SLIM A. & PRIETO M. [2020], « L'émergence des cryptomonnaies : preuve d'une utopie consumériste sur le déclin » in Olivier Badot, Philippe Moati (eds), *Utopies et consommation*, Editions EMS Management et Société, collection Societing, pp. 161-178.

L'émergence des *crypto* monnaies : preuve d'une utopie consumériste sur le déclin ?

Assen SLIM et Marc PRIETO

Depuis une vingtaine d'années, l'économie mondiale a opéré sa mue en intégrant à peu près partout le numérique. Sans aucun doute, le domaine de la monnaie a été celui dans lequel son entrée a été la plus inattendue. Si très tôt les banques et les acteurs du monde de la finance avaient annoncé l'arrivée massive des échanges virtuels et dématérialisés, peu nombreux sont celles ou ceux qui avaient misé sur le succès de monnaies d'un nouveau genre, concurrentes des monnaies « sonnantes et trébuchantes ». Les monnaies virtuelles, déconnectées de toutes banques centrales et en dehors de toute frontière physique, ont ainsi fait leur apparition, au premier rang desquelles le Bitcoin, considéré aujourd'hui comme l'une des principales *crypto* monnaies.

La promesse de cette utopie naissante est de se défaire de l'emprise d'un système bancaire devenu omnipotent. Un nouvel horizon d'émancipation est alors pensé et mis en pratique, porté par des valeurs originales issues de l'imaginaire de l'utopie *crypto* anarchiste. Ainsi, face au déclin de l'utopie consumériste tel qu'il se manifeste dans l'enquête réalisée en 2019 par l'ObSoCo, nous pourrions à première vue supposer une grande opposition entre les deux utopies. Pourtant, il n'en est rien. Malgré le radicalisme du projet *crypto* anarchiste, cette utopie peine à se défaire des idéaux consuméristes et matérialistes.

Les fondements de l'utopie *crypto* anarchiste illustrent en réalité la proximité du projet avec l'utopie consumériste. Le rejet d'un pouvoir des banques jugé excessif constitue un pilier essentiel de ce mouvement sans pour autant que ne soit remis en question le rôle de la consommation et sa place dans la société. De plus, en omettant de prendre en compte les conséquences de l'activité humaine sur l'environnement et la gestion des relations interhumaines, l'idéal *crypto* anarchiste ne participe aucunement au mouvement récent de rejet de la consommation de masse.

Aux fondements de l'utopie *crypto* monétaire

Le financement de l'utopie consumériste

L'utopie consumériste s'est nourrie du « compromis fordien » conclu durant les Trente Glorieuses et selon lequel la production de masse devait nécessairement avoir pour corollaire la consommation de masse. Sans la seconde, pas de débouché ni de valorisation pour la première. Avec le tournant libéral des années 1980 orchestré par le tandem Reagan-Thatcher, la conflictualité entre le travail et le capital s'est ravivée. Raboté par des décennies de politiques d'austérité, le pouvoir d'achat a stagné au point de saper les bases du financement de la demande. Les banques, portées par les politiques de « 3D » (déréglementation, désintermédiation, décloisonnement), ont alors pris une importance considérable dans le soutien à l'utopie consumériste. Elles ont redoublé de créativité pour maintenir un niveau de financement acceptable de la demande, mais au prix d'un endettement privé en forte augmentation. La titrisation des créances détenues par les institutions financières (dont les fameux « subprimes » en sont une bonne illustration) et leur revente sur les marchés financiers n'ont pas tardé à se traduire par leur lot de crises financières et autres explosions de bulles spéculatives, remettant en cause la pérennité du financement de la demande, au cœur même de l'utopie consumériste… C'est ainsi le pouvoir exorbitant des banques dans nos sociétés de consommation de masse qui va précipiter la réalisation du projet *crypto* anarchiste.

Le projet *crypto* anarchiste ou la contestation du pouvoir orwellien des banques

Les premiers groupes informels de *Cypherpunks* ou *Crypto anarchistes* apparaissent à partir des années 1980. Ils sont composés de chercheurs et spécialistes en informatique et en cryptographie dont ils souhaitent démocratiser l'usage (Castor, 2017). Ces groupes ont pour point commun de partager une défiance très forte envers toute institution centrale, à commencer par les banques et les gouvernements qui concentreraient, d'après eux, un pouvoir de contrôle exorbitant. Ils s'accordent tous pour dénoncer la collusion entre les pouvoirs politique et bancaire les rendant incapables d'offrir une monnaie de qualité (qui ne soit pas sujette à des crises à répétition) aux individus. Le projet utopique qui en émerge, et que nous nommerons « projet *crypto* anarchiste », se propose purement et simplement de se passer des banques et de toute autre autorité centrale pour payer les transactions. Cela revient à dire que les achats et les

ventes seraient réglés autrement qu'en utilisant de la monnaie bancaire (*fiat currency*). L'ambition des promoteurs de ce projet est de créer une monnaie alternative qui serait à la fois « un bien commun » rendus aux consommateurs, un moyen de « démocratiser la finance » et une voie de « réappropriation monétaire ».

