



BLOCKCHAIN, AU DÉFI DE LA CONFIANCE

Janvier 2018

**Cette étude a été réalisée avec le soutien de la
Fondation IF - International foundation**



Sous la direction de Pierre GUEYDIER, Directeur de la Recherche, OPTIC

Avec les contributions de :

Antonin PUJOS, Fondation Zermatt Summit
Renaud REDIEN-COLLOT, Institut Friedland

Et la participation de :

Serhane DENDANI, Institut Friedland
Adrian PABST, University of Kent
Thierry PHILIPPONNAT, Institut Friedland
Hubert de VAUPLANE
Izadora XAVIER

Le réseau OPTIC

Réseau de recherche internationale pluridisciplinaire créé en 2012, OPTIC anime des groupes de travail dans les lieux où se développent les technologies de rupture avec ceux qui les conçoivent. A Berkeley, Stanford, Boston, Genève ou Paris, les experts du réseau étudient l'impact de ces technologies d'avenir sur les activités humaines et sur nos sociétés.

OPTIC relie des universitaires (en sciences sociales, philosophie, économie, ...), des entrepreneurs et la société civile créant un cercle de réflexion et d'innovation dédié aux enjeux éthiques des technologies de rupture. L'objectif d'OPTIC est de créer des espaces de dialogue entre des acteurs majeurs de différentes disciplines tous tournés vers l'innovation technologique et ses implications sur la vie humaine.

OPTIC est porté par la Human Technology Fondation dont le Conseil d'Administration est présidé par S.E. le Prince Nicolas du Liechtenstein et le Comité Exécutif par le Fr. Eric Salobir.

Initié par l'Ordre catholique des Prêcheurs, OPTIC n'en reste pas moins totalement autonome dans le choix de ses recherches thématiques et la direction des travaux de recherche.

optictechnology.org
contact@optictechnology.org



Getty

Disruptive technologies, technologies de rupture. Le terme, qui a faveur des entrepreneurs et des médias, sonne comme l'annonce d'une révolution ; celle des nouvelles technes qui s'immiscent dans chaque aspect de notre quotidien, transformant notre façon de travailler, de communiquer, de nous divertir ou de nous soigner : l'économie, la politique, la finance et le système de santé en sont profondément impactés au point que la neutralité de ces technologies apparaît de plus en plus comme une illusion. On les découvre porteuses, de pré-requis, de valeurs et, pour tout dire, d'un projet de société, parfois inconsciemment inscrit dans leur code par leurs concepteurs.

Aborder la complexité et la rapidité de ces transformations, afin d'en évaluer les opportunités comme les risques, requiert une approche internationale et trans-disciplinaire, qui dépasse le monde de la « tech » et celui de l'entreprise. Pour mener à bien cette tâche, le réseau OPTIC rassemble depuis plusieurs années des spécialistes des sciences humaines et de la technologie, ainsi que des représentants du monde des affaires et de la société civile. Ces travaux, menés à huis clos, ont permis de dresser un panorama clair des enjeux sociétaux et de sensibiliser les acteurs de la révolution technologique aux enjeux éthiques de leurs décisions.

Pour la première fois en 2018, OPTIC a décidé d'ouvrir cette réflexion en publiant une série de courts livres blancs sur les sujets qui nous semblent les plus épineux. Cette démarche vient en complément du travail réalisé par les instituts de recherche public et les cabinets de conseil. Notre approche est spécifiquement centrée sur la place de l'humain dans les bouleversements que nous étudions.

Ces premiers documents, rédigés à Paris et présentés au Collège des Bernardins, ouvrent la voie à une série d'autres publications par les équipes de recherche d'OPTIC, en lien avec de grands centres universitaires, à Genève, Toronto, Boston, Berkeley, Rome et Oxford.

Je vous invite à consulter l'actualité de nos travaux de recherche sur www.optictechnology.org, à réagir et à prendre part à cette conversation.

Eric Salobir o.p.
Président d'OPTIC

Partenaires :



Résumé

Attraction 2017 du monde numérique, le Bitcoin, comme concrétisation la plus aboutie de la technologie Blockchain, subit en ces derniers jours de 2017 un prévisible réajustement après des mois de spéculation échevelée. Cette bulle spéculative n'est pas sans rappeler celle qui frappa quinze ans plus tôt un autre protocole : le TCP/IP plus connu sous le terme d'Internet.

En évitant de céder à un effet de mode, cette contribution a souhaité comprendre ce que changeait la Blockchain dans l'environnement socio-technique et politique du numérique. Après un rappel des fondements anthropologiques de la notion de monnaie et de contrat social - deux dimensions essentielles que les concepteurs de la Blockchain prétendent renouveler - nous affirmerons d'une part que le qualificatif de monnaie est impropre pour qualifier le Bitcoin et que les promesses de décentralisation du pouvoir promises par cette technologie font en réalité le lit d'une technocratie radicale.

Mais les discours prophétiques sur la Blockchain ne doivent pas cacher de nombreux horizons entrouverts, notamment au sein de communautés d'acteurs de l'innovation qui s'agrègent progressivement autour d'elle. Plus largement, nous concluons cette approche exploratoire du phénomène émergent par l'esquisse d'une géopolitique de formes de confiance distribuée et par un appel à de futurs chantiers de recherche transdisciplinaire.

Blockchain, au défi de la confiance

5	RÉSUMÉ
7	INTRODUCTION
9	APPROCHES ANTHROPOLOGIQUE ET TECHNO-POLITIQUE DE LA BLOCKCHAIN
10	Enjeux anthropologiques
10	Dette, souveraineté et confiance
12	Compte, paiement, monnayage
15	Enjeux techno-politiques
15	Blockchain, théories du contrat social et souveraineté
18	Blockchain et gouvernement invisible
20	Conclusion : Crypto ou pseudo-monnaies ?
23	IN CODE WE TRUST ? RUPTURES ET PROMESSES
23	Deux ruptures et une promesse
24	La rupture par l'innovation
25	La rupture par le modèle professionnel et social
26	La promesse d'une société de l'information distribuée
29	Vers une géopolitique de la Blockchain
29	La souveraineté contre la Blockchain
29	Criminalité organisée
30	Une souveraineté réaffirmée des régulateurs et des banques centrales
31	La souveraineté par la Blockchain
31	Identité
32	Puissance de calcul et puissance géopolitique
33	Une géopolitique de la confiance distribuée ?
35	CONCLUSION
37	RÉFÉRENCES

Introduction

L'actualité techno-économique des dernières semaines de l'année 2017 aura été largement accaparée par la thématique du Bitcoin et de la Blockchain. En effet, la "monnaie" virtuelle aura été l'objet d'une spéculation aussi échevelée qu'irrationnelle contraignant les autorités mondiales de régulation à tirer la sonnette d'alarme sur ce qui était encore considéré il y a peu comme un non-sujet par les acteurs et les responsables des politiques économiques et financières. Controverses, débordements, complexité, incertitude, contradictions transparaissent de la presse grand public aux rapports étatiques en passant par les rares articles académiques qui tentent simplement de comprendre ce phénomène émergent qui prétend révolutionner les modalités d'une composante essentielle des relations humaines et sociales : la confiance. Rarement un projet technologique n'aura

affirmé avec une telle force un projet éminemment politique en rupture avec le concept de confiance, une des valeurs cardinales du lien social, ciment de l'édification collective du Bien commun. Les promesses démesurées de cette technologie doivent nous conduire à la plus grande prudence. Les limites et les faiblesses inhérentes à ce projet comme à tous ceux qui promettent la résolution de questions socio-politiques par la technologie sont très nombreuses. Nous n'aurons pas ici la prétention de tirer en quelques dizaines de pages des conclusions définitives sur ce sujet. Néanmoins, la Blockchain et son idéologie nous poussent à tenter d'en explorer et comprendre les arcanes. La résistance de cet objet à la compréhension, comme défi intellectuel, nécessite des efforts collectifs, pluridisciplinaires et transversaux. Ce texte a donc un objectif largement

BLOCKCHAIN

La Blockchain est une technologie de stockage et de transmission d'informations à coût minime, sécurisée, transparente, et fonctionnant sans organe central de contrôle.

Par extension, une Blockchain (littéralement une « chaîne de blocs ») désigne une base de données sécurisée et distribuée (car partagée par ses différents utilisateurs), contenant un ensemble de transactions dont chacun peut vérifier la validité. Une Blockchain peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable.

Source : <https://Blockchainfrance.net/le-lexique-de-la-Blockchain/>

exploratoire. Il cherche modestement à éclairer sans naïveté ou défiance les enjeux de la Blockchain et à esquisser un programme de pistes de recherche. Pour ce faire, nous adopterons une approche « latérale » qui n'aborde pas de front la technicité de la Blockchain, ni ses applications entrepreneuriales que d'autres textes traitent déjà. Nous tenterons dans une première partie d'interroger les sous-bassements anthropologiques de la notion de monnaie que le Bitcoin, comme principale et première application concrète de la Blockchain, cherche à mimer. Puis, la question du contrat social comme mise en œuvre politique des mécanismes

de confiance sociale sera comparée aux promesses et aux contradictions politiques et sociales de cette technologie. Dans une seconde partie, en tentant de dépasser les écueils du catastrophisme ou de la fascination, nous donnerons la parole à des acteurs de la prospective et de la finance, témoins engagés des ruptures et des promesses de la Blockchain. Enfin, nous soulignerons la portée globale et polymorphe du sujet en dessinant les contours, certes encore largement incertains, d'une géopolitique de la confiance distribuée par la Blockchain.

Approches anthropologique et techno-politique de la Blockchain

Depuis son apparition en 2009, la crypto-monnaie Bitcoin et sa technologie sous-jacente, la Blockchain, ont affiché de profondes ambitions de disruption, non seulement envers les institutions bancaires et financières, mais jusqu'aux relations de pouvoir en général. Un tel horizon révolutionnaire demande à être replacé dans une perspective anthropologique et politique afin d'en comprendre les ressorts et les chances de succès éventuelles.

Le Bitcoin se présente idéologiquement comme l'accomplissement par la technique du projet néolibéral de fin de monopole de l'État-nation sur le corps social¹. Le caractère décentralisé et autogéré s'alimente du rêve libertarien de la fin d'un contrôle politique et gouvernemental des échanges, censé être la cause d'injustices sociales provoquées par l'entente anti-démocratique entre capital et pouvoir. La Blockchain souhaite donc résoudre les effets négatifs du centralisme étatique et économique par un assemblage socio-technique qui éliminerait les points de contrôle. Dans ce contexte, les méthodes cryptographiques, conçues comme garantes de la vie privée

et du secret des correspondances², sont promues comme capables de structurer des relations sociales auto-gérées et auto-organisées hors de la surveillance étatique, sans tierce partie source de confiance collective et assurant la coordination sociale.

Afin de mesurer les enjeux de la Blockchain en essayant d'éviter une lecture idéologique, nous nous proposons de revisiter les principaux fondements anthropologiques du concept de monnaie pour essayer de comprendre comment le Bitcoin tente de les traduire dans une technologie. Dans un second temps et face à l'ambition de renouvellement du contrat social, nous replacerons la discussion dans la perspective des principales théories politiques du contrat social pour, de nouveau, réarticuler le concept de Blockchain avec l'histoire politique afin de mieux saisir à la fois son originalité, ses limites théoriques et, éventuellement, ses apports positifs pour le Bien commun.

