INSTITUT
POUR QUE L'AVENIR AIT BESOIN DE NOUS
SAPIENS

Bitcoin, totem & tabou

Que présage l'essor des cryptomonnaies ?

Rapport — Février 2018

1. Table des matières

Les auteurs 3

A propos de Sapiens

Les 8 points clefs 5

Synthèse 8

La révolution de la monnaie
Une cryptomonnaie qui dérange
Des conséquences vertigineuses
Accompagner l'innovation

Introduction 16

Remerciements

1. Une technologie idéaliste, révolutionnaire et évolutive 19

1.1 Les idéaux fondateurs 19

1.1.1 Les germes philosophiques
1.1.2 Satoshi Nakamoto

1.2 La mise en œuvre technique 23

1.2.1 Internet, machine à copier
1.2.2 Principales caractéristiques
1.2.3 Evolution et gouvernance

2. Un sous-jacent bien réel 33

2.1 Le bitcoin repose sur la technologie et la liberté 33

2.1.1 Bulle ou antifragilité ?
2.1.2 La sécurité du réseau
2.1.3 La question énergétique
2.1.4 L'écosystème industriel et la communauté

2.2 Les monnaies étatiques ne reposent plus que sur l'autorité 48

2.2.1 Depuis 1971, les monnaies nationales n'ont pas de réel sous-jacent

2.2.2 Depuis 2008, les politiques monétaires créent de nouveaux risques
2.2.3 Quelle pérennité pour les monnaies nationales ?

3. Une monnaie en devenir 58
3.1 De réserve de valeur à moyen d'échange 58
3.1.1 Réserve de valeur et spéculation
3.1.2 Limite des 21 millions et caractère déflationniste
3.2 Les conséquences insoupçonnées de la liberté monétaire 65
3.2.1 Vers un nouveau paradigme monétaire ?
3.2.2 Une monnaie dénationalisée
3.2.3 Quel avenir pour les politiques monétaires et le secteur bancaire ?
3.2.4 La protection des individus
3.2.5 Quel avenir pour l'État-Providence ?

4. Une nouvelle ère de décentralisation et d'autonomie 79
4.1 La multiplication des blockchains 79
4.2 Le phénomène des ICO 83
4.3 Vers une décentralisation généralisée ? 85
4.4 Un défi lancé au droit 87
4.4.1 Quelle régulation ? Quelle réglementation ?
4.4.2 L'exemple des ICO

5. Conclusion 94

6. Annexes 96
6.1 The Crypto Anarchist Manifesto (Timothy May, 1988) 96
6.2 A Cypherpunk's Manifesto (Eric Hughes, 1993) 98
6.3 Extrait du white paper Bitcoin (Satoshi Nakamoto, 2008) 100
6.4 Les erreurs de l'approche keynésienne 102
6.5 La théorie autrichienne des cycles économiques 104

Les auteurs

Yorick de Mombynes

Chercheur associé à l'Institut Sapiens

Né en 1975, diplômé de l'École Supérieure de Commerce de Paris (ESCP) et de l'Institut d'Études Politiques de Paris (IEP), titulaire d'une licence de philosophie de l'Université Sorbonne-Paris IV, ancien élève de l'École Nationale d'Administration (ENA), il a été conseiller technique du premier ministre François Fillon et a travaillé chez Total. Il a enseigné l'économie et la philosophie politique à l'IEP de Paris. Il est conseiller référendaire à la Cour des comptes.

Gonzague Grandval

Professionnel du paiement électronique et entrepreneur

Il a participé à l'éclosion de l'écosystème Bitcoin depuis 2011 en France, et intervient dans de nombreuses initiatives Blockchain en Europe. Il est associé chez Pikcio AG et co-fondateur de Woorton et de Paymium.

A propos de Sapiens

L'Institut Sapiens est la première « think tech » française. Organisme indépendant à but non lucratif, sa vocation est de peser sur le débat économique et social français contemporain par la diffusion de ses idées et d'innover **par ses méthodes, son ancrage territorial et la diversité des intervenants qu'il mobilise, afin de mieux penser les enjeux vertigineux du siècle.**

Impulsé par Olivier Babeau, Laurent Alexandre et Dominique Calmels, en partenariat avec la chaire Capital Humain de l'université de Bordeaux, Sapiens a vocation à définir le rôle de l'humain dans une société bouleversée par le numérique. Son axe principal de travail est l'étude et la promotion des nouvelles formes d'écosystèmes favorables au développement économique et au bien-être social.

Sapiens fédère un large réseau d'experts issus de tous horizons, universitaires, avocats, chefs d'entreprise, entrepreneurs, hauts fonctionnaires, autour d'adhérents intéressés par le débat touchant aux grands enjeux actuels.

