D'autres politiques économiques sont possibles
Le blog de Les économistes atterrés
Faites entendre votre voix
Matthieu Montalban
03 Janvier 2018

Bitcoin, crypto-monnaies et blockchain : mirage ou miracle ? (2/2)

On a vu dans l'épisode précédent que le projet sous-jacent au Bitcoin, dont la valeur a pu atteindre des sommets stratosphériques ces dernières semaines avant de subir une correction suite au piratage d'une plateforme d'échange, est en partie critiquable sur le plan de la stabilité macroéconomique comme de ses coûts environnementaux s'il venait à être généralisé. Il n'en demeure pas moins que la technologie sous-jacente, la blockchain, possède des propriétés intéressantes dont les potentialités méritent d'être explorées.

Les potentialités offertes par la blockchain

Pour rappel, la blockchain peut être vue comme un registre transparent, distribué, automatisé et incorruptible de l'ensemble des transactions (ou actions) passées, où chaque participant a accès à une copie du registre. Chaque bloc de transactions est validé et "notarisé" pour toujours. On a déjà vu que la blockchain permet de faire fonctionner des crypto-monnaies, dont le Bitcoin n'est qu'un cas emblématique parmi d'autres. Chaque crypto-monnaie peut fonctionner sur des règles de fonctionnements différentes, tout dépend de l'algorithme de la blockchain sous-jacente.

Ainsi, la Banque centrale du Royaume-Uni réfléchit à la possibilité de mettre en place une monnaie électronique (central bank-issued digital currency ou CBDC). L'idée serait d'adopter des principes d'émissions différents de Bitcoin, mais en utilisant la blockchain[1], c'est-à-dire un registre distribué qui viendrait se substituer aux comptes bancaires traditionnels.

Différentes règles d'émission peuvent être inventées, allant des traditionnelles opérations de refinancement du secteur bancaire ou d'achat de bons du Trésor au paiement direct à la distribution d'un dividende aux citoyens. Dans le cas d'un achat de bons du Trésor, les économistes de la Banque centrale du Royaume-Uni montrent (via leur modèle qu'on ne détaillera ni ne critiquera ici), que le niveau du PIB de long terme pourrait être augmenté de 3% grâce à la baisse des taux d'intérêt réels et à la réduction d'un certain nombre de coûts de transactions et de distorsions fiscales[2].

---

1 https://www.bankofengland.co.uk/research/digital-currencies

2 https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1. Notre objet n'est pas ici de discuter de la pertinence de ce modèle de simulation, basé sur les principes DSGE, qui sont en eux-mêmes critiquables.

De son côté, l'Estonie est en train de réfléchir à lancer sa propre crypto-monnaie (l'*EstCoin*) via une *Initial Coin Offering*, c'est-à-dire une levée de fonds par émission de *tokens* (jetons)[3] ! Quoiqu'on pense de cette évaluation de la Banque centrale anglaise ou du projet estonien, cela montre que les banquiers centraux prennent au sérieux non seulement l'idée d'une monnaie numérique mais aussi la technique *blockchain*.

Cette technique offre en principe des possibilités d'applications très larges. Elle pourrait très bien faire appliquer d'autres règles institutionnelles que celle des crypto-monnaies (c'est-à-dire la règle basée sur la conservation de la valeur dans l'échange). D'où l'idée de l'appliquer à d'autres activités où il y a habituellement besoin d'utiliser des registres ou de faire des transactions ou transferts de droits ou d'actifs, et où des intermédiaires ou des autorités sont là pour assurer le bon fonctionnement du processus. En ajoutant à la *blockchain* un langage de programmation, il est possible de créer de multiples applications. C'est en particulier le cas sur *Ethereum*, une crypto-monnaie alternative à *Bitcoin*, qui permet de construire sur sa plateforme de nombreuses applications, monétaires ou non, via ce qu'on appelle des *smart contracts*.

Les *smarts contracts* ne sont pas des contrats au sens juridique du terme, ce sont simplement des programmes autonomes, qui, une fois démarrés, permettent d'exécuter automatiquement dans des conditions définies à l'avance n'importe quelle règle du jeu social, dont typiquement les contrats *"classiques"*. Ils permettent donc d'exécuter et vérifier automatiquement les termes des contrats ou de faire appliquer les sanctions en cas de non-respect des termes mais également de toute autre règle sociale. Cela pourrait réduire les coûts de transaction, l'aléa moral, les coûts de vérification, d'arbitrage, etc.