1. Friedrich HAYEK, *The Denationalization of Money*, 1976 et Milton FRIEDMANN, *The Counter-Revolution in Monetary Theory*, 1970.

2. Il s'agit ici du courant Cypherpunk de la fin des années 1980, porté par des manifestes comme le « Crypto Anarchist Manifesto » de Timothy C. MAY.

https://dpya.org/wiki/images/2/24/The_Crypto_Anarchist_Manifesto.pdf

Enjeux anthropologiques

Pour saisir les enjeux posés par la Blockchain et sa principale concrétisation – la crypto-monnaie – il est utile et nécessaire d'éclairer les fondements du concept de monnaie aussi universel que résistant à la compréhension. Dans un monde théorique sans monnaie, chaque individu serait contraint de trouver une situation où il représente pour autrui ce qu'autrui représente pour lui afin de réaliser ce que les économistes appellent « la double coïncidence des besoins », vulgarisée par le terme de « troc ». Face à cette situation extrêmement limitée en termes d'échange, l'individu sait néanmoins que ses homologues sont dans la même situation. Mais, l'intérêt personnel effondre cette fable qui consisterait à produire pour autrui sans dédommagement immédiat. Comme personne ne peut mémoriser l'histoire de toutes les transactions – ce que promet justement la Blockchain – la monnaie est parfois théorisée comme un *record keeping device* des sociétés nombreuses³ et décentralisées. La monnaie serait ainsi assimilable à une technologie d'enregistrement et à un substitut à la mémoire. Définition

partielle de la monnaie, que la technologie de la Blockchain assume comme registre infalsifiable et général de transactions.

Dette, souveraineté et confiance

Selon les travaux de Bruno Théret⁴, dont nous nous inspirerons ici, la science économique s'est paradoxalement peu intéressée à la monnaie. Pour l'essentiel, la monnaie est revêtue d'un caractère de neutralité – argument idéologique par ailleurs largement utilisé aussi pour la technologie en général – comme simple arbitraire numéraire. Pour la plupart des économistes, seule l'influence irrationnelle de l'État peut perturber cette transparence opérationnelle de la monnaie avec pour effet de perturber l'allocation optimale des ressources produites par la théorie de l'équilibre et du libre jeu des marchés.

Alors que les crises monétaires attestent de l'inverse⁵ - songeons aux liens entre crise de l'euro et crise politique du projet européen - les théories économiques n'ont eu de cesse de dépolitiser la question monétaire. Dans le sillage d'une approche interdisciplinaire initiée par Michel Aglietta, André

BITCOIN

(De l'anglais bit : unité d'information binaire et coin « pièce de monnaie »), est d'une part une monnaie virtuelle de type monnaie cryptographique et d'autre part un système de paiement pair-à-pair, présenté par une personne se cachant sous le pseudonyme Satoshi Nakamoto, qui annonce son système en 2008 et publie le code source accessible en 2009.

Source : <https://fr.wikipedia.org/wiki/Bitcoin>

Orléan ou Jean Cartelier, il semble nécessaire de replacer la question de la monnaie dans une approche plus large tracée par les sciences sociales.

Comme le droit ou le fait religieux, la monnaie frappe d'abord par son caractère a priori universel dans le temps et l'espace. Réduire la portée de cette réalité anthropologique à ce « que fait » la monnaie semble insuffisant pour comprendre son origine et sa portée.

Ainsi, plutôt qu'une simple rationalisation du troc ou une origine étatique, une hypothèse intéressante et globalement partagée par les anthropologues, pose une dimension sacrificielle liée à la dette de vie comme origine de la monnaie. La vie étant fondamentalement un don, celle-ci donnée, reçue et rendue, crée un ensemble de dettes et de créances réciproques. Ces dettes tutélaires à l'égard d'autorités symboliques variables selon les sociétés ne peuvent être soldées que par la mort ou l'exil, mort sociale hors du groupe structuré par cette dette tutélaire commune. La monnaie, abondamment utilisée au cours des rituels sacrés, « offre un substitut non violent aux victimes vivantes des paiements sacrificiels offerts aux créanciers éternels de la dette de vie ». La monnaie est le médium qui donne une forme mesurable et quantifiée à ce tissu de dettes, une unité de compte qui constitue une représentation symbolique de l'unité sociale. Par exemple, pour les

dettes verticales entre humains et autorités immortelles (ancêtres, divinités, clans, nation...) il peut s'agir de sacrifices aux dieux, d'impôts aux institutions religieuses ou étatiques, de dettes sociales mutuelles dans les sociétés solidaristes. Dans une approche horizontale entre groupes humains qui perdurent et croissent en échangeant du capital de vie, on peut citer les mécanismes de dots, d'héritage, de dons ou encore d'amendes pour rapt et meurtres... Ainsi, en dépit de la mort de ses membres, un groupe humain parvient par le paiement diversifié de ses dettes de vie à perdurer dans le temps et l'espace. La monnaie permet donc de totaliser et d'unifier ce système de dette de vie inscrit au cœur de la reproduction sociale.

Cette hypothèse sur l'origine de la monnaie permet d'en expliciter à la fois l'universalisme (il n'existe pas de société où l'homme soit immortel qui lui permettrait de se soustraire aux dettes de vie) et en même temps l'extraordinaire diversité formelle.

Le deuxième pilier de la notion de monnaie réside dans le lien qu'elle entretient avec la notion de souveraineté. La dette de vie due aux autorités suprahumaines d'une société doit être mise en relation avec le souverain qui incarne et condense la verticalité du pouvoir politique et avec l'immortalité en tant que ce qui survit collectivement à la mort individuelle. Qu'il s'agisse de souveraineté transcendante (divine ou

3. « If the function performed by money can be superseded by a perfect historical record of transactions, then money's only technological role must be to provide that record », Narayana R. Kocherlakota, « Money Is Memory », *Journal of economic theory* 81, 232-251 (1998).

4. Michel AGLIETTA et André ORLÉAN (dir.), *La monnaie souveraine*, Paris, Odile Jacob, 1998.

5. Bruno THÉRET (dir.), *La monnaie dévoilée par ses crises*, Paris, Éditions de l'eHESS, 2 volumes, 2007.

ancestrale) ou immanente (peuple, nation, contrat social), la dette de vie à l'égard du souverain ne peut être soldée. Pour renforcer le lien politique et le rendre perpétuel, la monnaie doit être souveraine et intouchable. Il en va du crédit de l'État qui doit s'auto-soumettre à cette autorité symbolique représentée par la monnaie. Y compris dans l'État moderne, cette fonction anthropologique de la monnaie perdure sous la forme de la fiscalité comme obligation viagère vis-à-vis de l'État avec la contrepartie de la dépense de protection sociale comme obligation de l'État envers chaque citoyen.

Troisième et dernier pilier : la confiance et la foi sociale instituées par la monnaie. Le concept de fiduciaire est lui aussi complexe : est-il généralisable à toute monnaie ? De quelle nature précise est le lien de confiance produit par la monnaie ? La confiance produit-elle l'efficacité de la monnaie ou est-ce l'inverse ? Pour tenter de clarifier ce point essentiel, notamment dans le cas des crypto-monnaies censées être « décentralisées » et affranchies de tiers de confiance, il est nécessaire de distinguer trois formes de la notion de crédibilité monétaire⁶ : la confiance méthodique, la confiance hiérarchique et la confiance éthique.

La confiance méthodique (*confidence*) est la plus évidente à admettre, elle participe d'un comportement mimétique qui fait que chaque individu croit de façon routinière en la valeur faciale de la monnaie

et à sa persistance dans le temps : la monnaie est socialement acceptée en raison du consensus social qui fait que chacun s'attend à ce qu'autrui accepte la monnaie comme moyen d'échange stabilisé. La confiance hiérarchique (*credibility*), quant à elle, désigne un mécanisme plus politique qui établit la crédibilité de l'émetteur de la monnaie par un représentant légitime de la communauté de compte et de paiement. Enfin, la confiance éthique (*trust*) renvoie à l'autorité symbolique du système de valeurs collectives que la monnaie incarne par ses modes d'émission, de distribution et de circulation qui doivent paraître comme capables d'assurer la reproduction de la société dans le respect de ses valeurs et la conformité aux principes de justice (à l'inverse des narco-dollars et de "l'argent sale" par exemple).

Compte, paiement, monnayage

En articulation avec ces trois formes de confiance, la monnaie assume trois états différents et complémentaires. Le premier état le plus évident est celui de pouvoir établir un compte, une comptabilité. Grâce à un système de signes reconnaissables, à leur utilisation répétitive et de règles du jeu connues, la monnaie permet au niveau individuel et mental de tisser un réseau de confiance. " Les personnes révélant leur confiance dans la monnaie en participant à l'utilisation des signes monétaires [révèlent] par là même, [...]

6. AGLIETTA et ORLÉAN (2002) l'affirment encore avec plus de force à la suite de Simiand (1934) en disant que la monnaie est un lien de confiance

qu'elles partagent une confiance commune dans l'ordre social⁷. Si l'on en reste à cette définition primaire de la monnaie comme simple confiance dans un système de signes – à l'instar des crypto-monnaies – on peut en effet considérer, comme les partisans du *free-banking*, que ce système de signes permet une compréhension partagée entre les utilisateurs sans autorité centralisée contrôlant la dissémination de cette compréhension.

Mais, tout comme la langue - ensemble de signes par excellence - permet l'interaction sociale mais distribue aussi le pouvoir en fonction du degré de maîtrise, la ressource monétaire est inégalement répartie, en tant que source d'appropriation et de contrôle privatif. D'outil de coopération et de coordination, la monnaie peut devenir source d'inégalités et de conflits en raison de sa distribution inégale qui porte atteinte à la justice des relations sociales. La monnaie n'est donc pas qu'un outil de compte capable d'engendrer de la coordination comptable. Pour maintenir la confiance, elle doit aussi permettre, par une régulation des conflits relatifs à la distribution des moyens de paiement, un bon compromis social capable d'apaiser les conflits d'appropriation en plus d'assurer une bonne convention de coordination. À la différence des crypto-monnaies, la monnaie classique ne s'exprime pas seulement dans un langage mais aussi par un système d'objets – les moyens de paiement – qui participent à objectiver la monnaie pour

compléter son premier état sous forme de langage de coordination.

C'est au sujet de ces deux états de la monnaie (système de compte et moyen de paiement) que vont s'opposer les principales théories économiques. Cette hybridation anthropologique entre matérialité et immatérialité est manifestement incarnée par le caractère biface des moyens classiques de paiement (pièces ou billets). Du côté face, est inscrit le symbole de l'autorité politique qui a frappé la monnaie, du côté pile, la valeur de compte facteur de coordination des échanges sociaux. Le paradoxe du moyen de paiement vient du fait qu'il incorpore à la fois une dimension qui permet une relation entre les personnes, évidence décrite par les théories économiques mais qui oublie en général le second aspect qui consiste à permettre aussi de clore une relation d'échange sous l'arbitrage d'une autorité de confiance qui permet aux acteurs d'être quittes dans leur échange marchand.