Plus d'informations sur http://institutsapiens.fr

INSTITUT SAPIENS
POUR QUE L'AVENIR AIT BESOIN DE NOUS

Les 8 points clefs

1 Le bitcoin et les cryptomonnaies s'apprêtent à nous faire changer de monde. Pourtant, nous continuons à nous méprendre sur ce sujet, entre totem et tabou. Comme avec le web dans les années 1990, la France, alors qu'elle a tous les atouts pour devenir un leader mondial de cette révolution économique et culturelle, risque de se laisser distancer.

2 La blockchain au sens strict est une technologie relativement ancienne, inventée avant le bitcoin. L'expression "technologie blokchain" recouvre des réalités disparates qui n'ont pas toujours grand-chose en commun. Le protocole Bitcoin, lui, est révolutionnaire : il permet, pour la première fois, de faire fonctionner un réseau où sont possibles des transferts de valeur de manière décentralisée, sans validation par un tiers de confiance et sans risque de censure.

3 La monnaie est donc la première "*killer app*" de ce que l'on appelle la "technologie blockchain", tout en étant également un rouage essentiel de son fonctionnement. Nous assistons à une accélération foudroyante du progrès technologique dans le domaine monétaire. Pour la première fois dans l'histoire de l'humanité, une monnaie a comme sous-jacent un réseau ultra-sécurisé : cela signifie l'intégration du système de paiement et de la monnaie, deux éléments qui étaient toujours restés distincts. La monnaie est mise en réseau, "*plateformisée*". Elle devient décentralisée et programmable. Elle

est transformée par la technologie de la même manière que les processus de production et de diffusion de l'information ont été totalement transformés par Internet. D'importants efforts de recherche sont en cours pour rendre possible, sur la blockchain Bitcoin, une forme de monnaie en "*streaming*", pour un coût négligeable et avec un anonymat renforcé. Bitoin sera une composante à part entière de la nouvelle révolution industrielle en germe avec l'intelligence artificielle, les objets connectés et les robots : pour s'échanger de la valeur, des données, des titres juridiques et des ordres, ces entités utiliseront en priorité les cryptomonnaies et les blockchains.

4 **Avec Bitcoin, la monnaie échappe, pour la première fois depuis des siècles, à l'État et aux banques.** Il s'agit d'un fait historique majeur. Les inquiétudes en matière de blanchiment, de financement d'activités illégales, de fraude fiscale, de spéculation, de volatilité et de coût environnemental sont certes légitimes. Mais Bitcoin et les cryptomonnaies sont des entités "*antifragiles*" au sens de Nassim Nicolas Taleb : l'adversité est un contexte propice à leur développement. Pour comprendre son origine et son évolution actuelle, il faut se souvenir que Bitcoin est l'aboutissement de plusieurs décennies d'expérimentations techniques et de réflexions philosophiques et économiques, bien avant la crise de 2008.

5 **Bitcoin est l'héritier des "*cypherpunks*" des années 1990** qui ont compris que l'essor d'internet, tout en libérant l'individu, allait aussi le soumettre à un risque de surveillance extrêmement préoccupant.

6 **L'accumulation de désastres monétaires tout au long du XXème siècle suggère que,** contrairement à l'idée reçue, la monnaie est une chose trop importante pour être laissée à l'État. Comme le montre l'école de pensée autrichienne, les cycles économiques sont essentiellement créés par les manipulations monétaires des autorités publiques, avec des conséquences sociales et économiques catastrophiques. Depuis 1971, par ailleurs, les monnaies étatiques n'ont plus aucun autre sous-jacent que la coercition qui rend leur usage obligatoire. Et, depuis 2008, les politiques monétaires ultra-expansionnistes créent de nouveaux risques et font peser des doutes croissants

sur la capacité des monnaies étatiques à jouer leur rôle de monnaie saine.

Dès 1984, Hayek déclarait : *"je ne crois pas au retour d'une monnaie saine tant que nous n'aurons pas retiré la monnaie des mains de l'État ; nous ne pouvons pas le faire violemment ; tout ce que nous pouvons faire, c'est, par quelque moyen indirect et rusé, introduire quelque chose qu'il ne peut pas stopper ".* C'est chose faite avec Bitcoin.

7 **Le fait que la monnaie devienne programmable ouvre, par ailleurs, une nouvelle ère** de décentralisation des institutions et d'autonomie pour les individus. De nouvelles blockchains comme Ethereum ont le potentiel de contribuer à révolutionner pratiquement tous les secteurs d'activité. De nouvelles formes d'organisation vont émerger, sans autorité centrale et sans assise nationale. Il est urgent de réfléchir aux conséquences juridiques, politiques et culturelles de cette évolution.

