available to everyone. The Federal Reserve will develop the FedNowSM Service as a platform for consumers and businesses to send and receive payments immediately and securely 24 hours a day, 7 days a week, 365 days a year. This initiative is intended to provide a neutral platform for new private-sector innovation in faster payment services. In addition to FedNow, we are exploring enhancements to same-day settlement of automated clearinghouse (ACH) transactions and expansion of Fedwire[®] Funds Service and National Settlement System operating hours. We are working with the industry to improve the security of the payments system by, for example, increasing understanding of synthetic identity fraud and identifying a fraud classification approach to improve information sharing.

As the public and private sectors work to reduce payment frictions, one of the most important use cases is for cross-border payments, such as remittances. Intermediation chains for cross-border payments are long, slow, cumbersome, and opaque. Technology enables e-commerce to transcend national borders, but current cross-border payments solutions often represent complicated workarounds rather than seamless end-to-end solutions. Authorities in different jurisdictions recognize the importance of cooperating across borders with each other and the private sector to address the very real cross-border frictions that exist today.

Concluding Thoughts

Our nation has rich and varied experiences to draw on as we assess various proposals for private money, from the period in our history when the colonial states each issued their own currencies to the many decades when the circulation of private commercial banknotes stood in for a national currency. The Federal Reserve was created in part to respond to the inability of many of these banks to make good on their obligations for the banknotes they issued and the panics and runs that ensued. Those experiences will help inform us as we potentially enter another phase in the evolution of money and payments.

Today, consumers and businesses have a variety of payment options, including physical cash, checks, ACH transfers, debit cards and credit cards, and mobile-based payment solutions, to name a few. These tend to have clearly defined legal rights and responsibilities. We will likely see far-reaching innovation in payments in the coming years, with a plethora of new and emerging options, including stablecoins.

The Federal Reserve remains confident in the power of technology and innovation to transform the financial system and reduce frictions and delays, while preserving consumer protections, data privacy and security, financial stability, and monetary policy transmission and guarding against illicit activity and cyber risks. Given the stakes, global stablecoin networks should be expected to meet a high threshold of legal and regulatory safeguards before launching operations. We are monitoring new technologies closely to ensure that the innovations that arise fit with our operational responsibilities and broader public policy goals, as reflected in the Federal Reserve Act. At the same time, we are upgrading our services to support innovation in new ways. And, we will continue to foster a safe and efficient payments system, including where money in all its myriad forms—present and future—is concerned, as we have for over a century.