Bruno Théret⁸ prolonge cette analyse pragmatique en constatant que la figure historique de la monnaie ne compte pas seulement deux faces qui permettent donc d'unifier relation et détachement entre les personnes, mais trois. En effet, la tranche d'une pièce, qui matérialise son poids par une épaisseur, exprime que le troisième état de la monnaie réside dans des règles d'émission et de circulation des moyens de paiement. Cet aspect institutionnalisé

7. Carl WENNERLIND, "Money Talks, but What is it Saying? The Semiotics of Money and Social Control." *Journal of Economic Issues*. September. 2001. Vol. 35. No. 3: 557-74.

8. THÉRET, Bruno. « Les trois états de la monnaie. Approche interdisciplinaire du fait monétaire », *Revue économique*, vol. vol. 59, no. 4, 2008, pp. 813-841.

SMART CONTRAT

Les smart contrats constituent l'un des types d'usage les plus prometteurs de la Blockchain. Concrètement, il s'agit de programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable et inscrites dans la Blockchain. Ils fonctionnent comme toute instruction conditionnelle de type « if – then » (si telle condition est vérifiée, alors telle conséquence s'exécute).

Source : <https://Blockchainfrance.net/2016/01/28/applications-smart-contracts/>

définit ainsi les fonctions de monnayage et de régulation propre à la monnaie.

Après la dimension comptable de la monnaie qui se situe au niveau mental et cognitif, celle d'un objet/moyen de paiement qui engendre la fonction économique de la monnaie, la monnaie est inséparable d'un point de vue anthropologique d'une forme politique de la communauté de paiement. Une communauté de paiement est un groupe humain dans lequel circule un ensemble de moyens de paiement convertibles articulés à un système de compte. En définitive, le cœur du mécanisme anthropologique de la monnaie réside dans sa capacité à articuler les contradictions entre un système de compte rationnel et réaliste (la monnaie réelle) et un système abstrait de moyens de paiement (la monnaie abstraite). La monnaie permet de créer un espace homogène de valeur au sein d'un groupe humain par-delà les discontinuités. Il est alors crucial qu'une régulation institutionnelle s'opère entre forme unitaire de compte et forme plurielle de paiement.

Pour résumer, la monnaie se présente dans trois états complémentaires qui lui confèrent sa puissance totalisante d'opérateur social de premier plan : le compte incorporé dans chaque sphère mentale et cognitive individuelle, les instruments de paiement matériels comme support objectivé et des institutions garantes de l'organisation des règles du jeu du monnayage. En ce sens, la jonction entre un langage spécifique (le système de compte), un objet (les moyens de paiement) et une institution (règle du jeu de monnayage) confère à la monnaie le statut de fait social total⁹ symbolique, économique et politique. À chaque état correspond un effet de confiance : une confiance méthodique dans le système de calcul, une confiance éthique dans les valeurs d'usage des moyens de paiement et une confiance hiérarchique dans les institutions garantes des règles du jeu. Ceci explique à la fois sa dimension universelle comme fait social et son immense pluralité de manifestations.

9. Marcel MAUSS, « Essai sur le don : Forme et raison de l'échange dans les sociétés archaïques », *L'Année sociologique*, 1923-24.

Enjeux techno-politiques

Face à ces fondements anthropologiques de la monnaie brièvement rappelés, quelles conclusions en tirer à propos des crypto-monnaies à l'usage encore balbutiant ? Finalement, sont-elles, comme le prétendent leurs promoteurs, de futurs substituts parfaits aux divers sources de conflits que la monnaie classique a tenté au cours de l'histoire de l'humanité de contrôler au point de devenir, comme nous l'avons souligné, un opérateur social totalisant et englobant ?

Plus largement, nous avons vu que l'ambition des concepteurs de la Blockchain est de déployer un substitut total aux modes classiques de distribution du pouvoir. La monnaie n'étant qu'un cas, certes emblématique, de cette rupture, il faut ici se replonger dans les fondements de l'histoire politique des théories du contrat social pour en saisir les enjeux. Mais surtout, malgré sa très courte existence, nous allons voir que le Bitcoin a déjà traversé plusieurs crises de gouvernance dont la gestion a pu révéler les limites des postulats techno-politiques de cette technologie.

Blockchain, théories du contrat social et souveraineté

Pour tenter de mieux cerner la portée politique de la Blockchain en tant que registre public et source de contrats décentralisés, une mise en perspective avec les théories politiques et philosophiques

du contrat social semble donc judicieuse. Au-delà des premières applications de crypto-monnaie, la technologie de la Blockchain au sens large permet de conclure, sans tiers de confiance, des « contrats intelligents » (*smart contracts*). Il ne s'agit plus dans ce cas de transactions de quantité de jetons, mais de textes et de règles d'accord généraux applicables entre deux contractants, quel que soit le domaine. Dans cette perspective, la Blockchain serait donc capable, au-delà du cas de la monnaie, de configurer des formes spécifiques d'organisation sociale et politique. Il semble ainsi intéressant à l'instar de Reijers, O'Brolchain et Haynes, d'approcher les enjeux de la Blockchain à travers les théories du contrat social. Ces auteurs nous invitent à suivre trois des principales théories politiques libérales du contrat social en les confrontant aux caractéristiques de la Blockchain : celles de Thomas Hobbes, Jean Jacques Rousseau et John Rawls¹⁰. Hobbes et Rousseau postuleront un « état de nature » comme situation initiale pour tenter d'en déduire les prémisses des organisations sociales et politiques. Mais leur postulat est radicalement opposé. Comme on le sait, Rousseau postulera un état pacifique et idyllique de la situation pré-sociale, les institutions comme la propriété privée ou la monnaie n'auront pour effet que de corrompre cet état primitif. À l'inverse, Hobbes et le célèbre « l'Homme est un loup pour l'homme » postule une situation initiale pré-civilisée comme un état de nature produisant entre les hommes un haut degré d'incertitude marqué par l'absence

10. REIJERS, O'BROLCHAIN et HAYNES, « Governance in Blockchain Technologies & Social Contract Theories », *Ledger*, Vol 1, 2016

de confiance réciproque entre les individus. Ces deux visions pessimistes de l'Homme – l'individu pour Hobbes, la société pour Rousseau – imposent une définition d'un contrat social doté d'un État fort. La tradition de Locke, pour sa part, prône un marché libre comme remède à l'égoïsme individuel. Rawls pour sa part, dans une perspective plus rousseauiste, postule comme situation originelle au contrat social un « voile d'ignorance » qui masque la position réciproque des contractants entre eux. Ce « voile d'ignorance » qui dissimule chaque contractant aurait pour effet de faire tendre les contrats sociaux vers un optimum d'équité.

Dans une certaine mesure, l'avènement de la Blockchain et son impact sur la formulation d'un contrat social qui lui serait associé, peut s'inspirer du concept du « voile d'ignorance » de Rawls. La technologie de la Blockchain, qui embarque des notions comme l'anonymat et semble distribuer équitablement le pouvoir, devient elle-même ce voile d'ignorance jeté sur les relations sociales. Une telle technologie semble permettre d'effacer en quelque

sorte les situations sociales relatives des contractants susceptibles de fausser la relation contractuelle (genre, origine, statut social...). Pour reprendre une approche rousseauiste, la Blockchain prétend assurer par le code deux fonctions centrales : empêcher structurellement la fraude et libérer les utilisateurs de toutes autorités étatiques ou bancaires. La veine libertarienne et anarchiste trouve ici le remède à la tendance irrémédiable des États et des banques à la corruption et ouvre une voie possible à la capacité des individus à s'auto-gérer. Enfin, les concepteurs de la Blockchain eux-mêmes présentent une version clairement hobbsienne de leur initiative. L'idée originelle de Nakamoto – l'initiateur anonyme du Bitcoin – reposant sur le constat des incertitudes de paiement entre vendeur et acheteur reprend finalement une vision pessimiste des rapports humains marqués par l'intérêt personnel et proche de la « théorie des jeux » qui voit dans la recherche de l'équilibre des menaces et des intérêts la source du contrat social.

L'apport des théories politiques du contrat social pour saisir la situation politique

ETHEREUM

Plateforme décentralisée, basée sur une Blockchain, permettant à son réseau d'utilisateurs de créer des smart contracts. La Blockchain d'ethereum fonctionne avec la monnaie Ether. Contrairement à la Blockchain du bitcoin, focalisée sur l'aspect monétaire, la Blockchain d'ethereum a vocation à accueillir des programmes très divers, qui sortent du cadre purement monétaire.

<https://Blockchainfrance.net/le-lexique-de-la-Blockchain/>

initiale de la Blockchain permet donc de conclure en premier lieu que le type de contrat social qui lui a donné naissance repose sur un modèle inspiré par une conception pessimiste des relations humaines réduite à l'équilibre de la théorie des jeux telle que Hobbes a pu la définir. Parallèlement, l'idée inspirée par Proudhon¹¹, le courant anarchiste et libertarien, d'une corruption immanente à toute institution de pouvoir (États, banques...) associée à la capacité théorique des groupes humains à s'autogérer a aussi servi de récit fondateur à la mythologie de la Blockchain. Enfin, le caractère disruptif de cette technologie, au moins dans les premiers temps, a pu construire la fiction de pairs rendus égaux par le "voile d'ignorance" qui recouvrait leurs relations sociales.

Mais ces théories du contrat social ne se sont pas uniquement intéressées aux situations initiales de l'entrée en relation sociale des individus. Elles ont aussi défini les principaux modèles de souveraineté qu'il est très utile de confronter à ceux de la Blockchain et à sa gouvernance.

Pour Hobbes, une forme de gouvernement absolue est la seule solution rationnelle capable de permettre aux individus de s'arracher à leur condition de guerre de tous contre chacun. La célèbre métaphore du Léviathan concentre cette idée d'une souveraineté absolue et totalitaire à laquelle les contractants choisissent de

s'aliéner en vue de garantir l'équilibre des intérêts et des menaces. Le corps social est ainsi maintenu par la menace constante d'un système institutionnalisé de punition. D'une certaine manière, le mode de gouvernance de la Blockchain revêt des aspects d'un Léviathan technologique¹². Si les règles internes au système ne sont certes pas assorties de punitions physiques, l'impossibilité théorique de leur violation, inscrite dans le *design* de la Blockchain, oblige à ne pas avoir d'autre choix que de respecter les règles du contrat, ce qui engendre des effets d'obéissance collective comparables à ceux du pouvoir du Léviathan de Hobbes.

Néanmoins l'absence de punition physique dans la gouvernance de la Blockchain fait aussi écho à l'approche de Rousseau et à son concept « d'intérêt général » porté par la force sociale des mécanismes de consensus. Si un nœud du système décide de s'écarter des règles générales, il le peut sans risque de punition, mais se retrouve exclu et dans la situation de travailler pour rien, ce qui n'est naturellement pas dans son intérêt, ni dans l'intérêt général de tous les autres nœuds d'un système décentralisé. Il faut aussi souligner que le concept d'intérêt général présent dans la gouvernance des réseaux distribués n'est pas aussi extensif que l'idée de Rousseau. La souveraineté ne repose pas ici, comme dans le modèle de Rousseau, sur une distribution politique mais plutôt sur une distribution technologique du pouvoir,

11. Pierre-Joseph PROUDHON, *Qu'est-ce que la propriété ? ou Recherche sur le principe du Droit et du Gouvernement*, Paris, 1840.