Plusieurs tentatives se succèdent, cherchant toutes à concevoir des protocoles informatiques dont l'architecture décentralisée permettrait la coopération interindividuelle sans identification des vrais noms et identités juridiques des coéchangistes. Thimothy C. May en appelle à une révolution technique qui rendrait possible la consommation de tous types de biens et services, même les plus immoraux : « un marché informatisé anonyme rendra même possible des marchés odieux pour les assassinats et l'extorsion » (May, 1992). Dans le cyberespace, perçu comme le lieu privilégié et autoréférentiel des interactions sociales, « le gouvernement n'est pas temporairement détruit, mais devient inutile et interdit de manière permanente » (Dai, 1998).

David Chaum (cofondateur l'*International Association for Cryptologic Research* – IACR), est le premier à théoriser « DigiCash » en 1983 et à lancer la première expérience de monnaie électronique alternative en 1990 (Chaum, 1983). Cette tentative, restée quasi-confidentielle et reposant sur une architecture encore centralisée, tourne court et disparaît en 1999, à la suite de la faillite de l'entreprise sur laquelle le système reposait. Wai Dai, influencé par le projet *crypto* anarchiste de Thimoty C. May, élabore sa « b-money », annonçant un système de paiement décentralisé et intraçable par l'utilisation de clefs cryptographiques en mesure de protéger efficacement l'anonymat des utilisateurs (vendeurs, acheteurs) (Dai, 1998). De son côté, Nick Szabo développe, entre 1998 et 2005, son projet de monnaie décentralisée appelée « Bit gold » dans lequel il cherche à résoudre le problème de la « double dépense » (*double spending*), *i.e.* éviter que les unités monétaires soient frauduleusement dupliquées pour être dépensées plusieurs fois de suite (Szabo, 1998 et 2005). Les avancées tant logicielles que matérielles (augmentation concomitante des puissances de calcul et des capacités de traitement tant en quantité qu'en vitesse) et l'émergence des réseaux *Peer-to-Peer* (*P2P*) évitant les points de contrôle unique, rendent progressivement possible la conception d'un projet de monnaie digitale cumulant tous les avantages des expériences passées : le Bitcoin.

Le Bitcoin, une autre manière de payer sa consommation

Si l'une des fonctions de l'utopie est d'alimenter le rêve « d'une autre manière de s'approprier les choses » (Ricoeur, 1984), alors le Bitcoin s'y inscrit parfaitement. Il cherche tout à la fois à corriger l'imperfection des paiements monétaires traditionnels, remettre en cause le pouvoir des banques, offrir un autre mode de paiement pour les achats, libérer et affranchir les individus de toute forme d'assujettissement.

L'article fondateur du Bitcoin est publié en 2008. L' « auteur »[1], Satochi Nakamoto, dit y travailler depuis 2007 en réponse à la crise mondiale. Il annonce vouloir résoudre pratiquement les problèmes des monnaies qui impliquent l'existence de médiations certifiées et d'institutions tierces. Or ces institutions s'érigeraient en médiateurs des conflits (réversibilité des transactions, création monétaire arbitraire) au prix d'une augmentation des coûts de transaction et de la fréquence et de l'intensité des crises monétaires et financières. Le Bitcoin se propose d'offrir « un nouvel espace de liberté » *via* une infrastructure technique censée générer de la confiance en se passant de toute autorité centrale (Nakamoto, 2008). Contrairement aux paiements réalisés en monnaie bancaire, le système imaginé par Nakamoto se présente comme un protocole de réseau *P2P* collaboratif, sécurisé et résilient, permettant de transférer des données sécurisés (les bitcoins), sans l'intermédiation d'une autorité centrale de confiance (la banque).

L'infrastructure technique du Bitcoin repose sur la cryptographie à double-clés, la Blockchain et l'activité de minage.