8 **Une compétition mondiale intense est engagée dans ce domaine.** Identifier les risques de la technologie est bien sûr nécessaire mais ne doit pas conduire à étouffer l'innovation et la création, ce qui priverait la France des bénéfices d'une des révolutions économiques et culturelles majeures de notre époque. Les régulateurs devraient donc adopter une attitude raisonnable face aux cryptomonnaies et aux blockchains. Il convient de maintenir aussi faible que possible le poids de la fiscalité et des contraintes réglementaires pesant sur les entrepreneurs, les investisseurs, les créateurs et les consommateurs. D'autres pays ont déjà compris cette nécessité.

Synthèse

En 2005, le controversé Ray Kurzweil publiait un livre qui allait poser les bases de pratiquement tout le débat mondial sur les nouvelles technologies jusqu'à aujourd'hui, notamment en matière d'intelligence artificielle : *The Singularity is near*. Ce qu'il appelle "*singularité*" est ce moment à venir où le progrès technologique exponentiel deviendra si rapide que nos esprits d'aujourd'hui sont incapables d'en penser toutes les conséquences.

Aujourd'hui, une forme de singularité se rapproche aussi en matière monétaire. **Le bitcoin et les cryptomonnaies s'apprêtent à nous faire changer de monde, avec des conséquences particulièrement difficiles à imaginer.**

Une prise de conscience est pourtant urgente. Face au web dans les années 1990, la France a connu une forme de "*marginalisation paradoxale*" : alors qu'elle avait tous les atouts pour devenir un leader de cette révolution économique et culturelle, elle s'est laissée distancer, évincer de la compétition mondiale. Elle et l'Europe ont ensuite reproduit le même schéma avec l'intelligence artificielle. Aujourd'hui, notre pays risque de subir le même sort avec Bitcoin et les technologies qui en découlent.

La révolution de la monnaie

En nous focalisant sur la fameuse "technologie blockchain", nouveau totem moderne, et sur les travers des cryptomonnaies, jusqu'à transformer Bitcoin en quasi-tabou, nous commettons deux erreurs préoccupantes.

D'une part, nous oublions que **la blockchain au sens strict est une technologie relativement ancienne**, inventée bien avant le bitcoin. Le protocole Bitcoin (avec une majuscule, pour le distinguer du jeton numérique et monétaire "*bitcoin*"), lui, est révolutionnaire : par une intégration extraordinairement ingénieuse de plusieurs technologies (blockchain, cryptographie asymétrique, réseau pair-à-pair, minage par la preuve de travail), il permet, pour la première fois, de faire fonctionner un réseau où sont possibles des transferts de valeur de manière décentralisée, sans validation par un tiers de confiance et sans risque de censure.

Le fait que le protocole soit open source permet de le copier, d'en modifier certains paramètres et de créer de nouveaux réseaux, de nouvelles blockchains, de nouveaux jetons numériques et donc de nouvelles cryptomonnaies. Mais, l'expression "technologie blokchain" recouvre en fin de compte des réalités disparates qui n'ont parfois plus grand chose en commun : les blockchains "mères" comme Bitcoin et Ehtereum, les "altcoins" (soit émis en totalité dans le cadre d'une *initial coin offering*, soit "minés" dans le cadre d'un "copier-coller" d'un protocole original), et les blockchains sans token (elles peuvent représenter une innovation prometteuse au sein de certaines organisations mais sont très éloignées du modèle décentralisé de Bitcoin).

Illustration : Valentina Picozzi, http://www.satoshigallery.com/

D'autre part, nous négligeons le fait que **la monnaie est la première "** killer app **" de ce que l'on appelle vaguement la " technologie blockchain ", tout en étant également un rouage essentiel de son fonctionnement**. La monnaie est une institution vieille comme l'humanité. Depuis des millénaires, elle se transforme, notamment sous l'effet du progrès technique, mais avec un rythme toujours très lent : le passage des coquillages et autres anciens intermédiaires d'échanges aux métaux précieux, puis à la monnaie scripturale et aux billets de banque, et enfin au numérique et à la carte bancaire s'est effectué sur des siècles, avec une accélération notable dans la seconde moitié du 20ème siècle. Avec les cryptomonnaies, nous assistons à une accélération foudroyante de ce rythme En quelques années, **la notion même de monnaie a pratiquement volé en éclats**. La monnaie est mise en réseau, " plateformisée ", elle devient décentralisée et programmable. Elle est transformée par la technologie de la même manière que l'information a été transformée par Internet.