12. Brett SCOTT, *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance ?* févr. 2016, United Nations Research Institute for Social Development.

matérialisée par les capacités de calcul des mineurs qui, on le verra, ne sont que théoriquement incapables de centraliser le pouvoir techno-politique de la Blockchain.

Enfin, pour Rawls la souveraineté repose sur le principe de justice qui doit permettre aux individus de jouir des mêmes droits et libertés, ce qui semble être le cas dans le *design* de la Blockchain. Les utilisateurs ne sont pas discriminés en raison de leur statut social au sein d'une Blockchain et jouissent donc des mêmes droits et libertés. En revanche, le principe de justice distribuée semble défaillant dans la Blockchain où aucune autorité n'est en mesure de garantir une bonne redistribution des droits en cas de déséquilibre. Ce fut le cas lors de l'attaque sur le DAO en juin 2016, quand environ 50 millions de dollars de jetons Ethereum ont été détournés. La communauté *open source* des codeurs de la Blockchain s'est trouvée face à un dilemme qui dégénéra en conflit idéologique : intervenir dans le code pour rétablir la justice contredisait le principe même du système. Dans ce cas, la souveraineté de la technologie laisse apparaître de grandes faiblesses en étant incapable, sans structure de gouvernement externe au code, de gouverner la communauté des utilisateurs et d'éventuelles déviances en termes de justice. En fait, le code, dans sa version absolue c'est à dire non modifiable, peut s'assimiler à une structure tyrannique puisque le débat et tout changement y sont impossibles.

En conclusion de cette confrontation entre des modèles théoriques du contrat social et la façon dont la Blockchain produit des relations entre individus, il ressort en

premier lieu que la technologie n'est non seulement jamais neutre, mais qu'elle embarque dans son code et son *design* des modèles hybrides de gouvernance. En effet, Reijers, O'Brolchain et Haynes ont démontré que l'origine de l'idée de registre décentralisé repose à la fois sur une conception anarcho-libertarienne et sur une vision négative de la capacité des individus à entretenir des relations pacifiées. Ces postulats ont conduit les initiateurs de la Blockchain à l'ancrer dans un techno-totalitarisme qui exclut tout questionnement de son autorité. La décentralisation du pouvoir et la punition par l'exclusion portées par une vision rousseauiste de la volonté et de l'intérêt général transparaît aussi à l'étude du contrat social permit par la Blockchain. Concernant l'approche de Rawls, si cette technologie peut s'apparenter à une version limitée du « voile de l'ignorance », elle est incapable d'organiser une justice distribuée.

Blockchain et gouvernement invisible

C'est à travers les crises et les controverses que la distribution de pouvoir et la répartition de la gouvernance apparaissent au grand jour. Malgré son histoire récente, la Blockchain, et sa principale traduction le Bitcoin, ont connu trois graves crises de gouvernance : en août 2015 à l'occasion d'un conflit entre développeurs sur une question technique, en juin 2016 à l'occasion du *hack* d'un DAO avec la subtilisation de jetons d'ethereum d'une valeur d'environ 50 millions de dollars et en août 2017 à l'occasion d'un *fork* qui a donné naissance au Bitcoin Cash incompatible désormais avec la chaîne Bitcoin historique.

Dans leur article¹³, De Filippi et Loveluck explorent à l'aune de ces crises de gouvernance deux types de mécanismes de coordination au sein de la Blockchain : la gouvernance par l'infrastructure embarquée dans la technologie et la gouvernance de l'infrastructure par la communauté restreinte et élitiste des développeurs et ce, en dépit des mythes fondateurs de la Blockchain présentée comme le parachèvement d'un registre infalsifiable, open source et décentralisé. Une première remarque à propos de la gouvernance du Bitcoin repose sur l'évidence - toujours utile à rappeler - qu'entre les intentions originelles d'une technologie et sa confrontation à son environnement socio-culturel dans lequel elle opère, se créent inévitablement de nombreuses divergences. Notamment la tendance, dans une économie de marché, à inexorablement concentrer la richesse et le pouvoir entre les mains de quelques acteurs ayant progressivement acquis des positions de domination. C'est ainsi magistralement le cas des mineurs, dont l'existence comme système incitatif de sécurisation est une originalité de la Blockchain mais qui au bout de quelques années se concentrent progressivement entre les mains de quelques majors chinoises. Pour reprendre une image de la thématique marxiste, les mineurs jouent le rôle de capitalistes quand les développeurs et autres utilisateurs représentent la force de travail. En fait, la gouvernance de la Blockchain repose sur une fiction (ou une utopie) : considérant que ce que le protocole de base a été rédigé et écrit sans qu'il soit possible de le modifier de près ou de

loin (le fameux "code is law" de L. Lessig), la réalité est bien différente dès lors que les enjeux dépassent la seule question de principe pour toucher à des considérations plus financières. Ce qui explique que dans le piratage de The DAO, au mépris de tous ces principes, la majorité des membres du projet a préféré modifier les tables de la loi plutôt que de voir s'évaporer 50 millions de dollars.

La structure implicite de gouvernement du Bitcoin présentée comme auto-entretenu par une communauté *open source* de contributeurs repose en définitive sur la compétence technique très pointue d'un très petit nombre de développeurs qui sont en mesure d'accepter ou non telle amélioration du code proposée par la communauté. Cette élite littéralement technocratique, et aux compétences néanmoins avérées, entre en contradiction avec le mythe originel du Bitcoin. En effet, lors de la « crise de la taille de bloc »²², la controverse a surgi parmi l'équipe centrale des développeurs entre une approche qui préservait le caractère ouvert et distribué avec une autre qui souhaitait techniquement accroître le rendement de la technologie en restreignant la décentralisation au risque d'une plus faible sécurité et d'une forme de « trahison » idéologique de l'héritage du fondateur Nakamoto. Ce conflit ne trouva pas d'issue et engendra un *fork*, c'est à dire une nouvelle Blockchain (Bitcoin XT) qui permit exactement ce que la technologie Bitcoin affirmait comme impossible : dépenser deux fois le même Bitcoin.

13. DE FILIPPI, P. & LOVELUCK, B. (2016). "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure". *Internet Policy Review*, 5(3).

En tout état de cause, les intentions politiques d'une technologie – nombreuses et ambitieuses dans le cas de la Blockchain – ne peuvent pas être uniquement résolues par des moyens techniques comme le montre l'histoire récente du Bitcoin et de la Blockchain. Une technologie algorithmique ne peut, à elle seule, organiser les relations humaines. Des arènes de discussions publiques sont indispensables pour résoudre et coordonner les problèmes issus de la rencontre des postulats des initiateurs de cette technologie avec la réalité et la complexité de la réception sociale des usagers. En définitive, le Bitcoin comme infrastructure informationnelle doit être compris comme introduisant et produisant un certain type de relations sociales. Comme toute infrastructure, le Bitcoin est une technologie de pouvoir invisible qui opère comme une boîte noire à l'abri d'un *design* technocratique qui obscurcit les relations de pouvoir.

Pour conclure, la gouvernance du Bitcoin est donc composée de deux dimensions, l'une est constituée par une infrastructure technique qui embarque dans son *design* un certain nombre de principes de fonctionnement et l'autre par une petite communauté élitiste de développeurs. La suppression de tiers de confiance encodée dans la technologie croit pouvoir se passer de point de contrôle. Mais en pratique, dès que la technologie se déploie, des problèmes ne manquent pas de surgir par les usages non anticipés qui exigent en retour l'établissement d'institutions sociales

capables de résoudre les conflits de pouvoir. Au point de revoir apparaître une figure majeure de l'institution étatique, à savoir le juge, appelé à trancher les différends nés des problèmes de gouvernance¹⁴.

Conclusion : Crypto ou pseudo-monnaies ?

Sans s'attarder sur le souhait de confidentialité qui, dans un esprit libertarien, est à l'origine même de la création de la technologie Blockchain, il est opportun de s'interroger pour essayer de mieux cerner les caractéristiques proprement monétaires des crypto-monnaies¹⁵.

Comme nous l'avons déjà vu, les économistes - depuis Aristote - s'entendent pour considérer comme monnaie tout instrument qui remplit les trois fonctions d'instrument de paiement, de réserve de valeur et d'unité de compte. Ceci ne suffit toutefois pas pour en faire une monnaie à part entière. En effet, une condition supplémentaire doit aussi être satisfaite : que cet instrument ait « cours légal » (*legal tender*) ce que les juristes appellent le « pouvoir libérateur » de la monnaie, et soit unanimement accepté dans une « zone monétaire ».

Une telle zone monétaire est donc corrélative d'une communauté et liée à la présence d'un État qui est la manifestation d'un certain contrat social et qui – au plan monétaire - garantit le « cours légal » de la monnaie et permet à tous les utilisateurs de faire

14. Suite à des problèmes de gouvernance lors de la levée de fonds Tezos en 2017 sur cette nouvelle crypto-monnaies, cinq class actions ont été déposées aux États Unis.

15. Cette conclusion a été rédigée par Antonin PUJOS, Fondation Zermatt Summit

confiance à la monnaie ayant cours dans la zone. L'État assume ainsi la responsabilité pleine et entière pour la monnaie et pour l'usage qui en est fait par la communauté.

Cette notion "d'acceptabilité" d'une monnaie est d'ailleurs celle reprise par la BCE pour expliquer qu'à l'heure des monnaies scripturales, ce n'est plus le montant de réserves d'or qui permet d'apprécier la valeur d'une devise, mais son « acceptabilité » en tant que moyen d'échange et son attrait comme réserve de valeur. C'est aussi de la même manière que le FMI présente le fonctionnement d'une monnaie lorsque l'institution précise qu'une monnaie fiduciaire n'a de valeur « *que celle qu'une nation décide de lui assigner* ». Ainsi, le Bitcoin tout comme l'euro ou le dollar n'a pas de valeur intrinsèque ou matérielle, mais il se distingue justement des monnaies légales par son acceptabilité, laquelle est aussi fonction de la richesse du pays émetteur.

En l'absence d'un État qui permettrait de repérer une « zone monétaire » relevant d'un contrat social visant le Bien commun de la communauté en question, les crypto-monnaies doivent fonctionner en s'adossant à des technologies numériques qui ont pour effet de permettre aux utilisateurs d'avoir confiance dans la crypto-monnaie et de pouvoir se passer de toute référence à quelque « cours légal » que ce soit. On voit immédiatement que le point d'application de la confiance s'est déplacé de l'État et des institutions monétaires (Banque centrale et/ou banques commerciales) vers les technologies digitales auxquelles les utilisateurs doivent se fier.

Ceci soulève un certain nombre d'interrogations sur la technologie Blockchain lorsqu'elle

est appliquée au domaine monétaire, interrogation quant à l'intégrité des « mineurs », à la dépendance géographique et énergétique à leur égard, à la gouvernance régissant le protocole utilisé, toutes questions auxquelles il est impossible de répondre de façon définitive et parfaitement satisfaisante. A ceci s'ajoute que la « zone monétaire » dans laquelle la crypto-monnaie sera utilisée sera dématérialisée et bénéficiera ainsi d'une extraterritorialité de fait, hors de tout Contrat social (qui pourrait renvoyer à un certain Bien commun) et échappant a priori à toute réglementation et à tout contrôle. Sans parler des questions de liquidité et de convertibilité qui resteront sans doute longtemps problématiques.