La cryptographie asymétrique à double-clés (publique, privée) permet en principe de garantir le « pseudonymat » des parties prenantes, tout en rendant impossible la falsification des identifiants et des montants de bitcoins inscrits dans les porte-monnaie électroniques (*wallets*). Le pseudonymat est un terme dérivé de pseudonyme en référence à « faux nom ». Chaque coéchangiste est identifié par sa clé publique sans pour autant que soient divulgués les véritables noms et prénoms (identité légale). Lors d'un paiement, l'émetteur de bitcoins signe et authentifie son ordre de paiement avec sa clé privée. Le bénéficiaire du règlement recevra les sommes envoyées sur son propre porte-monnaie si cette clé correspond à la clé publique

[1] Pseudonyme utilisé lors de la publication et sur les forums. Le mystère subsiste quant à l'identité véritable du ou des concepteurs du Bitcoin. En 2010, S. Nakamoto a définitivement cessé de communiquer. Il possède également un million de Bitcoin (soit 10 milliards d'euros) qu'il n'a jamais utilisé ou dépensé.

diffusée par l'émetteur pour décrypter le transfert et en authentifier l'origine sans pour autant révéler l'identité des acteurs.

La Blockchain, de son côté, correspond à l'historique de toutes les transactions traitées et validées par le système Bitcoin depuis sa création : c'est « une base de données qui enregistre à l'aide d'un réseau d'ordinateurs des transactions » (Peters & Panayi, 2016). Cette dernière est répliquée à l'identique dans certains ordinateurs du système, appelés « nœuds complets ». Il n'existe, en effet, pas un mais plusieurs dizaines de milliers d'exemplaires de la Blockchain, construits et gérés par autant d'ordinateurs sur toute la planète. Les « nœuds complets » maintiennent à jour un exemplaire de la Blockchain, téléchargent et vérifient la validité des nouveaux blocs aux règles reconnues de tous, puis les diffusent sur le réseau.

Le minage, enfin, par résolution de « preuves de travail » (ou *PoW* pour *Proof of Work*), correspond à l'étape où les nouvelles transactions émises sont validées et inscrites dans un nouveau bloc s'ajoutant à la Blockchain. Dans une blockchain, les transactions sont validées par bloc. Cette validation est réalisée par des « mineurs » qui sont des utilisateurs volontaires dotés de logiciels particuliers. La validation consiste en la résolution de problèmes mathématiques complexes. La résolution de ces problèmes dépend d'une variable aléatoire inscrite dans les règles de la blockchain, qui fait en sorte que ce ne soit pas les mêmes mineurs qui valident les blocs (Ribeiro, 2016). C'est ce caractère aléatoire qui empêche un mineur de prendre le pouvoir sur les autres et c'est l'une des clés de la sûreté de la blockchain. Lorsqu'un mineur résout le premier les problèmes mathématiques, sa solution est diffusée à tous les autres mineurs qui la valident (à la majorité de 51 % des mineurs) et enregistrent le nouveau bloc dans la Blockchain. Cette procédure, qui dure environ dix minutes, permet d'éviter les problèmes de double-dépenses frauduleuses des mêmes Bitcoins (*double spending problem*). Les mineurs sont en concurrence les uns avec les autres. Leur chance de trouver la bonne solution avant les autres dépend directement de la puissance qu'ils y dédient, relativement à la puissance totale cumulée dans le réseau. En contrepartie de leur travail de vérification (*PoW*), les mineurs sont récompensés en obtenant une certaine quantité de Bitcoins.

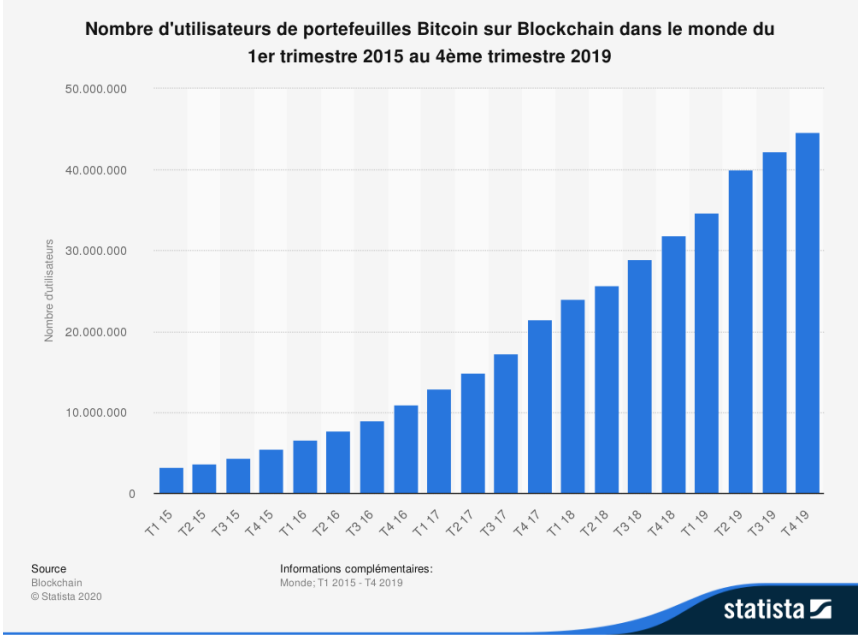
L'infrastructure technique du Bitcoin, ouverte, transparente, incorruptible, permettant l'interaction directe des individus sans l'intermédiation d'un tiers de confiance, constitue pour les *crypto* anarchistes un projet de plus grande justice sociale en ce sens qu'il évite à la fois toute collusion anti-démocratique entre les représentants du capital et les gouvernements et qu'il rend accessible à tous des services de paiement (*wallet* personnel, virements).