On peut même penser à créer un cadastre ou un système notarial numérique où toutes les transactions seraient décentralisées et contrôlées par l'algorithme, laissant entrevoir la possibilité de se passer (au moins dans la partie enregistrement des actes) des notaires – ce qu'expérimentent actuellement l'Estonie et le Ghana[4].

On pourrait aussi par exemple songer à gérer automatiquement l'exécution de certains contrats d'assurance sans intervention humaine, notamment en s'émancipant des phases de déclaration (formulaires, réclamations, etc.).

Par exemple, pour une assurance contre le retard d'un vol, avec une *blockchain*, il serait possible d'être automatiquement indemnisé pour le retard sans avoir à en faire la demande – la limite étant que les compagnies aériennes préfèrent ne rembourser que les clients qui en font la demande. La *blockchain* permettrait aussi d'améliorer la traçabilité des produits et les chaînes logistiques.

De même, on pourrait aussi envisager de se passer de nombreux intermédiaires financiers : un marché financier n'est rien d'autre qu'une plateforme centralisée d'échanges. Avec la *blockchain*, il devient techniquement possible de créer des plateformes décentralisées d'échanges sécurisés de titres entre ménages et entreprises sans passer par la case Wall Street et toute *"l'industrie financière"*. Les banques et *"l'industrie financière"* le savent, c'est pourquoi elles investissent elles-mêmes dans cette technologie pour conserver leur position dominante. Il va de soi que ce serait encore du capitalisme et que cela ne règlerait en rien les pathologies de ce mode de production. En

---

[3] La BCE, à juste titre, s'en émeut.

[4] http://www.journaldunet.com/economie/finance/1176465-estonie-blockchain/ ; https://www.franceinter.fr/emissions/le-zoom-de-la-redaction/le-zoom-de-la-redaction-27-juin-2016 ; https://www.info-afrique.com/cadastre-ghana-blockchain/

l'occurrence, pour le moment, si la *blockchain* en tant que telle est sécurisée, il n'en va pas encore de même de ces plateformes en ligne, deux d'entre elles ayant été piratées[5].

Gouverner les communs

Certains réfléchissent aux applications de la *blockchain* à la gouvernance de communs. La technique pourrait permettre de résoudre des problèmes classiques de coordination et de confiance (problème du passager clandestin par exemple) de manière plus décentralisée que les gouvernances hiérarchiques traditionnelles, tout en créant des systèmes d'incitations non marchandes. Le problème des communs, c'est que la taille de la communauté ne peut s'étendre beaucoup sans faire perdre la confiance et faire augmenter les risques d'opportunisme et de coûts de transaction. La *blockchain* pourrait résoudre une partie de ces problèmes[6].

Il serait également possible d'organiser une économie du partage et collaborative, c'est-à-dire une économie de l'usage partagé des biens et des communs. Ce serait l'occasion de se débarrasser des plateformes de type *Uber* ou *Airbnb* puisqu'on pourrait relier utilisateurs et prestataires en définissant les droits et devoirs de chacun, sans passer par les plateformes qui exploitent les chauffeurs. On pourrait aussi partager des biens en définissant des droits aux usagers de ces biens (qui seraient des objets connectés) et en les faisant appliquer[7].

Des réflexions se développent sur un usage de la *blockchain* pour gérer le dossier numérique de santé du patient et tout son parcours de soins (prescriptions, consultations, maladies, remboursement etc.) qui pourraient être *"notarisés"*[8] dans cette base de données inviolable[9] et économiser un certain nombre de coûts bureaucratiques. Les données du patient seraient sécurisées et il pourrait choisir d'ouvrir son dossier médical aux seuls professionnels de santé qu'il souhaite. Qui plus est, la *blockchain* permettrait d'accumuler des données de santé anonymes pour faire de l'épidémiologie en étant moins dépendant de l'industrie pharmaceutique.

En mettant en place des enregistrements inviolables et transparents, il serait possible d'éviter les manipulations des données que peut pratiquer l'industrie pharmaceutique dans les essais cliniques et de plus facilement mettre en relation les firmes, administrations, Sécu/assureurs, etc.