Des utilisateurs avertis pourront éventuellement juger de la fiabilité des technologies appliquées – y compris celles de cryptographie – mais le grand public en restera encore longtemps incapable. Dès lors, il est possible d'affirmer que l'utilisation de crypto-monnaies restera réservée soit à des experts en technologies numériques et cryptologiques soit à des utilisateurs prêts à « jouer le jeu », à leurs risques et périls. Il est important de noter que, conformément aux objectifs que s'étaient fixés les créateurs des premières crypto-monnaies, les transactions effectuées en crypto-monnaies ne sont pas nécessairement confidentielles mais, parce qu'elles peuvent être effectuées de façon anonyme, elles permettent d'échapper au regard des États et des autorités fiscales et réglementaires.

La combinaison de l'anonymat des utilisateurs et de l'absence de contrôle des transactions a pour effet d'attirer bien entendu les trafics les plus douteux, ce qui gêne certains opérateurs mais pas tous....

Jusqu'ici nous nous sommes attardés sur l'utilisation qui est faite des crypto-monnaies dans les transactions économiques courantes. Le rôle de la Blockchain, dans ce domaine, se limite au fait de lister – de façon irréversible – les transactions, leurs contenus et les parties concernées. Ce n'est en définitive qu'un Grand-Livre comptable et, de ce point de vue, elle ne constitue aucun progrès significatif, en dehors des aspects de cryptologie, de vitesse d'enregistrement, de traçabilité et probablement de simplicité et de coût.

Le domaine dans lequel les crypto-monnaies présentent un désavantage immédiat est celui de l'accompagnement de l'économie par la voie du crédit. En effet, le crédit est la voie royale de la création de monnaie, puisque plus de 90% de la création de monnaie résulte d'opérations de crédit à l'origine desquelles se trouvent les banques commerciales qui ont toujours été des "tiers de confiance" par excellence. Qui dit crédit, dit en effet confiance mais confiance non pas en une technologie mais en la capacité d'une personne à remplir son obligation de remboursement. Or les promoteurs des crypto-monnaies ne veulent pas entendre parler de confiance, qu'il s'agisse de faire confiance à des personnes ou à des institutions. Dès lors, ils rendent impossible l'activité de crédit en tant que telle et interdisent aux crypto-monnaies de jouer le rôle de soutien à la croissance économique que les monnaies jouent habituellement.

Les mécanismes de création des crypto-monnaies, extrêmement complexes et contraignants, sont sans lien avec l'activité économique sous-jacente et interdisent toute possibilité de crédit. De

plus, le montant de crypto-monnaie en circulation entre les utilisateurs de celle-ci est limité artificiellement et par postulat. Cette limitation, créant dès le départ la rareté, est très favorable à l'appréciation du Bitcoin mais aurait des effets fortement déflationnistes si cette crypto-monnaie devait un jour soutenir une économie quelconque.

Cette forte capacité d'appréciation n'a pas échappé aux spéculateurs et s'est manifestée plus vivement que jamais en 2017. Elle résulte essentiellement du fait que la quantité de Bitcoin en circulation reste fixe alors que la demande de Bitcoin ne fait que croître auprès des investisseurs à la recherche d'anonymat et de complète défiscalisation. De plus, l'absence de liens fondamentaux du Bitcoin avec l'économie réelle et l'étroitesse relative de son marché lui donnent un caractère volatile et instable et en fait un instrument idéal pour la constitution d'une bulle. Ceci explique à la fois pourquoi, pendant l'année 2017, la valeur du Bitcoin est passée de 1000 \$ à près de 20 000 \$ mais aussi pourquoi le Bitcoin a très récemment perdu près de 30% de sa valeur en quelques jours fin décembre 2017, renforçant ainsi le caractère hautement spéculatif de son utilisation comme instrument d'investissement financier.

Dans le droit fil des préoccupations libertariennes, les crypto-monnaies semblent en définitive par leur caractère rare, anonyme et mécanique, favorables aux intérêts individuels des utilisateurs prêts à en accepter les risques mais, comme, par construction, tout est fait pour empêcher de les réunir dans une même communauté, ces monnaies restent très loin de ce qui pourrait être un Bien Commun.

In code we trust ?

Ruptures et promesses

Deux ruptures et une promesse

La plupart des travaux produits actuellement sur la Blockchain s'interrogent sur sa robustesse et son optimisation technologique ; les autres études publiées par les médias et les réseaux sociaux discutent de la pertinence du modèle d'affaires que promeut la Blockchain¹⁶. Toutefois, la Blockchain prétend aussi avoir un agenda social et politique. C'est sous son angle conflictuel que cet agenda s'est imposé dans les médias. Suite à l'exploitation d'une faille dans le codage du fond d'investissement (The DAO), la crise de l'été 2016 a démontré que la seule règle du code incorruptible pliait devant celle de la majorité des contributeurs. La compréhension de la dimension sociale de la Blockchain ne peut pas se réduire à l'analyse de ces/ses conflits d'intérêt. Du point de vue de la sociologie pragmatique (Lemieux,

2012), cela mérite une analyse en profondeur des représentations sociales à l'œuvre susceptibles de déterminer les tendances à agir de ses protagonistes. Dans le contexte d'innovations émergentes, Camagni (2017) suggère que les témoignages des développeurs sont soit trop techniques soit trop évangéliques pour rendre compte des dynamiques sociales qui y sont en jeu. Il semble que les acteurs périphériques mais directement associés au déploiement des innovations émergentes puissent produire des représentations sociales plus cohérentes de ce phénomène. Aussi, avons-nous décidé d'interroger des représentants de deux catégories assez hétérogènes associées à l'émergence de la Blockchain mais qui ne sont ni mineurs ni fondateurs. A partir des deux entretiens réalisés avec un investisseur – Greg Revenu¹⁷, managing Partner de Bryan Garnier -- et un prospectiviste Nicolas Loubet¹⁸, co-développeur de

16. Chapitre rédigé par Renaud Redien-Collot, Institut Friedland.

17. Greg Revenu a co-fondé Bryan Garnier en 1996 et co-dirige depuis son développement. Il a accompagné en 2015 les actionnaires de Talentia dans sa cession à Argos Soditic et a réalisé la levée de fonds de 25 millions d'euros de Jahia auprès d'Invus, ou le PIPE sur près de 20 % du capital de CAST. Depuis près de dix ans, il accompagne l'actionnaire du groupe Innov8 dans son développement, réalisant pour lui en 2015 l'acquisition d'Ascendeo (leader de la distribution d'accessoires telecom) ainsi qu'une levée de fonds de 23 millions d'euros en juillet. En 2015, ses équipes ont conseillé près d'une quarantaine d'entreprises dans les secteurs innovants, dont DBV Technologies dans une augmentation de capital après avoir organisé son IPO sur le Nasdaq pour plus de 110 millions d'euros levés.

18. Géologue de formation, Nicolas Loubet, quitte en 2008 la recherche dans son domaine pour s'engager dans de nombreux projets sur le web. En 2012, il co-fonde Bluenod (application de data viz pour le suivi de communautés Twitter) et Umeps (agence de services pour la recherche et l'innovation). Depuis 2015, il co-développe Cellabz avec Clément Epié pour faciliter l'appropriation culturelle des technologies émergentes (à commencer par la Blockchain). Il est co-producteur de DAISEE, un programme de recherche contributif sur les modes de transition énergétique. Il se définit aussi comme un analyste d'écosystèmes d'innovation.

Cellabz, nous avons identifié trois niveaux de représentations sociales qui nourrissent le développement de la Blockchain. Les représentations des acteurs de la Blockchain s'affirment en contraste de celles développées par la galaxie internet. Les tenants de la Blockchain revendiquent vis-à-vis de celle-ci une première rupture de nature technologique attribuée non seulement à l'outil Blockchain mais aussi au modèle d'innovation qu'il propose. Ils assument un second type de rupture de nature socio-professionnelle qui lie travail et engagement politique. Enfin, il est question d'accomplir un agenda socio-politique proprement dit – celui d'une société de l'information distribuée. Sur ces trois axes, nous observerons comment se situent nos deux interlocuteurs qui peuvent avoir des points de vue contrastés.

La rupture par l'innovation

La Blockchain offre une modalité innovante de transaction. Elle n'est pas garantie par un tiers mais par un algorithme. Cette proposition de valeur s'appuie sur une convention et une représentation sociale qui visent à marquer une rupture avec le modèle 'restreint' d'innovation promu par les champions d'internet.

En tant que convention qui impose un certain nombre de contraintes aux développeurs et aux spéculateurs, l'architecture de la Blockchain est asymétrique de celle d'internet. Greg Revenu note : « *Pour l'internet, le protocole n'a pas de valeur ; il appartient au domaine public (organisations à but non-lucratif, université) ; en revanche la valeur est dans l'application car c'est là que sont capturées les données qui sont*

monétisées -- revendues, traitées, analysées etc... [...] Pour la Blockchain, le protocole détient la valeur : il est très efficient, intègre des éléments de sécurité ; c'est un bien public qui est distribué à un nombre réduit de mineurs et de fondateurs de la Blockchain ; l'application et ses données, elles, sont automatiquement livrées via le ledger ! »

En tant que bien commun, parce qu'il n'est pas payant, le protocole internet est sous-évalué. La Blockchain tend à ramener les forces de recherche et de développement sur le protocole, comme bien commun détenu par une oligarchie éclairée. Pour les premiers concepteurs de la Blockchain, le protocole, s'il est affiné, doit permettre d'améliorer l'analyse de cet outil qui est un lieu d'enregistrement de toutes les transactions. Selon Loubet et Epié (2015), on pourrait ainsi mieux mettre en regard pour une activité donnée la capture de valeur sur un temps relativement court (qui demeure le seul indicateur retenu aujourd'hui) et l'effective création de valeur de ladite activité si on lui soustrait tous les coûts directs et indirects (que l'on cache le plus souvent). Parmi les coûts cachés des modèles économiques flamboyants du net -- et nous y reviendrons -- se trouvent, entre autres, les dépenses énergétiques qui vont crescendo.

Pour bien comprendre cette rupture en matière de modèle d'innovation, Nicolas Loubet rappelle que les communautés de la Blockchain critiquent fréquemment les modèles économiques des géants de l'innovation dont les outils (comptables), certes très efficaces, favorisent des scénarii d'investissements très patrimoniaux ainsi que des tentations de fraudes vieilles comme le monde : « *Les modèles économiques des entreprises les plus innovantes de*

notre siècle sont éventuellement innovants mais ils s'appuient sur des règles comptables qui datent du XIII^{ème}-XIV^{ème} siècle dont l'esprit a été le plus souvent oublié...quitte à revenir à des stratégies très patrimoniales, voire à éviter de payer ses impôts pour préserver ses intérêts, alors même qu'il y a une demande sociale pour plus d'éthique de la part des consommateurs et des leaders de l'innovation...". La transparence par la Blockchain permettrait ainsi de mesurer si un modèle économique célébré est si innovant et si vertueux qu'il le prétend. Plus rigoureux qu'un bilan d'activité, le ledger pourrait fournir les preuves tangibles d'une approche vraiment holistique de l'innovation par les entreprises.