Le projet *crypto* anarchiste face à ses impensés

Une diffusion des *crypto* monnaies en deçà des prévisions

Depuis sa création, l'infrastructure du Bitcoin va servir de modèle à plus de 1500 autres *crypto* monnaies donnant plus de profondeur au projet *crypto* anarchiste. Toutes reposent sur une technologie Blockchain spécifique leur conférant des propriétés différentes (rapidité, traçabilité, faible coût de transaction, authentification, taille des blocs, etc.). Le nombre d'utilisateurs de *crypto* monnaies est en constante augmentation. A la fin de l'année 2019, on en dénombrait plus de 44 millions dans le monde pour le seul bitcoin (Illustration 1).

Illustration 1 : Nombre d'utilisateurs du Bitcoin de 2015 à 2019



Source : Statista

Toutefois, ce nombre reste relativement limité au regard de l'ambition première des *crypto* anarchistes et témoigne d'une certaine méfiance du grand public à l'égard d'un projet mal compris. La sphère circulatoire des *crypto* monnaies reste relativement limitée. Peu de vendeurs décident de franchir le Rubicon. Les services de paiements en Bitcoin tels que *Coinbase* et *Bitpay*, par exemple, annoncent 89 000 entreprises utilisatrices de leurs services (dont *Microsoft, Dell, Bloomberg, Google, Paypal, Amazon, Ikea, Twitch, airBaltic, Lush, Wikimedia*, etc.). Le site de vente sur Internet *Shopify* (sorte d'*e-bay* du bitcoin) recense 1 million de vendeurs inscrits à travers le monde. En définitive, il n'est pas surprenant de constater que seuls 13 % des bitcoins émis sont réellement utilisés pour payer des transactions,

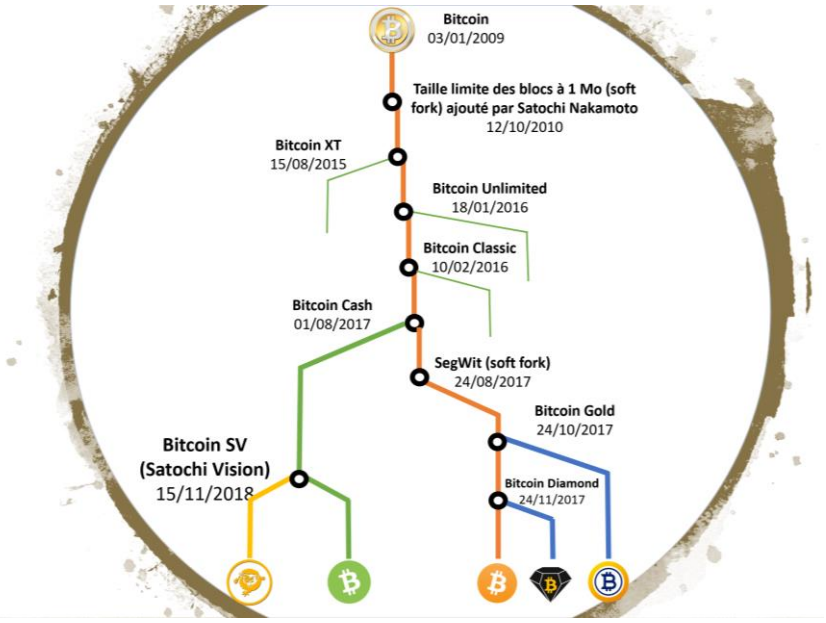
le restant étant épargné. De plus, 62 % des bitcoins émis sont détenus par 0,1 % des 44,69 millions de portefeuilles, ce qui n'est pas propice à leur circulation.