Les potentialités les plus importantes sont liées à ce qu'on appelle les *Decentralized autonomous organizations* (*organisations autonomes décentralisées ou DAO*), aussi appelées *Distributed collaborative organizations* ou encore plus simplement *decentralized cooperation*. Une DOA est une organisation permettant de se coordonner de manière décentralisée sur un but commun sans autorité centrale en utilisant la *blockchain* pour attribuer, gérer et garantir des droits à ses membres et faire appliquer les

---

5 http://www.lefigaro.fr/secteur/high-tech/2017/12/20/32001-20171220ARTFIG00116-le-cours-du-bitcoin-tangue-apres-le-piratage-d-une-plateforme-d-echange.php ; http://bfmbusiness.bfmtv.com/hightech/une-plateforme-de-bitcoins-se-fait-pirater-pres-de-80-millions-de-dollars-1322265.html

6 Pazaitis A., De Filippi P. et Kostakis (2017) "Blockchain and value systems in the sharing economy : The illustrative case of Backfeed", *Technological Forecasting & Social Change*, http://www.sciencedirect.com/science/article/pii/S0040162517307084

7 C'est le projet de l'entreprise Slock.it par exemple

8 https://blogs.dxc.technology/2017/01/03/blockchain-et-sante-de-nouveaux-usages-vertueux-envisageables-a-moyen-terme/ ; https://mbamci.com/blockchain-et-sante/ ; http://healthcaredatainstitute.com/wp-content/uploads/2015/02/livre-blanc-hdi-2017-web.pdf ; http://www.theconnectedmag.fr/blockchain-nouveau-modele-securite-donnees-de-sante/

9 Précisons que c'est le registre qui est inviolable. Mais une plateforme d'échange de bitcoins ou votre wallet/compte peut se faire pirater. C'est ce qui s'est passé dans les récentes attaques de NiceHash. Pour comprendre, voir : http://www.businessinsider.fr/us/nicehash-bitcoin-wallet-hacked-contents-stolen-in-security-breach-2017-12/ ; https://www.hacker9.com/how-to-hack-bitcoin-system-wallet-password.html

règles[10]. Elle est gérée via les *smart contracts* (la DOA est en quelque sorte un nœud de *smart contracts*).

Une DOA ne peut être fermée ou arrêtée, elle ne peut être contrôlée par aucune personne et elle est transparente et auditable.

La DOA est un moyen de mettre en place une production de communs sur une base décentralisée entre agents en pair à pair qui ne se connaissent pas, grâce à la transparence et au caractère (apparemment) *trustless* (c'est à dire ne nécessitant pas de garant, ou *"tiers de confiance"*) de la *blockchain*.

La première DAO (The DAO) était en quelque sorte une organisation de *crowd funding* (finance collaborative) : chaque membre de la DAO possédait des *tokens* (jetons) qui donnaient des droits de vote, et la communauté devait choisir d'allouer ses fonds aux projets qui lui apparaissaient les plus intéressants.

Une DAO est au fond une sorte d'entreprise dont les règles sont implémentées par le code informatique des *smart contracts,* dont les membres en sont actionnaires (les *tokens* ne sont guère différents d'actions en réalité, puisqu'ils servent à financer, rémunérer, donnent des droits de vote et sont cessibles, ce qu'une décision d'une cour fédérale américaine semble confirmer), et qui fonctionne sans cadres dirigeants.

Une DAO pourrait très bien se fonder sur un principe d'économie coopérative plutôt que capitaliste, tout dépend ici du code.

Plus généralement, la *blockchain* pourrait être utilisée pour transformer nos institutions démocratiques, en facilitant l'organisation de votes (donc la démocratie directe). Autrement dit, la *blockchain* pourrait être vue comme un système permettant de créer et de faire fonctionner des institutions collaboratives et démocratiques de manière décentralisée.

Au-delà du mythe de l'absence de *"tiers de confiance"* et de l'automatisation de la société

Nombre des membres de la communauté *blockchain* n'hésitent pas à parler de révolution. Mais n'oublions pas que les discours prophétiques annoncent souvent des révolutions qui n'ont jamais lieu.