La rupture par le modèle professionnel et social

La communauté de la Blockchain se positionne par rapport à un premier groupe social – un groupe professionnel, celui des *geeks* de la galaxie internet qui développent de multiples projets, appartiennent à une communauté qui se prétend universelle mais demeure non ou peu engagée (concernée) par rapport à ce qui est développé sur le long terme sur un site ou une plateforme. Les acteurs de la Blockchain définissent aussi leur mission en contraste avec celle des membres des réseaux sociaux où il s'agit de valoriser son point de vue sur l'information, en général.

Pour un acteur de la Blockchain, s'affirment deux contributions qui participent directement au déploiement du réseau :

- Une contribution technique qui, par la validation d'algorithmes, permet de

valider les transactions et de les rendre visibles

- Une contribution politique qui est censée déterminer l'orientation de la Blockchain dans ses choix de développements (technologiques) et de projets

A travers cette double contribution technique et politique, les membres de la Blockchain cherchent à approfondir leur conscience voire leur sens de la responsabilité de ce qui se déploie technologiquement grâce à eux. En revendiquant une conscience à l'œuvre dans leur objet d'action professionnelle et en se démarquant des *geeks* et des simples membres de réseaux sociaux, ils cherchent à ancrer une légitimité et une autorité pour engager l'ensemble de la société à changer avec eux (Radu & Redien-Collot, 2008). Cette posture d'autorité affirme une rupture avec la posture propre à la génération internet qui s'interroge davantage sur la compétitivité que sur la soutenabilité des technologies. En même temps, elle marque un sur-engagement de l'individu par la technologie (toute relation est validée par un algorithme) et pour la technologie (tout individu sait ce qu'il a fait dans la Blockchain puisque cela est enregistré).

On peut nuancer à trois égards cette forme de rupture proclamée par la communauté de la Blockchain dans la relation sociale qui lie l'individu à la technologie.

Greg Revenu note que l'implication dans la Blockchain n'est pas une rupture avec le mode de fonctionnement de la génération internet mais un prolongement via la *tokenisation* : « La rémunération des membres

de la Blockchain pour leur expertise mise en jeu, en particulier, dans le minage et la résolution l'algorithme – suppose que plus tu contribues à la Blockchain, plus tu es rémunéré et plus le réseau et ses tokens gagnent en valeur ; c'est un prolongement et une concrétisation de la valeur des réseaux sociaux. D'où le pouvoir d'attractivité de la Blockchain qui rassemble ceux qui veulent donner plus de valeur et de sens à leurs interactions dans les réseaux... » La posture militante des mineurs est donc sujette à caution sur ce terrain-là. De plus, Greg Revenu rappelle que le minage s'industrialise. Il se désindividualise et permet de rassembler aux mains de quelques-uns le pouvoir de décision : « *L'univers du minage qui était celui de particuliers historiquement s'est fortement professionnalisé ! Il y a une course à la rapidité de résolution des algorithmes car il y a une montée du nombre de transactions et une gestion de flux toujours plus importante. Les mineurs s'équipent toujours plus pour répondre à cette demande et le travail s'organise ainsi :*

- les mineurs solitaires équipés de cartes/machines résolvant les algorithmes (vendues par des industriels) et à la recherche d'énergie bon marché
- les mineurs organisés en pool
- quelques grands industriels du minage tel que Bitfury en Occident (opérateur B to B qui tient 9% du marché du minage et Bitmain (Chine) (opérateur B to B to C qui couvre 10% du marché) »

Enfin, Nicolas Loubet souligne le caractère transitoire du développement technologique actuel de nos sociétés où il existe un décalage frappant entre leur potentiel

technologique et leurs pratiques de coordination et de décision : « *Les grands principes sur l'autonomie des organisations de la Blockchain demeurent théoriques. Et les expériences de prise de décision par consensus n'ont pas lieu (par exemple) chez Ethereum ; on est dans une technocratie ; seules quelques personnes très impliquées peuvent agir sur le protocole ; ceci donne lieu à des confrontations qui ont pimenté les deux années qui se sont écoulées.* »

La promesse d'une société de l'information distribuée

Comme le rappelle une note du Ministère de l'enseignement supérieur de 2011, la société de l'information distribuée devrait se caractériser par une puissante réflexivité qui amène l'univers du numérique à prendre en compte les effets qu'il produit nécessairement en matière de croisement d'informations, de production de connaissances et de comportements pour guider l'agenda du développement de ses processus et de ses outils. La réflexivité sur les effets du numérique est certes présente partout mais il semble difficile de lui fixer une gouvernance. A ce propos, Nicolas Loubet note : « *Le régime actuel de propriété limite l'accomplissement total d'une société de l'information distribuée ! [...] Il n'y a pas un cadastre d'information ! s'il y a une perte d'information de masse, il n'y a pas de recours vraiment légal ! [...] Google est, par exemple, souverain sur l'information. Il peut fermer un compte à discrétion.* »

Dans la Blockchain, le *ledger* constitue un livre comptable, a priori incorruptible, de l'information distribuée et archivée. Ce livre demeure un outil ; même si on

peut lui adjoindre de nombreux outils de croisement et d'analyse des données, idéalement, seule la communauté des usagers, et bien au-delà, la communauté humaine, demeure souveraine pour déterminer les modalités d'interprétation de l'information distribuée et surtout les modalités de dialogue pour engager une quelconque interprétation de ce qui est enregistré. L'absence de débat sur les modalités d'interprétation des données de l'univers numérique laisse planer un silence dont beaucoup profitent.

Afin de progresser vers la découverte de solutions acceptables pour tous via la Blockchain, Nicolas Loubet souligne qu'il faut que la communauté de la Blockchain s'interroge sur les gains et les pertes de souveraineté individuelle et collective *“d'une société où le système de calcul est incorruptible ?”* L'avènement de la société de l'information distribuée doit s'appuyer sur des outils très performants mais aussi sur des règles de coordination que la communauté du numérique n'est peut-être pas encore prête à formuler.

Il n'y a pas que la communauté humaine qui doit être prise en compte dans l'élaboration de la Blockchain. La nature et la dépense énergétique sont directement impactées. Nicolas Loubet rappelle qu'une question majeure doit constituer l'horizon de toute forme de recherche technologique : *“Jusqu'où doit-on allouer des moyens énergétiques supplémentaires pour progresser technologiquement ?”*. Bien entendu, l'avènement de la société de l'information distribuée via un *ledger* régulé et enrichi de mille et un logiciels et capteurs a un coût énergétique démesuré ! La question est d'autant plus pertinente lorsque le besoin énergétique pour le fonctionnement de la Blockchain croît de 25 % par mois, pour un niveau de consommation annuel aujourd'hui équivalent à celui du Danemark. Les projections sont encore plus effrayantes lorsqu'il apparaît qu'à l'horizon 2020 la Blockchain consommera annuellement plus d'énergie que l'ensemble du monde n'en consomme aujourd'hui !

Le procès actuel qui est fait à la Blockchain ne doit pas nous enfermer dans les trois

MINAGE ET MINEUR

Minage : utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés.

Mineur : personnes (particuliers ou sociétés) qui connectent sur le réseau une ou plusieurs machines équipées pour effectuer du minage. Chaque mineur est rémunéré au prorata de la puissance de calcul qu'il apporte au réseau.

Source : <https://Blockchainfrance.net/le-lexique-de-la-Blockchain/>

débats inévitables de la faisabilité, de la convenance ou de la soutenabilité qui doivent cependant être menés courageusement. Au sein même de la notion de progrès technologique, le débat sur la Blockchain rappelle qu'il n'y aura pas de progrès scientifique acceptable si la science ne fait pas de place au politique. Nicolas Loubet note : « [...] avec la Blockchain, la technologie remet le débat politique au centre des préoccupations économiques et financières et démontre indirectement que la critique politique est utile pour progresser technologiquement... Le bitcoin est une composition avec le monde économique/financier plus pertinente que la posture de protestation (Occupy Wallstreet) ; le bitcoin crée des situations sociales qui ne devaient pas se produire, des rencontres, des conversations qui n'arrivaient plus à se produire en société, par effet de cloisonnement. »

La société de l'information distribuée ne s'accomplira donc pas qu'au prix d'efforts démesurés pour élaborer des méthodologies

et des outils. Nicolas Loubet souligne que la Blockchain est précieuse par ce qu'elle réintroduit la valeur du débat au sein du monde des technologies. N'oublions pas, toutefois, que la technicité des préoccupations réglementaires peut, elle aussi, faire mourir ce débat. C'est peut-être pour cela que Greg Revenu invite ceux qui s'intéressent à la Blockchain à adopter une perception très fluide dans ce qu'elle produit en termes de ramifications financières. Dans le cas où surgissent des segmentations dans la chaîne de déploiement de la Blockchain (les forks), il ne faut pas lire une fragmentation de la valeur de la cryptomonnaie. C'est la Blockchain comme ressource qui présente une rupture qui prend un caractère presque organique : on parle de ressource mutante. Greg Revenu note : « [...] posséder un bitcoin et un bitcoin cash, ce n'est pas posséder deux types de devises ; c'est posséder deux graines, l'une originelle et l'autre une graine en mutation, chacune ouvrant sur des ressources et des compétences (de minage et plus) différentes. » A travers cette invite à ne pas voir dans les forks de la Blockchain la seule

FORK

Pour une « cryptomonnaie », un « fork » (un embranchement) est une modification des règles qui la régissent. Certaines transformations peuvent être mineures et rétrocompatibles – on parle alors de “soft fork” – ou plus importantes et sans compatibilité ascendante, c'est un “hard fork”. Un “soft fork” peut se contenter du soutien de la majorité de nœuds et mineurs pour devenir fonctionnel. Un “hard fork” en revanche nécessite un très large consensus, voire une unanimité.

Source : <https://bitcoin.fr/hard-fork-soft-fork/>

marque d'une volonté humaine, sanctionnée par la dépréciation d'une devise, mais à porter son attention sur ce qui mute, sur ce qui se déplie, il s'agit d'engager la communauté humaine à fonder un débat politique crucial ni sur un principe de précaution ni sur un principe de spéculation mais sur un principe soutenu d'observation.

Vers une géopolitique de la Blockchain

De nombreux travaux enseignent non seulement qu'aucun protocole technologique n'est neutre mais qu'ils « embarquent » souvent de nombreuses fonctions politiques. Si un exemple devait être donné, celui de la Blockchain serait l'un des plus parlants notamment en ce qui concerne la notion de souveraineté dont nous voudrions ici tenter de dresser quelques hypothèses de développement à la lumière de la très courte histoire de cette technologie encore balbutiante.

La souveraineté contre la Blockchain

Criminalité organisée

Dès les premiers temps du développement du *Bitcoin*, de nombreuses affaires criminelles retentissantes ont défrayé la

chronique. Du blanchiment d'argent, des arnaques en tout genre aux trafics illicites massifs, les monnaies virtuelles ont rapidement révélé leur potentiel antisocial et les risques en matière de délinquance. La fermeture en octobre 2013 de *Silk Road*, le « supermarché de la drogue¹⁹ » en ligne et l'arrestation le 6 novembre 2014 du créateur d'un *Silk Road 2.0* permise par une coopération internationale du FBI, d'Europol, d'Euojust et de cinq États reste l'affaire emblématique de l'usage criminel du *Bitcoin* et de la coopération judiciaire internationale qu'il a motivée.