Le projet *crypto* anarchiste peine à convaincre notamment parce qu'il bute sur deux impensés majeurs : impensé des institutions sociales, impensé de l'empreinte écologique.

L'impensé des institutions sociales

Alors que le Bitcoin a été pensé comme un système dans lequel l'intégralité de la coordination se ferait sur un plan purement technique (gouvernance par l'infrastructure), il est en revanche démuni pour répondre à des problématiques relevant d'une coordination non exclusivement technique (gouvernance de l'infrastructure). Or le Bitcoin apparaît bien comme un système « sociotechnique » au sens où il implique des utilisateurs humains (acheteurs, vendeurs, développeurs, mineurs). Cependant, « les systèmes sociotechniques ne peuvent pas, du fait de leur intégration dans un contexte social et culturel, assurer leur propre autonomie et leur autosuffisance grâce à la seule technologie » (De Filippi & Loveluck, 2016). Ainsi, l'infrastructure technique n'est pas en mesure, à elle seule, de répondre à des problématiques telles que : définir et protéger les frontières de sa communauté, établir des incitations à la participation des membres et leur reconnaître des statuts, pacifier les conflits (Auray, 2012). Le conflit survenu en 2015-2016, par exemple, entre développeurs du Bitcoin illustre bien ce point. Pour des raisons variées (sécurité, stabilité du système, décentralisation), la taille des blocs a été initialement fixée à 1 Mo (Mégaoctet) par Satochi Nakamoto. Plusieurs développeurs ont proposé d'augmenter cette taille afin de pouvoir traiter un nombre plus important de transactions par bloc. En 2015, les débats qui ont eu lieu sur les forums et les réseaux sociaux dédiés ont été si vifs qu'on a rapidement parlé de « guerre civile ouverte » (Hearn, 2016). En l'absence de tout consensus, deux développeurs (Gavin Andresen et Mike Hearn) lançaient un Bitcoin alternatif (le Bitcoin XT) avec une taille de bloc théorique de 8 Mo et devant augmenter de 40 % par an. Ce « divorce » s'appelle un *Hard fork* dans le jargon *crypto* anarchiste. Même si ce projet alternatif a rapidement été abandonné, d'autres *forks* se sont produits sur le Bitcoin conduisant à l'existence de cinq Bitcoins différents (illustration 2).

Illustration 2 : Quelques *Soft* et *Hard forks* du Bitcoin



Source : Assen Slim et Marc Prieto.

Il ressort de cet exemple que l'infrastructure du Bitcoin n'est pas en mesure d'apporter des réponses aux conflits interhumains. Contrairement au récit de ses promoteurs, le Bitcoin est une construction profondément politique et sociale. A ce titre, elle requiert des institutions en mesure de préserver la légitimité d'ensemble du système. Plusieurs formes « pré-institutionnelles » d'arbitrage des désaccords ont ainsi spontanément émergé : les propositions d'amélioration du Bitcoin (*BIPs*), les réseaux sociaux dédiés (*GitHub*, *Reddit*, *Bitcointalk*, *twitter*), les rencontres physiques, les votes, les *forks* (Rolland & Slim, 2017).

L'impensé de l'empreinte écologique

Ce second impensé fait référence à la « matérialité » du Bitcoin. En effet, son infrastructure repose sur l'existence d'équipements informatiques bien réels. Le minage, par exemple, requiert des équipements munis de processeurs (CPU), de cartes graphiques (GPU) et d'ASIC (circuits intégrés dédiés spécifiquement au minage de certaines *crypto* monnaies). Progressivement, les mineurs se sont constitués en groupes (*pools*) leur permettant ainsi de mutualiser leur puissance de calcul et d'augmenter leurs chances dans la course à la résolution des blocs. La consommation électrique de ces équipements ainsi que les systèmes de refroidissement qui leur sont associés est estimée pour le seul Bitcoin à environ 30,14 térawatts-h par an (30,14 milliards de kilowatts-heure), soit l'équivalent de la production électrique de quatre centrales nucléaires. Cette dérive énergivore fait écho à la prise de conscience très récente de l'empreinte

environnementale du numérique qui a été jusqu'ici occultée. Le projet *crypto* anarchiste ne s'inscrit donc pas dans la dynamique de transition écologique du numérique voulue par une frange croissante de la société à l'instar de l'économiste Éric Vidalenc (2019).