Certaines potentialités de la *blockchain* pourraient de fait ne jamais être exploitées. La diffusion d'une technologie dépend des coûts relatifs (y compris écologiques pour des questions de régulation), par rapport aux autres, des habitudes des acteurs économiques (il y a des apprentissages, des compétences qui sont développés sur des technologies préexistantes), des effets de réseau, des complémentarités technologiques (la compatibilité de telle technologie avec telle autre), des rapports de pouvoir et du lobbying.

Pour prendre un exemple, dans le cas de la e-santé et de la protection des données, il faudrait s'assurer que la *blockchain* apporte une réelle plus-value par rapport au système actuel en France.

[10] https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/

Plus généralement, quid de l'effet sur la consommation énergétique globale en cas de généralisation de l'usage des blockchains ?[11]

La blockchain est-elle une révolution ?

La communauté blockchain, et spécifiquement celle d'Ethereum, fonctionne sur un mythe : celui de créer un système "trustless", sans tiers de confiance. Si la blockchain tente de se passer de certains tiers de confiance, elle ne pourra malgré tout pas les éliminer. En effet, pour que les informations soient intégrées dans la blockchain et qu'ensuite, le smart contract "s'active", encore faut-il que quelqu'un rentre cette information. Par exemple, admettons qu'un contrat d'assurance climatique sous forme smart contract ait été rédigé entre un agent A et un agent B, impliquant que lorsque A (un agriculteur par exemple) a subi un épisode de gel qui lui fait perdre une partie de ses récoltes, B s'engage à compenser une partie de la perte. Pour que ce contrat puisse s'appliquer dans la blockchain, encore faut-il que l'information sur les intempéries ou le gel ait été rentrée dans la chaîne de bloc, ce qui suppose l'intervention d'un agent extérieur à la blockchain pour le faire. La communauté Ethereum appelle cet agent qui rentre l'information nécessaire à la vérification et l'implémentation du smart contract un "oracle". Cet oracle est soit une ou des personnes, des organisations ou un algorithme quand cela est possible (par exemple, un algorithme qui va chercher automatiquement l'information sur Internet, quand cette information existe, comme les cours de Bourse). La question de la confiance dans l'oracle (quand il s'agit d'un humain ou d'une organisation) et des moyens de l'inciter à agir dans l'intérêt commun se repose. De même que se pose la question de l'arbitrage en cas de litige – ce qui renvoie aux limites de l'automatisation de la société.

La blockchain comme la communauté qui la compose pour l'essentiel repose sur le mantra du "code is law", c'est-à-dire que c'est l'algorithme, le langage machine et l'architecture des plateformes numériques qui fait loi. Cette idée relève du fantasme dans la mesure où le net et la blockchain ne sont pas hors droit. S'il est possible d'incorporer des règles de droit dans le code informatique, certaines règles de droit pourraient limiter la possibilité d'adopter cette technologie. Par exemple, dans le cas de la e-santé, il y a un débat sur la possibilité de rendre compatible le droit à l'oubli[12] et l'immuabilité de l'information dans la blockchain. Si on applique strictement le fantasme "code is law", l'immuabilité du code dans la blockchain risque de poser problème.

Une machine applique "bêtement" (automatiquement) ce que le code du logiciel lui indique. A la différence du langage ordinaire, plein de métaphores, le code informatique ne laisse pas de place à l'interprétation. Donc si les règles que se sont données les membres d'une blockchain n'ont pas anticipé tous les cas particuliers, le code risque de ne pas pouvoir en tenir compte et ne pourra être révisé a posteriori. C'est ce qui s'est passé pour The DAO et qui a causé sa perte : un hacker a profité d'une faille dans le code pour s'accaparer une partie des fonds accumulés[13]. Cela a bien entendu amené une réaction de la communauté Ethereum. Fallait-il réécrire le bloc de transactions en question, restaurer l'état de The DAO avant cette transaction "illicite", et effectuer ainsi une

---

[11] On rappelle, comme on l'a vu lors du précédent texte, qu'à elle seule, la *blockchain* Bitcoin est un gouffre énergétique insoutenable, puisque sa consommation annuelle est entre 10 et 30 mTWh par an supérieure à celle de 159 états dans le monde. Voir : https://www.sciencesetavenir.fr/high-tech/la-crypto-monnaie-bictoin-consomme-plus-d-electricite-que-159-etats-dans-le-monde_118729 ; https://bitcoin.fr/la-depense-electrique-des-crypto-monnaies/

[12] https://linc.cnil.fr/fr/blockchain-et-rgpd-une-union-impossible-0 ; https://blockchainpartner.fr/blockchain-gdpr-malentendu/

[13] Il ne s'agit pas ici du code d'Ethereum en tant que tel, mais des programmes (les *smart contracts*) qui ont été implémentés à partir d'Ethereum, qui, pour rappel, a intégré un langage de programmation Turing-complet.

