puissance des ordinateurs rendent le système beaucoup trop compliqué à gérer et à réguler, et à plus forte raison à comprendre.

Le plus inquiétant dans cette affaire, c'est que le principal cadre que nous utilisons pour guider l'activité macroéconomique est fondé sur des paradigmes dépassés. Les modèles généralement utilisés pour régir la création de monnaie et les taux d'intérêt, par exemple, traitent encore les banques privées comme de simples intermédiaires, en ignorant le fait qu'elles constituent des protagonistes majeurs, qui créent activement de l'argent. Les banques ont leurs propres motivations, et leurs stratégies pour engranger des bénéfices introduisent dans le système une grande opacité. Il n'est guère étonnant que la crise des *subprimes* (prêts hypothécaires à risque) de 2008 ait été difficile à voir venir.

Il faudrait modéliser le très complexe circuit monétaire actuel avec un luxe de détails sans précédent pour que nous puissions le comprendre. Les limites technologiques ont longtemps rendu impossible une tâche aussi pharaonique. Mais avec la disponibilité de données massives ainsi que l'émergence des monnaies virtuelles et des contrats numériques, la situation est en train de changer. Plutôt que de s'appuyer sur des moyennes historiques pour estimer ce qui pourrait arriver à un système économique donné, il devient enfin possible de simuler la totalité des échanges et transactions individuels et d'en analyser toutes les conséquences possibles. Cette perspective est en passe d'ébranler le fonctionnement et l'idéologie de la finance globale, et ses implications pourraient grandement améliorer la sécurité économique – ou la dégrader considérablement…

Il y a à peine une dizaine d'années, des techniques autorisant une réinvention de notre système financier sont apparues. Presque tout le monde a entendu parler du bitcoin, mais ce dernier n'est qu'un élément d'une vaste industrie montante de technologies financières, caractérisée par le buzz et la spéculation. Ce qu'il est important de savoir, c'est que l'invention centrale est un « registre distribué », une base de données partagée et gérée par de multiples participants – une sorte de système informatisé et commun de comptabilité.

LES BLOCKCHAINS, TECHNOLOGIE FONDATRICE DES CRYPTOMONNAIES

Ce registre distribué constitue la technologie fondatrice qui a rendu possible l'avènement de cryptomonnaies – des monnaies cryptées numériquement – telles que le bitcoin. Sa structure de données sous-jacente, nommée blockchain, ou chaîne de blocs, consiste en une série de blocs enchaînés les uns à la suite des autres, chaque bloc regroupant un grand nombre de transactions sous forme de données numérisées. La chaîne est mise à jour de façon consensuelle par ajouts de nouveaux blocs au moyen de divers mécanismes de « preuve » faisant intervenir à la fois des humains et des ordinateurs (*voir l'article de John Pavlus, page 28*).

Conceptuellement parlant, les chaînes de blocs et les registres distribués ne sont pas nouveaux; par exemple, des enchaînements se produisent naturellement chaque fois que du pouvoir, des terres ou des biens changent de mains. Ce qui est nouveau, c'est l'association des deux concepts dans un système informatique infalsifiable qui peut être appliqué à un grand éventail de problèmes pratiques. Grâce aux nouvelles techniques de registres distribués fondés sur les blockchains, il est possible de créer des devises numériques beaucoup plus efficaces que le dollar américain ou l'euro, et même plus efficaces que le bitcoin.

Ces outils nous permettraient de suivre et d'analyser les transactions à un niveau suffisamment granulaire pour que nous puissions enfin comprendre le circuit monétaire. Avec un niveau de clarté sans précédent, nous pourrions apprendre à reconnaître de précoces signaux d'alerte se manifestant dans les milliers de milliards de transactions consignées dans le registre, et réagir de façon appropriée, ce qui augmenterait la stabilité et la sécurité du système.

Ce type de suivi à livre ouvert en temps réel serait également plus sûr pour l'ensemble de la communauté. Dans le krach de 2008, par exemple, la capacité administrative était insuffisante pour traiter les pertes individuelles de dizaines de millions de citoyens. En conséquence, les régulateurs se sont concentrés sur le sauvetage des grandes banques, relativement peu nombreuses, laissant les individus ordinaires payer le prix fort. >

BIBLIOGRAPHIE

J. Barrdear et M. Kumhof, **The macroeconomics of central bank issued digital currencies**, document de travail n° 605, Banque d'Angleterre, juillet 2016.

A. Lipton, **Modern monetary circuit theory, stability of interconnected banking network, and balance sheet optimization for individual banks**, *International Journal of Theoretical and Applied Finance*, vol. 19(6), article 1650034, 2016.