Fortement énergivore, incapable de se penser en système « sociotechnique », le projet *crypto* anarchiste peine à convaincre le grand public.

L'horizon indépassable de l'utopie consumériste

Le projet *crypto* anarchiste n'a jamais eu l'ambition de mettre fin à la consommation de masse. Son but est plus modeste : rendre l'usage plein et entier de la monnaie aux gens et leur permettre de régler directement leurs transactions entre eux sans passer par l'intermédiation des banques. Non seulement les *crypto* monnaies ne sont pas parvenues à cet objectif, mais la technologie Blockchain est en passe d'être réabsorber par les acteurs traditionnels de l'économie capitaliste, à commencer par les banques elles-mêmes. En 2015, *The Economist* ne s'y trompait pas en titrant sur la Blockchain qui allait « changer le monde » (illustration 3).

Illustration 3 : page de couverture de *The Economist* du 31 octobre au 5 novembre 2015

Source : The Economist

Des Blockchains classiques aux Blockchains « infrastructures », outils précieux pour la consommation et les échanges dans le capitalisme

La technologie Blockchain possède, en effet, de nombreuses propriétés susceptibles d'intéresser de nombreux secteurs d'activité. Dans sa version classique (celle du Bitcoin par exemple), elle contient des informations qui peuvent être consultées par tous à tout moment. Elle fonctionne alors à l'image d'un *data center* sûr, incorruptible et inviolable. Ces informations peuvent être de natures très différentes : preuves d'achat, actes de propriété, preuves de paiement, brevets, tickets, etc. Dans sa version dite « infrastructure », la Blockchain peut contenir et gérer d'autres types d'informations qu'on appelle des *smart contracts*. La première Blockchain de ce type, appelée Ethereum, a été inventée par Vitalik Buterin en 2013. Ce dernier définit les *smart contracts* comme « des boîtes 'cryptographiques' qui contiennent de la valeur et ne la déverrouillent que si certaines conditions sont remplies » (Buterin, 2013). Il ne faut pas voir les *smart contracts* comme des contrats au sens propre du terme, mais davantage comme des applications informatiques autonomes ayant enregistré les termes d'un accord et qui s'autoexécutent lorsque les conditions de l'accord sont remplies. Ils n'ont pas en eux-mêmes d'autorité juridique. Lorsqu'un contrat juridique existe, le *smart contract* en est son application technique. Ils fonctionnent sur le principe du « if-then » (si la condition est vérifiée alors la conséquence est exécutée). L'originalité ici réside dans le fait que ces smart contacts sont écrits sur une Blockchain et bénéficient donc de tous les avantages de cette technologie (horodatage, inviolabilité, couts de transaction réduits, etc.). Ils permettent d'éviter les coûts élevés de rédaction d'un contrat, les interventions judiciaires, les comportements opportunistes et les ambiguïtés inhérentes au langage écrit. On est certain que les *smarts contracts* s'exécuteront comme attendus, rapidement et sans intervention humaine (source potentielle de biais). Buterin voit trois grands débouchés pour les Blockchains infrastructures : les applications financières, semi-financières et non financières. Et de fait, les Blockchains privées ne vont pas tarder à émerger hors de toute référence aux *crypto* monnaies, diffusant cette technologie à l'ensemble de l'économie. Les entreprises mettent en avant sept grands facteurs d'attractivité de la Blockchain : données infalsifiables, sécurité par cryptographie, baisse significative des coûts de transaction, authentification des données par consensus, organisation communautaire, registre de compte public et rapidité des transactions. (Godebarge & Rossat, 2016).

Sur les marchés financiers, l'adoption de Blockchains infrastructures utilisant des *smarts contracts* serait susceptible d'apporter trois grands types d'améliorations : la réduction des délais entre la transaction et le règlement, la réduction des coûts de transaction, l'intégration des systèmes de compensation et de règlement/livraison. Ainsi, les transactions pourraient s'effectuer très rapidement, en quelques secondes contre 2 à 3 jours actuellement, diminuant les risques et donc les coûts. La société *HitFin*, qui propose une Blockchain privée pouvant gérer les échanges de titres financiers et une chambre de compensation bilatérale, estime un temps d'exécution de 17 secondes. Cette organisation permettrait également de mettre en lien les chambres de compensation et les organismes de règlement-livraison dans un système intégré automatique. Ajoutons que les tâches de reporting seraient facilitées car directement traitées sur la Blockchain. D'après Peters et Panayi, il serait même possible de se passer de la rédaction de contrats physiques grâce à la généralisation des portefeuilles multi-signatures gérés directement sur la Blockchain (Peters et Panayi, 2016). En définitive, Wyman estime l'économie de coûts de transaction apportée par la Blockchain de l'ordre de 15 à 20 milliards de dollars par an (Wyman, 2016).