Dès son apparition, le *Bitcoin* a donc alerté les services d'ordre du monde entier au regard de ses potentialités de nuisance et de contournement des circuits et des méthodes anciennes de criminalité organisée et de financement du terrorisme. À ce titre, le Groupe d'action financière²⁰ (GAFI) créé en 1989 lors du Sommet du G7 à Paris planche régulièrement sur les normes et mesures à déployer pour assainir le secteur des échanges financiers via Blockchain. Si cette technologie ouvre de nouveaux horizons à la grande délinquance, son *design* offre aussi de nouvelles armes aux forces de l'ordre. En effet, sa capacité à enregistrer de manière inviolable toutes les transactions des possesseurs de comptes, certes de manière anonyme, donne aux enquêteurs d'étonnantes perspectives : « si vous attrapez quelqu'un qui utilise un site comme *Silk Road*, vous avez découvert l'intégralité de son passé criminel. C'est

19. Mais aussi armes, faux papiers, logiciels de piratage, numéros de cartes bancaires, etc.

20. Dont l'objectif est « l'élaboration des normes et la promotion de l'efficace application de mesures législatives, réglementaires et opérationnelles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et les autres menaces liées pour l'intégrité du système financier international ».

<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

comme découvrir un livre de comptes”²¹. Ainsi, la potentialité d’usage illicite de la Blockchain au niveau global est importante, mais les organisations internationales judiciaires et la coopération pénale internationale semblent aussi obtenir des résultats. Ce nouvel équilibre des forces ne supprimera pas les transactions criminelles mais la Blockchain n’est pas l’arme absolue de la criminalité organisée. Il existe cependant un cas important pour lequel la vigilance doit être accentuée : le rôle naissant des technologies de Blockchain dans la traite humaine. Face aux graves lacunes en matière de preuve légale de l’identité des migrants, plusieurs autorités – dont récemment le Saint Siège²² – ont attiré l’attention de la communauté internationale sur ce fléau en développement.

Une souveraineté réaffirmée des régulateurs et des banques centrales

Au sujet de la portée géopolitique naissante de la Blockchain dont les institutions souveraines se saisissent, on pourra remarquer le rôle et les actions croissantes des régulateurs nationaux et internationaux. La position récente du Fonds Monétaire International de septembre 2017 lors du discours²³ de Christine Lagarde pour l’anniversaire de la Banque d’Angleterre est importante dans la mesure où le FMI presse officiellement les acteurs de l’économie mondiale à s’intéresser aux applications financières de la Blockchain.

La directrice générale du FMI, tout en soulignant les nombreux défauts de jeunesse des monnaies virtuelles (volatilité, risque, complexité), insiste sur leurs potentialités et la portée géopolitique notamment pour les pays dont l’économie est institutionnellement fragile. En prenant l’exemple de la dollarisation dans les régions isolées ou faiblement bancarisées, Christine Lagarde fait l’hypothèse qu’une monnaie virtuelle dont l’émission, rattachée à un panier de devises stables et dont la transparence est assurée par un algorithme qui peut être surveillé, pourrait « donner le change » aux monnaies existantes et à la politique monétaire. Le FMI invite donc les banquiers centraux à certes continuer d’appliquer une politique monétaire qui fonctionne pour les monnaies existantes mais à être aussi ouverts à de telles évolutions géo-économiques. Sur le plan des nouveaux moyens de paiement, la demande est croissante en raison de l’essor des services partagés et décentralisés à l’échelle globale. Une économie fondée sur les transactions internationales de pair à pair pour des paiements fréquents et de faible valeur doit disposer de nouveaux moyens de paiement “sans risque de règlement, sans délai d’autorisation, sans registre central, sans intermédiaires pour vérifier les comptes et les identités”. Dans un retour de souveraineté des banques centrales face à des monnaies virtuelles encore risquées et instables, une demande globale pourrait voir le jour auprès des banques centrales pour disposer de monnaies numériques fiables et ayant cours légal basées sur la technologie de la Blockchain.

21. <http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>

22. <https://www.coindesk.com/vatican-address-highlight-bitcoin-use-human-slave-trade/>

23. <http://www.imf.org/fr/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>

Dans cette dynamique de conquête de souveraineté par les banques centrales, le FMI leur prédit donc un mandat étoffé voire même un moindre des banques privées dans ce contexte paradoxale de recentralisation des activités bancaires. Les banques centrales seraient donc invitées à augmenter le nombre de contreparties à leurs opérations : « La Banque d'Angleterre montre déjà la voie en associant de grands opérateurs pour compte de tiers et des chambres de compensation centrales de contreparties ». Cette évolution liée à la Blockchain et aux monnaies virtuelles va donc accroître le nombre de sociétés susceptibles d'être réglementées, donnant aussi aux côtés des banques centrales un rôle prépondérant aux instances de régulation²⁴. Les frontières des entités surveillées par les régulateurs des marchés risquent de se brouiller et de se complexifier²⁵. Ce ne sera plus seulement aux entités financières qu'il faudra s'intéresser mais aux activités financières elles-mêmes et à la sécurité des algorithmes que les régulateurs devront être capables d'évaluer.

Ainsi, la technologie de la Blockchain devient peu à peu un sujet géo-économique et géopolitique d'envergure que ni les États, ni les banques centrales ou les organisations internationales ne peuvent ignorer. Cette prise en main par les instances de souveraineté n'est

pas sans paradoxe pour cette technologie fondée sur le mythe de la décentralisation.

La souveraineté par la Blockchain

Malgré l'omniprésence des questions de crypto-monnaie, comme principale réalisation opérationnelle, la Blockchain en tant que technologie recouvre une multitude d'applications possibles. Paradoxalement, bon nombre d'entre elles sont en mesure de conforter, voire de contribuer à édifier une souveraineté dans les cas où celle-ci se trouve dégradée soit en conséquence de conflits armés, soit dans le cas d'États faibles. Au sens large en effet, la Blockchain semble prometteuse dans le vaste domaine de la logistique de l'information, de sa distribution, de sa stabilité ou encore de son incorruptibilité.

Identité

La principale contribution à cette souveraineté réaffirmée touche aux vastes problèmes de la question de l'identité à l'ère numérique. Pour chacun, dans une situation courante ou pour des populations vulnérables comme les migrants dans un contexte dégradé²⁶, la

24. C'est par exemple déjà le cas en France avec la consultation publique sur le projet d'ordonnance « Blockchain » applicable à certains titres financiers.

https://www.tresor.economie.gouv.fr/Ressources/16101_consultation-publique-ordonnance-Blockchain-applicable-a-certains-titres-financiers

Nathalie Beaudemoulin et al., « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3 (Août 2017), p. 29-33.

25. La directrice du FMI prend ainsi l'exemple d'une entreprise de médias sociaux qui propose des services de paiement sans gestion active de son bilan.

26. L'Union européenne a voté en août 2017 des amendements budgétaires en ce sens. p.9.

<http://www.europarl.europa.eu/sides/getDoc.do?type=COMPART&reference=PE-609.538&format=PDF&language=EN&secondRef=01>

question de la résilience et de la robustesse des moyens numériques d'identité se pose à chaque instant. Le rattachement des données générées par un individu à son identité est un point central de l'économie du monde numérique. Ces données massives, essentiellement personnelles, servent pour l'instant de carburant à l'économie numérique sans que leur propriétaire ne soit en mesure de contrôler précisément leur diffusion, leur usage voire leur monnayage. Outre la possibilité via la technologie de la Blockchain de suppléer des infrastructures administratives défaillantes dans certains États, la Blockchain pourrait participer à l'élaboration d'une véritable auto-souveraineté sur ses propres données personnelles en vue d'équilibrer l'oligarchie des plateformes, les menaces sur la concurrence économique et le débat démocratique. Aujourd'hui, en effet, un pourcentage considérable²⁷ de la population mondiale ne possède aucun titre d'identité officiel et garanti par une autorité politique souveraine capable d'administrer un état civil fiable.

Articulée à cette question de la souveraineté politique individuelle et collective des registres d'état civil, celle de la fiscalité est tout aussi cruciale, notamment pour les pays dépourvus de système fiable d'identité qui ne peuvent lever l'impôt. Pour certaines études, la Blockchain permettrait

une fluidification de la logistique inhérente aux systèmes de taxation²⁸. Transparence, contrôle, sécurité, temps réel seraient autant d'avantages apportés par cette technologie. La réduction du coût de la levée de l'impôt, sa précision et son homogénéisation seraient aussi des arguments en vue d'une meilleure égalité devant l'impôt et d'un gain de productivité. Enfin, sur le plan des actes juridiques liés à l'identité et la fiscalité comme le cadastre ou les actes notariés, plusieurs expérimentations ont d'ores et déjà eu lieu²⁹.

Puissance de calcul et puissance géopolitique

Parmi les attributs classiques de la souveraineté et les moyens de la faire respecter, le concept de puissance (économique, politique, militaire, culturelle) est naturellement essentiel. Avec les nouveaux horizons que laisse entrevoir la Blockchain, un nouvel attribut de cette puissance semble devenir tout aussi déterminant que les plus anciens. En effet, la puissance de calcul mobilisable par un acteur de la scène internationale semble devenir un élément central de la souveraineté. L'effet de parc produit par la mobilisation décentralisée d'un très grand nombre de machines de minage des Bitcoin représente probablement la plus importante capacité de calcul jamais rassemblée³⁰. Face

27. Selon une étude de l'Unicef, 230 millions d'enfants de moins de 5 ans n'ont jamais été déclarés à leur État civil. Un enfant sur sept dans le monde ne possède pas de certificat de naissance.

<https://www.unicef.fr/article/230-millions-d-enfants-n-existent-pas-officiellement>

28. <https://www.pwc.co.uk/issues/futuretax/how-Blockchain-technology-could-improve-tax-system.html>

29. Au Ghana, <https://www.info-afrique.com/cadastre-ghana-Blockchain/>, ou encore au Honduras,

<https://www.usine-digitale.fr/article/un-titre-de-propriete-inscrit-sur-la-Blockchain-a-t-il-une-valeur-legale.N377408>

30. Il est avancé que le réseau de minage Bitcoin représente en puissance de calcul 10000 fois les top 500 des supercalculateurs centralisés. <http://jasondrowley.com/2015/12/04/the-bitcoin-network-is-11000x-faster-than-the-top-500-supercomputers-combined/>

aux enjeux liés à la cryptographie dans le domaine de l'information, peut-on envisager que cette puissance soit éventuellement assimilée à une arme mobilisable à des fins offensives, voire militaires ? À ce titre certaines puissances, comme la Chine³¹, concentrent déjà sur leur territoire, à défaut d'un contrôle direct, une bonne part de l'activité de minage. Mais en raison de la rentabilité de cette activité à mesure que le Bitcoin prend de la valeur, de nouvelles zones géographiques entrent en compétition. Le risque de voir se concentrer sur un seul territoire souverain plus des 50 % des capacités de minage suffisantes pour falsifier le processus n'est pas exclu. L'introduction de monnaies numériques souveraines et régulées³², qui semble envisagée à terme par le FMI³³, nécessitera pour les États la mise en place de lourdes infrastructures, même décentralisées, de calcul. Cette puissance de calcul peut servir à de nombreuses applications comme la modélisation scientifique, le renseignement ou encore la cybersécurité défensive et/ou offensive. Cette nouvelle dimension de la puissance peut aussi perturber les rapports antérieurs, des nations de moindre importance pouvant choisir d'investir cette forme de souveraineté par la puissance de calcul, tributaire cependant des capacités de production électrique³⁴. Au final, c'est

toute l'industrie du hardware (course vers la puissance des microprocesseurs et de leur bilan énergétique) et du software qui va se trouver impactée par cette hypothèse géostratégique du rôle de la puissance de calcul dans les rapports de puissance.