T. Hardjono *et al.* (éd.), **Trust : Data. A New Framework for Identity and Data Sharing**, Visionary Future, 2016.

A. Laurent et V. Monvoisin, **Les nouvelles monnaies numériques : au-delà de la dématérialisation**

> À l'heure où cette technologie en évolution rapide commence à être exploitée pour des applications de plus en plus nombreuses et variées, la confusion règne dans de nombreux esprits. Comme le bitcoin est actuellement la forme de monnaie numérique la plus connue (en bien ou en mal, les avis sont partagés), il est utile de revenir un peu en arrière pour explorer ses origines et ses faiblesses, et comprendre en quoi elle diffère des versions plus prometteuses qui sont maintenant à l'étude.

La monnaie bitcoin a été conçue comme un système de paiement numérique pair à pair qui fonctionne sans autorité centrale. N'importe qui peut y adhérer, ce qui est à la fois une force et une faiblesse. Les utilisateurs effectuent entre eux des transactions financières directes (par exemple l'achat d'un bien), sans l'aide d'intermédiaires. Ces transactions sont inscrites dans un registre à blockchain distribué publiquement, que tous les participants peuvent (théoriquement) voir. Depuis la création du bitcoin en 2009, son cours a augmenté de plusieurs ordres de grandeur, ce qui en fait la coqueluche des spéculateurs.

Les promesses du système des bitcoins sont grandes. Ses partisans – essentiellement des idéalistes et libertaires férus de technologie, mais aussi certains criminels – s'attendent à ce que le bitcoin devienne une devise mondiale qui finira par supplanter les devises nationales, facilement manipulables selon eux. Certains enthousiastes voient même dans le bitcoin une version numérique de l'or, oubliant peut-être que l'or tient sa stabilité à la fois de ses attributs physiques et de ses milliards de détenteurs, et que dans le monde numérique les bonnes techniques sont régulièrement dépassées par de meilleures encore.

Le bitcoin n'est d'ailleurs pas la première monnaie virtuelle, et ce ne sera très probablement pas la dernière non plus à jouer dans la cour des grands. Elle souffre par ailleurs de sérieuses contraintes logistiques.

LE BITCOIN N'EST PAS LA PANACÉE

Par exemple, le nombre de transactions qui peuvent être traitées à chaque seconde tourne autour de 7, à comparer avec les 2000 que traite en moyenne le système Visa de cartes de paiement.

De plus, c'est un gouffre à énergie : le minage (le processus par lequel les membres du réseau de cryptomonnaie se font la compétition pour ajouter de nouveaux blocs de transactions à la blockchain, et ainsi gagner des bitcoins) consomme une énorme quantité d'électricité. Dans les pays où l'électricité coûte cher, les mineurs font rapidement faillite s'ils ne peuvent honorer les factures d'électricité des systèmes informatiques. On ne connaît pas les chiffres exacts, mais on estime que le système des bitcoins consomme autant d'électricité qu'eBay, Facebook et Google réunis.

Le bitcoin a également été mis en place pour que l'autorité soit répartie entre de nombreux mineurs ; or en se rassemblant pour former de gigantesques pools, un petit nombre de groupes sont devenus suffisamment puissants pour contrôler le système. Peut-on encore parler de pair à pair ?

L'utilisation du bitcoin est de plus limitée. Le terme « monnaie » peut être défini par ses trois types d'utilisation : pour les transactions, comme réserve de valeur et en tant qu'unité de compte. Comme le cours du bitcoin par rapport aux monnaies légales, reconnues par les États, est extrêmement instable, il est difficile à utiliser au quotidien. Le bitcoin et l'ether, une autre grande cryptomonnaie, ne sont pas couverts par des biens réels ni même par des engagements gouvernementaux. Par conséquent, ils sont purement spéculatifs. En termes familiers, cela signifie que ces monnaies numériques ne sont pas de l'argent « véritable » : ce qui n'a pas de valeur ne peut avoir de prix. Certains enthousiastes du bitcoin présentent cette absence de valeur comme un avantage et affirment que, dans le futur, tout l'argent sera du même type que le bitcoin. Cela est hautement improbable, pour des raisons à la fois techniques et politiques.

Cependant, en tant que première monnaie virtuelle décentralisée prospère, le bitcoin

À PROPOS DES AUTEURS

ALEXANDER LIPTON
a fondé une jeune entreprise, StrongHold Labs. Il a auparavant occupé plusieurs hautes fonctions à la Bank of America, et des postes de professeur invité à l'université d'Oxford et à l'Imperial College de Londres.

ALEX « SANDY » PENTLAND
**dirige le laboratoire Human Dynamics du MIT, et est notamment membre de l'Académie d'ingénierie des États-Unis.
Son dernier ouvrage en date est *Social Physics* (Penguin Books, 2015).**