Les applications non financières de la technologie Blockchain sont *a priori* sans limites. Elles peuvent consister à lever des fonds pour financer un projet d'investissement (*Initial Coin Offering* ou ICO). Contrairement à l'IPO (*Initial Public Offering*) qui implique toujours une introduction en bourse, l'ICO est une levée de fonds sur le modèle du *crowdfunding* mais durant laquelle les sommes récoltées le sont en *crypto* monnaies Concrètement, une entreprise décide d'émettre des *tokens* qu'elle vend contre des *crypto* monnaies lors de la phase de démarrage de l'un de ses projets. Les ICO permettent de s'affranchir du système classique de Capital-risque (*Venture Capital*) qui ne financent pas de projets à un stade aussi précoce de développement. Les *tokens* peuvent être utilisés pour : acheter le service qui sera produit par l'initiateur de l'ICO ; être revendus contre d'autres *crypto* monnaies à des fins spéculatives ; être convertis en monnaie bancaire. Il y aurait eu ainsi plus de 13 milliards de dollars levés en ICO dans le monde en 2018 contre 4 milliards en 2017 (Perreau, 2020). Les dix plus grosses ICO réalisées dans le monde entre 2014 et 2020 sont : EOS (4000 millions de dollars), Telegram (1700), Bitfinex (1000) ; TaTaTu (575), Dragon Coin (320), HDAC (258), Filecoin (257), Tezos (233), Sirin Labs (157), Bancor (153). Les ICO servent le plus souvent à financer le lancement d'applications décentralisées, parfois des protocoles blockchain. Toutefois, il n'existe aucune garantie pour les investisseurs et certaines ICO peuvent se révéler être de vraies escroqueries.

Les usages illimités de la Blockchain

De nombreux domaines d'activité ont déjà adopté la technologie Blockchain. Il n'est pas question ici d'en donner une liste détaillée et exhaustive mais d'en présenter les grandes lignes directrices. Les différentes facettes de l'usage de la Blockchain se résument aux points suivants : traçabilité ; digitalisation, envoi, stockage de contenus ; traçabilité, contrôle et certification ; activités de gestion des autorisations et des authentifications, activités de l'Internet of Things (IoT), activités collaboratives.

D'abord, il existe les cas d'usage de la Blockchain qui rassemblent des activités de digitalisation de documents ou de contenus, d'envoi, puis de stockage. On peut prendre, par exemple, le cas de la génération d'un diplôme officiel, sa numérisation et son stockage définitif sur une blockchain. La preuve obtenue (ici le diplôme) est infalsifiable et inscrite pour toujours sur la Blockchain. Cela peut convenir à de nombreux autres types de documents (tickets, brevets, contrats, certificats d'authenticité, etc.).

Il y a ensuite les cas d'usage de la Blockchain qui rassemble les activités de traçabilité, de contrôle et de certification. L'enseigne de grande distribution *Carrefour* applique depuis 2018 la technologie Blockchain pour garantir au consommateur la traçabilité de ses produits. Par l'intermédiaire d'un QR Code apposé sur l'étiquette de l'article, le consommateur est en mesure d'accéder à un grand nombre d'information contenues dans la Blockchain comme, dans le cas des poulets, le lieu et le mode d'élevage, le nom de l'éleveur, l'alimentation reçue, l'absence de traitement, les labels et le lieu d'abattage.

Les cas d'usage de la Blockchain tournés vers la gestion des autorisations et des authentifications sont aussi à considérer. De nombreuses entreprises, à l'instar de *BlockStack,* proposent à leurs clients de créer une identité sur la Blockchain qui peut être utilisé pour toute authentification ou inscription sur différents sites.

Les cas d'usage de la Blockchain pour des activités de l'*Internet of Things* (IoT) concernent les objets connectés. Les solutions proposées permettent de stocker l'information collectée par ces objets directement dans une blockchain afin d'assurer la sécurité, la traçabilité et surtout la confidentialité des utilisateurs.

Les cas d'usage de la Blockchain pour des activités collaboratives consistent à mettre directement en relation offreurs et demandeurs d'un service en se passant de la présence d'un intermédiaire (de type *Uber* ou *AirBnB*).