Une géopolitique de la confiance distribuée ?

Sans naïveté excessive et sans minimiser les risques et les lourdes incertitudes qui pèsent sur la Blockchain, des perspectives positives peuvent être envisagées, notamment en ce qui concerne une forme de « géopolitique de la confiance », là où les incertitudes et les aléas pèsent sur les capacités de développement de telle ou telle région du monde.

Dans la lignée de notre propos sur les solutions possibles que la Blockchain pourrait apporter à la résolution des questions liées à la certification de l'identité au sens large, on pourrait supposer que de vastes champs de fragilités des États faibles ou faillis trouvent un début de réponse. En premier lieu, la question des réfugiés³⁵ et des déplacés³⁶ voit déjà se mettre en place des initiatives à base de technologie Blockchain pour sécuriser et certifier l'identité des

31. Sans pouvoir entrer ici dans le détail, cette puissance de calcul est aussi corrélée au coût de l'électricité. Plus largement, le minage reste une activité énormément énergivore. Ce qui pose à terme une limite environnementale à cette activité au final « polluante ».

32. Regulated and Sovereign Backed Cryptocurrencies - RSBC

33. Discours de la Directrice générale du FMI, Christine Lagarde en septembre 2017

34. Certains États au climat froid étant cependant avantagés en matière de capacité de refroidissement des centres de calcul. Capacité qui constitue une part importante de la facture énergétique.

35. Les Nations Unies ont lancé une expérimentation en Jordanie de distribution de coupons d'aide basés sur une Blockchain Ethereum pour 100 000 réfugiés.

<https://www.wfp.org/news/news-release/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu>

36. <https://www.coindesk.com/eu-politician-pushes-parliament-test-Blockchain-identity-refugees/>

individus et, en conséquence, sécuriser la distribution et le soutien humanitaire de première nécessité. Plus largement, la sécurisation et l'optimisation de l'aide humanitaire pourrait être améliorée par les applications de "Blockchain Aid" qui se multiplient, notamment à propos des risques de détournement.

Au-delà de l'aide d'urgence, c'est tout le système de bancarisation, de micro paiements et de lutte contre la corruption qui pourrait se voir transformé dans les pays à faible revenu et plus largement dans les échanges financiers. Nous retrouvons ici comme application large et positive de la Blockchain un moyen d'accélérer et de sécuriser de nouveaux moyens de paiement pour les zones sous-bancarisées dont les lacunes des infrastructures financières pèsent sur les capacités de développement. L'essor récent des portefeuilles virtuels adossés aux réseaux de téléphonie mobile augure de besoins massifs et de comportements innovants dans ce domaine³⁷. La sécurisation de la logistique informationnelle de ces systèmes pourrait sans doute être supportée par des technologies inspirées par la Blockchain³⁸.

Les processus électoraux pourraient aussi bénéficier des avantages de la Blockchain dans la mesure où les résultats pourraient être, au moins théoriquement, auditables par tous. La fluidité et la garantie permises par la Blockchain permettraient, outre la transparence et la confiance dans le processus, de minimiser les coûts d'un scrutin et de simplifier le système de procurement et de dépouillement. Plus largement encore, et alors que les expérimentations se multiplient au sein même des autorités de régulation des marchés³⁹, les capacités de la technologie Blockchain semblent réelles dans le domaine de la tenue de registres au sens large. Politiquement, et Max Weber dans ses réflexions sur la bureaucratie l'a souligné, tenir un registre est loin d'être neutre et constitue même une fonction fondamentale de tout acte de gouvernement. En ce sens, la Blockchain comme technologie de distribution de confiance dans la tenue de registres, c'est-à-dire l'organisation et la certification de données liées notamment à l'identité, est sans doute capable de renouveler de nombreux pans de la gouvernance.

37. Dans les pays en développement, seuls 41% des adultes auraient un compte bancaire contre 89% dans les pays occidentaux et 7% une carte bancaire. Source « Quel est l'état de la bancarisation en Afrique ? », <http://terangaweb.com/quel-est-letat-de-la-bancarisation-en-afrique/>

38. BOURJII Saïd, « Innovations technologiques et offre de services financiers en appui au Développement. Note de Conjoncture et de problématique », *Techniques Financières et Développement*, 2016/3 (n° 124), p. 7-26. URL : <https://www.cairn.info/revue-techniques-financieres-et-developpement-2016-3-page-7.html>

39. Nathalie Beaudemoulin et al., « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3 (Août 2017), p. 33.

Conclusion

Au terme de ce texte qui avait pour objectif d'appréhender le phénomène émergent de la Blockchain autrement que par la technicité ou la faisabilité, nous voudrions souligner à quel point cette technologie correspond à ce que Michel Foucault a défini comme une « hétérotopie de crise »⁴⁰. Hétérotopie, dans la mesure où le discours fondateur de la Blockchain et de sa première application, le Bitcoin, définit le code informatique comme le lieu de la réalisation d'une utopie : celle de résoudre techniquement la question de la confiance dans les rapports humains. Hétérotopie de crise, car il faut toujours se souvenir que la Blockchain a été pensée et *désignée* comme une réponse à la crise financière de 2007-2008 au moment où le système économique mondial aurait pu s'effondrer.

En creux, le déploiement de la Blockchain au-delà des cercles confidentiels de hackers, souligne les fragilités théoriques du système économique post-capitaliste. Les experts, y compris ceux des plus puissantes instances régulatrices, sont pris de vertige et versent souvent dans la confusion et la contradiction. Ne serait-ce que pour déterminer si oui ou non le Bitcoin est une monnaie ou un actif. Alors que nous avons montré que le mimétisme affiché du Bitcoin envers cette réalité anthropologique ne parvient clairement pas à le confondre avec une monnaie.

Par ailleurs, l'idéalisme distributif de la Blockchain qui prétend pouvoir réduire les mécanismes de confiance humaine à un protocole informatique peine à dissimuler une technocratie hyperconcentrée entre les mains d'une élite de programmeurs, pour peu qu'on la compare aux principales théories du contrat social et que l'on examine ses premières crises révélatrices.

Mais, nous avons aussi montré que la Blockchain et son pouvoir subversif sont capables d'interroger de nombreux pans de la sociabilité humaine en surface (échanges marchands, identité, fiscalité) et en profondeur (confiance, contrat social) en réintroduisant brutalement du politique là où les idéologies technicistes cherchent justement à dépolitiser les problèmes.

En raison de son caractère balbutiant et de l'amplitude de ses effets possibles sur la définition et la réalisation du Bien commun, ce texte avait surtout comme ambition d'inviter à esquisser les grandes lignes d'un programme de recherche transdisciplinaire, urgent et indispensable.

L'une des pistes possibles serait une étude sociologique approfondie des communautés d'acteurs qui émergent autour de la Blockchain (mineurs, développeurs, investisseurs...). Une autre réside dans l'étude de l'impact des externalités de la

40. Michel Foucault, *Le corps utopique ; suivi de Les hétérotopies*, Paris, Éditions Lignes, 2009, p. 61.

Blockchain, notamment sa dimension énergivore⁴¹ et ses impacts géopolitiques en matière d'accès aux ressources énergétiques. Enfin, l'entrée dans les arènes de débat public des controverses actuelles

et futures produites par la Blockchain se dessine comme un autre axe fructueux de travaux d'enquête et de collaborations interdisciplinaires.

41. En décembre 2017, le minage du Bitcoin représentait 0,16% de la consommation mondiale d'électricité avec près de 35 TWh. Au rythme actuel de croissance, près de 30% par mois, en raison des spéculations sur le Bitcoin, toute l'électricité mondiale de suffirait pas en février 2020. Le Bitcoin consomme plus d'électricité que 159 États individuellement. <https://powercompare.co.uk/bitcoin/>

Références

- AGLIETTA Michel et ORLÉAN André (dir.) (1998), *La monnaie souveraine*, Paris, Odile Jacob, 1998.
- BEAUDEMOULIN Nathalie et al., (2017) « Les enjeux de la Blockchain pour la Banque de France et l’Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3.
- BOURJIJ Saïd (2016), « Innovations technologiques et offre de services financiers en appui au Développement. Note de Conjoncture et de problématique », *Techniques Financières et Développement*, 2016/3 (n° 124).
- CAMAGNI, R. (2017), Technological change, uncertainty and innovation systems : Toward a dynamic theory of economic space, in R. Capello (Ed.), *Seminal Studies in Regional and Urban Economics*, pp.65-97.
- DE FILIPPI, P. & LOVELUCK, B. (2016). The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. *Internet Policy Review*, 5(3).
- FRIEDMANN, Milton (1970), *The Counter-Revolution in Monetary Theory*, 1970.
- HAYEK, Friedrich (1976), *The Denationalization of Money*, 1976.
- KOCHERLAKOTA Narayana R. 1998), « Money Is Memory », *Journal of economic theory* 81, 232-251 (1998).
- LEMIEUX, C. (2012), Peut-on ne pas être constructiviste ?, *Politix*, 100(4) : 169-187
- MISCIONE Gianluca and KAVANAGH Donncha (2015), Bitcoin and the Blockchain: “A Coup D’État through Digital Heterotopia?”, *Humanistic Management Network*, Research Paper Series No. 23/15. <https://ssrn.com/abstract=2624922> or <http://dx.doi.org/10.2139/ssrn.2624922>
- LOUBET, N. & EPIÉ, C. (2015), *Blockchain and Beyond*, <https://blockchainfrance.files.wordpress.com/2015/12/cellabz-Blockchain-beyond.pdf>
- MINISTÈRE DE L’ÉDUCATION NATIONALE, DE L’ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE (2011), *Stratégie de recherche pour le numérique*, https://cache.media.enseignementsup-recherche.gouv.fr/file/Strategie_Recherche/28/1/Rapport_atelier_7_314281.pdf
- MAUSS Marcel (1924), « Essai sur le don : Forme et raison de l’échange dans les sociétés archaïques », *L’Année sociologique*, 1923-24.
- RADU, M. & REDIEN-COLLOT, R. (2008). The Social Representation of Entrepreneurs in the French Press: Desirable and Feasible Models? *International Small Business Journal*, 26 (3), 259-298.

REIJERS, O'BROLCHAIN et HAYNES 2016), « Governance in Blockchain Technologies & Social Contract Theories », *Ledger*, Vol 1.

SCOTT Brett (2016), *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance ?* févr. 2016, United Nations Research Institute for Social Development.

THÉRET Bruno (dir.) (2007), *La monnaie dévoilée par ses crises*, Paris, Éditions de l'EHESS, 2 volumes, 2007.

WENNERLIND Carl (2001), "Money Talks, but What is it Saying? The Semiotics of Money and Social Control." *Journal of Economic Issues*. September. 2001. Vol. 35. No. 3: 557-74.

YOUNG Sherman (1998), «Of Cyber Spaces: The Internet & Heterotopias.» *M/C: A Journal of Media and Culture* 1.4, <http://www.uq.edu.au/mc/9811/hetero.php>

