L'ESSENTIEL

> Augmenter la transparence du système financier moderne réduirait les risques qui lui sont associés, mais cela suppose de modéliser le circuit monétaire à un niveau de détail qui dépasse les capacités techniques actuelles.

> Avec les cryptomonnaies, il est désormais possible de mémoriser et analyser tous les échanges ou transactions. Ces outils permettraient d'élaborer des réseaux financiers plus efficaces et de décentraliser le contrôle de l'argent.

> Bien conçus et utilisés, ces réseaux numériques favoriseront l'équité et la responsabilité. Mais ils pourraient tout aussi bien servir à un contrôle centralisé extrême.

LES AUTEURS

ALEXANDER LIPTON
membre du groupe MIT Connection Science à l'institut de technologie du Massachusetts (MIT), aux États-Unis

ALEX « SANDY » PENTLAND
professeur au MIT et directeur du groupe MIT Connection Science

Faire sauter la banque avec des cryptomonnaies

Les monnaies numériques fondées sur la technologie des blockchains ont un fonctionnement transparent. Elles préfigurent peut-être de nouveaux réseaux financiers qui mettront un terme à la concentration des richesses et qui stimuleront l'économie.

Par une belle journée de printemps, il y a plus de cinq mille ans, dans la cité mésopotamienne d'Ur, un commerçant étranger vendit sa marchandise en échange d'une bonne quantité de métal précieux, de l'argent. Il ne voulait pas ramener ce lot chez lui, sachant qu'il reviendrait à la fin de la saison des moissons acheter du grain. Il décida donc plutôt de se rendre au temple local, où étaient souvent conservés des objets de valeur, et demanda au prêtre de garder le lot d'argent pour lui.

Quelque temps après, le neveu du prêtre se présenta chez son oncle pour solliciter un prêt. Il souhaitait acheter des semences pour avoir ses propres récoltes, souhait qui fit vibrer la corde sensible de l'oncle. Ce dernier prêta donc au jeune homme une partie de l'argent qu'on lui avait confié, faisant le raisonnement que si jamais son neveu ne parvenait pas à le rembourser avant que le commerçant étranger ne le lui réclame, il pourrait remplacer le métal manquant en puisant dans ses fonds propres ou emprunter l'équivalent auprès de ses amis. En utilisant un contrat à long terme avec le commerçant pour financer un prêt à court terme à son neveu, le prêtre doublait le nombre de transactions commerciales effectuées avec le même montant. En d'autres termes, il avait inventé le système de « réserves fractionnaires » (ou de « couverture partielle »).

D'après des données archéologiques, nous savons que des scénarios de ce type se sont joués en Mésopotamie. Et cela a profondément changé l'environnement financier de deux façons : tout d'abord, en augmentant la productivité globale de l'économie – ainsi, le neveu était désormais en mesure de se payer des semences ; en second lieu, en introduisant le risque – puisque le neveu ne serait peut-être pas en mesure de rembourser l'argent à temps.

Quelques millénaires plus tard, dans l'Europe du XVII^e siècle, l'émergence de banques centrales adossées aux États a créé le lien entre de telles « doubles dépenses » et la perception de taxes. Le roi empruntait de l'argent aux marchands afin de financer ses guerres ou la construction de routes, et l'utilisait pour payer >

© Borja Bonaque

> les fabricants et fournisseurs d'armes, ainsi que ses troupes. Cet argent commençait à circuler et à engendrer de l'activité économique et des profits, et à chaque étape la quantité d'argent était doublée (ou plus). Généralement, le roi remboursait les prêts à l'aide des impôts levés sur les bénéfices. L'ensemble de ce processus constituait un prototype de circuit monétaire qui a marqué la naissance du système bancaire en vigueur aujourd'hui.

Très schématiquement, le circuit moderne fonctionne de la façon suivante. Tout d'abord, une entreprise emprunte de l'argent à des banques privées telles que JPMorgan Chase ou HSBC pour payer les salaires de ses employés et d'autres frais. C'est l'étape où la monnaie est créée. Puis les consommateurs achètent les biens produits par les entreprises ou déposent leurs liquidités sous forme d'économies à la banque. Enfin, ces entreprises utilisent les sommes qu'elles ont perçues pour rembourser les banques, et la boucle est bouclée. À ce stade, l'argent prêté au départ disparaît, mais les intérêts versés restent dans le système.

C'est ainsi que les banques privées peuvent stimuler les économies en créant de la monnaie *ex nihilo*. Leur capacité à procéder de la sorte est régulée en partie par les banques centrales, qui imposent des limites à la quantité de capital et de liquidités que les banques privées doivent toujours détenir pour financer leurs activités de prêt.

LE SYSTÈME MONÉTAIRE ACTUEL EST DEVENU TROP COMPLIQUÉ À GÉRER ET À RÉGULER

Si seulement tout était si simple ! Le circuit monétaire introduit hélas des problèmes de société fondamentaux. Pour commencer, il se crée inévitablement une poignée de milliardaires qui contrôlent une vaste concentration de la richesse totale. Il est également affligeant de voir combien il est courant de créer de la monnaie par le crédit (par effet de levier) sans en comprendre suffisamment les risques ou s'en soucier. C'est ainsi que se produisent les krachs financiers, tel celui de 2008 : quand les banques et les autorités politiques ont encouragé une demande insatiable d'emprunts, cette demande a été satisfaite par une augmentation notable de la masse monétaire créée, et une augmentation encore plus grande du risque.