Enfin, de nombreuses autres initiatives émergent en ce moment même dans les domaines des assurances (*Axa*, *MS Amlin*), jeux en ligne, de la santé, du stockage des données, etc. qu'il serait impossible d'établir une liste exhaustive.

Conclusion

De crise en crise, l'utopie consumériste, dans son stade financiarisé, chancelle. A l'issue de celle dite du « subprime » (2007), celle de trop pour les *crypto* anarchistes, le Bitcoin voit le jour. Son « concepteur » a explicitement glissé le message suivant dans le texte séminal de cette première *crypto* monnaie : « Le Chancelier est sur le point de lancer un deuxième plan de sauvetage pour les banques » (Nakamoto, 2008). Il s'agit d'une reprise du titre en une du *Times* du 3 janvier 2008 qui fait explicitement référence à la responsabilité des banques dans cette nième crise du capitalisme. Le Bitcoin est conçu d'emblée comme une monnaie sans intermédiaires bancaires ou financiers, une monnaie rendu aux individus. Le projet *crypto* anarchiste ne cherche pas à sortir du capitalisme mais bien à établir des relations directes entre les individus, à la manière d'un langage commun nouveau entre eux.

Alors que l'utopie consumériste courrait vers son point de rupture, le projet *crypto* anarchiste d'émancipation a, contre toute attente, réussi l'exploit… de raviver la production et la consommation de masse ! La technologie Blockchain infuse partout, donnant des marges de manœuvre inespérées à des activités à bout de souffle, comme la grande distribution par exemple, et réoxygénant un « capitalisme absolutisé » (Rancière, 2020). Alors que tous les avenirs mobilisateurs ont été ruinés (communisme devenu dictature policière, socialisme réduit à une imposture gouvernementale, républicanisme synonyme d'idéologie raciste, démocratie détournée par des oligarchies), l'utopie *crypto* monétaire démontre qu'il reste encore des horizons émancipateurs à explorer.

Bibliographie

Auray N. (2012), “Online communities and governance mechanisms”, in E. Brousseau, M. Brousseau, E., Marzouki, M., & Méadel, C. eds. (2012), Governance, Regulation and Powers on the Internet. Cambridge and New York: Cambridge University Press.

Buterin V. (2013), “Ethereum White Paper: A next generation smart contract & decentralized application plateform”, https://whitepaper.io/document/5/ethereum-whitepaper

Castor A. (2017), “In Santa Barbara, An Annual Event Brings Together Those Closest To Bitcoin’s Roots”, Forbes.

Chaum D. (1983), “Blind Signatures for Untraceable Payments”, Advances in Cryptology Proceeding, vol. 82, n°3, pp. 199-203.

Dai W. (1998), “b-money”, Forbes.

De Filippi P., Loveluck B. (2016), “The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure”, Internet Policy Review, vol. 5, n°4.

Godefarge F., Rossat R. (2016), Principes clés d’une application Blockchain, EM Lyon, https://www.academia.edu/36197380/Principes_cl%C3%A9s_dune_application_blockchain

Hearn M. (2016), « The resolution of the Bitcoin experiment », https://www.finyear.com/Mike-Hearn-The-resolution-of-the-Bitcoin-experiment_a35109.html

May T. (1992), “The Crypto Anarchist Manifesto”, November, https://www.activism.net/cypherpunk/crypto-anarchy.html

Nakamoto S. (2008), “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf

Perreau C. (2020), “ICO : définition, liste, la situation en France…”. JDN, https://www.journaldunet.com/economie/finance/1195462-ico-definition-liste-la-situation-en-france-decembre-2019/

Peters G. W., Panayi E. (2016), Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money.

Rancière J. (2020), « L'offensive du capitalisme absolutisé », Les Inrockuptibles n°1262, pp. 24-25.

Ribeiro A. (2016), La Blockchain et ses potentielles applications, Université de Genève.

Ricoeur P. (1984), « L'idéologie et l'utopie : deux expressions de l'imaginaire social », Autres Temps. Les cahiers du christianisme social, n°2, p. 53-64.

Rolland M., Slim A. (2017), « Economie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions », Revue Economie et institutions, n° 26.

Szabo N. (1998), "Secure Property Titles with Owner Authority", https://nakamotoinstitute.org/secure-property-titles/

Szabo N. (2005), "Bit Gold", https://nakamotoinstitute.org/bit-gold/

Vidalenc E. (2019), Pour une écologie numérique, Les Petits Matins, collection « essai ».

Wyman O. (2016), The Finetech 2.0 Paper. Rebooting Financial Services, Santander InnoVenture.