"bifurcation" (hard fork), ou bien fallait-il seulement censurer les mouvements de fonds issus du compte du hacker en censurant les transactions qu'il avait effectuées (soft fork) ? Le problème de la solution hard fork, c'est qu'il fallait le consensus de la communauté. Or, alors qu'une majorité était favorable à ce choix, certains membres ont considéré que comme le hacker n'avait fait qu'appliquer le code ("code is law") pour profiter de sa faille, son acte n'était pas illégitime et que l'on ne devait pas annuler sa transaction[14]. La blockchain Ethereum s'est donc divisée en deux (Ethereum et Ethereum classic), entre ceux qui avaient en quelque sorte une lecture "légaliste" du code (ceux qui étaient contre le hard fork) et ceux qui défendaient "l'esprit du code" (pour le hard fork). Cet épisode montre que "code is law" est en partie une utopie, et que toute communauté doit pouvoir réécrire et réinterpréter ses propres lois, sous peine d'exploser.

Autre problème : seuls les codeurs comprennent réellement ce que recouvre le code. Ce sont eux qui fabriquent les blockchains. Les profanes n'y comprenant pas grand-chose (l'auteur de ces lignes y compris). Les codeurs ont donc entre leurs mains un outil pour l'instant peu accessible aux citoyens lambda, dont l'usage à grande échelle n'est pas sans poser des risques démocratiques. Qui est capable de comprendre le code d'un smart contract ? Les risques d'exclusion des "incompétents" du numérique est grand, d'où le danger d'un système purement basé sur le code informatique. Le langage de la loi, bien que complexe, reste écrit en langage naturel et donc compréhensible relativement facilement par tout citoyen. Loin de supprimer le tiers de confiance, l'utopie "code is law" pourrait simplement faire changer les tiers de confiance : de l'avocat vers le codeur…

Et de toute façon, il y aura toujours besoin de tiers de confiance. Par exemple, la blockchain plutôt que de supprimer le notaire, pourrait inciter ce dernier à redoubler son rôle de conseil et l'amener à recourir à un codeur pour rédiger certains smart contracts, réputés conformes au droit. En l'occurrence, les évolutions possibles sont encore assez imprévisibles.

Cette obsession de l'abolition du tiers de confiance trahit l'absence de confiance que les membres de cette communauté ont entre eux et vis-à-vis des autres, soit une forme sociale assez stupéfiante de paranoïa. On retrouve la méfiance (en partie compréhensible) à l'égard des institutions verticales et qui est une constante de la culture des hackers[15]. D'une certaine façon, la blockchain pourrait être vue comme un moyen inventé par cette communauté de codeurs de résoudre le problème de la confiance qu'eux-mêmes ont vis-à-vis des autres et de toute forme d'autorité. Ce serait la technologie concrétisant le mythe de l'élimination des humains de toute fonction de contrôle, par l'invention d'un code qui évite toute délégation de pouvoir.

Les effets de la technologie blockchain dépendront fondamentalement de ce à quoi elle sera appliquée et de la manière dont les agents se l'approprieront : une technique peut apporter le meilleur (dans le cas présent, réduire les coûts de transaction, faciliter certaines formes d'organisation ou de démocratie) ou le pire (l'empreinte énergétique et les risques d'automatisation du social). Il paraît impossible d'y échapper, la difficulté sera ici son appropriation raisonnée par tout le monde.

Si les promesses de la blockchain sont nombreuses, il est probable malgré tout que toutes ne se réaliseront pas.

Il convient quoiqu'il en soit de ne surtout pas s'en désintéresser et d'en faciliter la compréhension.

---

[14] https://blockchainfrance.net/2016/07/20/la-fin-de-lideal-trustless/#comments

[15] Flichy P. (2017), Les nouvelles frontières du travail à l'ère du numérique, Seuil, Paris.