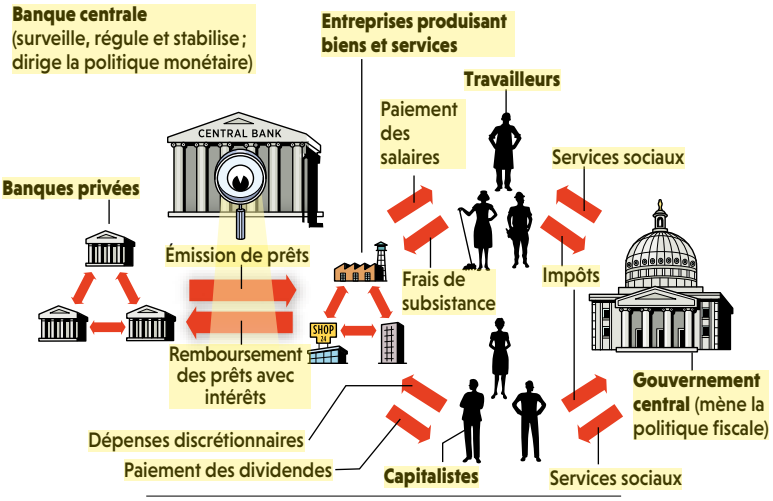
Il peut sembler évident d'imputer ces problèmes au circuit financier lui-même. Mais ce n'est pas le fond de la question. La création d'argent par effet de levier fonctionne bien tant que nous sommes capables de comprendre et de maîtriser ses risques inhérents tout en empêchant une concentration indésirable de richesses. Mais aujourd'hui, un écheveau de facteurs tels que l'explosion démographique, l'internationalisation du commerce et la

TROIS TYPES DE SYSTÈMES FINANCIERS

Le circuit monétaire actuel est devenu trop complexe pour être compris. Des technologies émergentes à « chaînes de blocs », ou blockchains, comme celle qui sert de base au bitcoin, décentralisent (et clarifient) le système. De nouveaux réseaux, tel celui du tradecoin, sont en cours de développement.

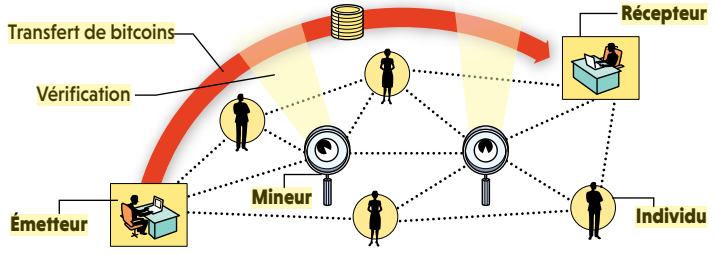
LE SYSTÈME DE RÉSERVES FRACTIONNAIRES (CIRCUIT MONÉTAIRE ACTUEL)

Les banques créent de la monnaie *ex nihilo* lorsqu'elles émettent des prêts aux entreprises. Les entreprises paient les salaires et les dividendes aux ménages. Les ménages achètent des biens et des services aux entreprises. Quand les prêts sont remboursés, la monnaie « créée » est détruite, mais les intérêts versés restent dans le système.



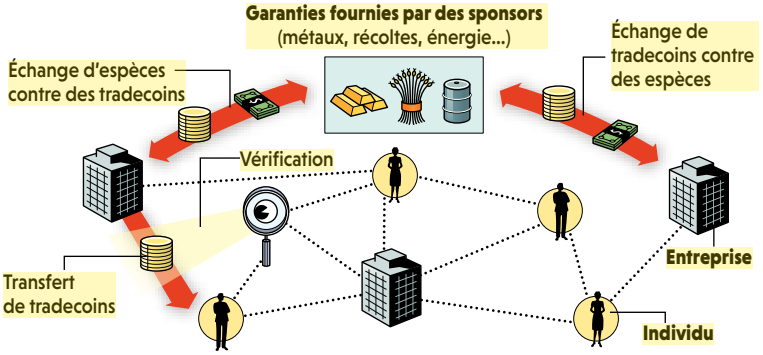
LE RÉSEAU PAIR À PAIR DU BITCOIN

Les transactions se font directement entre utilisateurs, sans l'aide d'intermédiaires désignés. Elles sont publiquement diffusées et enregistrées dans une blockchain. Le consensus est assuré par des « mineurs » qui gagnent des bitcoins s'ils enregistrent de nouveaux blocs. Le bitcoin n'a pas de valeur intrinsèque ; son cours est donc par nature instable.



LE RÉSEAU PAIR À PAIR DU TRADECOIN

Comme avec le bitcoin, les transactions se feront directement entre utilisateurs et seront enregistrées publiquement dans une blockchain. Mais le consensus sera assuré par des validateurs désignés. La valeur du tradecoin sera couverte par des biens réels liés à des sponsors ; son cours sera donc relativement stable.



© Peter et Maria Hoey

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**