Nous nous gaussons aujourd'hui des piètres performances techniques du bitcoin, comme nous ricanions hier face aux balbutiements du web. Mais **nous oublions que, dans ce domaine aussi, le progrès est exponentiel.** Nous ignorons que sont actuellement posés, loin du regard des médias et du grand public, les jalons techniques qui vont bientôt rendre possibles, sur ces nouveaux réseaux, d'énormes quantités de transactions, parfois pour des montants très réduits et sur d'infimes périodes de temps (une véritable monnaie en " streaming ", donnant tout son sens à l'expression " *cash flow* "), le tout pour un coût négligeable pour l'utilisateur et avec une sécurité et un anonymat renforcés. Ces caractéristiques constitueront l'un des aspects de la nouvelle révolution industrielle en germe avec l'intelligence artificielle, les objets connectés et les robots : pour s'échanger de la valeur, des données, des titres juridiques et des ordres, ces entités utiliseront en priorité les cryptomonnaies et les blockchains.

La monnaie est une institution vieille comme l'humanité. Depuis des millénaires, elle se transforme (...)

Les questions posées au bitcoin en matière de blanchiment, de financement d'activités illégales, de fraude fiscale, de spéculation, de volatilité et de coût environnemental sont parfaitement légitimes. Il ne s'agit pas de les esquiver ou d'en contester la pertinence. En même temps, il est intéressant de se demander pourquoi Bitcoin et les cryptomonnaies continuent de se développer malgré leurs innombrables lacunes sans cesse dénoncées, et alors que l'on annonce régulièrement leur fin prochaine depuis le premier jour de leur existence. La réalité est que, **contrairement aux institutions bancaires et monétaires traditionnelles, ce sont des entités "antifragiles" au sens de Nassim Nicolas Taleb** : l'adversité est un contexte propice à leur développement. Surtout, si des questions similaires sont adressées aux institutions en charge des systèmes monétaires et financiers traditionnels, elles ne le sont sans doute pas de manière aussi concentrée, virulente et partisane. Ces institutions sont à la fois étroitement encadrées par le droit et relativement moins exposées à la critique de l'opinion publique.

Une cryptomonnaie qui dérange

Pourquoi Bitcoin dérange-t-il autant ? Pourquoi est-il systématiquement soupçonné de tous les maux, condamné d'avance ? Pourquoi n'est-il pas possible de l'évoquer de manière apaisée, sans suspicion a priori ? Pourquoi cette présomption instantanée de culpabilité, alors que, comme toute technologie nouvelle, il peut être bien ou mal utilisé ?

Bien sûr, toute nouveauté suscite des réactions émotives de crainte et de méfiance. Mais, au-delà, si les cryptomonnaies dérangent, c'est fondamentalement parce que, depuis des millénaires, la monnaie est associée au pouvoir. A l'origine création sociale spontanée, la monnaie a progressivement été accaparée par le pouvoir politique, jusqu'à devenir un moyen de pilotage de l'économie et de contrôle des citoyens. **Avec Bitcoin, la monnaie échappe à l'État et aux banques. Il s'agit d'un fait historique majeur**. Pour le comprendre, il faut remonter aux origines de Bitcoin.

Certes, la crise de 2008 a confirmé l'intérêt pour une nouvelle forme de monnaie plus libre. Mais en ne retenant que cet aspect, on oublierait que l'apparition de Bitcoin est l'aboutissement

de plusieurs décennies d'expérimentations techniques et de réflexions philosophiques et économiques.

(...) si les cryptomonnaies dérangent, c'est fondamentalement parce que, depuis des millénaires, la monnaie est associée au pouvoir.

Du côté technique : la prouesse de Satoshi Nakamoto est d'organiser un agencement d'incitations rendant immensément plus rentable de contribuer au système plutôt que de le pirater : si des plateformes d'échange ont pu être hackées, le réseau Bitcoin ne l'a jamais été. A l'inverse des systèmes traditionnels, le coût de la validation des transactions est négligeable, tandis que celui de l'inscription des transactions validées dans le registre est phénoménal. **Pour la première fois dans l'histoire de l'humanité, une monnaie a comme sous-jacent un réseau ultra-sécurisé** (complété par un écosystème industriel et une communauté humaine) : cela permet l'intégration du système de paiement et de la monnaie, deux éléments qui étaient toujours restés distincts depuis la création de la monnaie.

Du côté philosophique : **les "cypherpunks" ont compris dès les années 1990 que l'essor d'internet, tout en offrant un instrument de libération historique à l'individu, allait aussi le soumettre à un risque de surveillance accru**. Ils ont aussi compris que, grâce à l'alliance des États et des banques, la surveillance financière rendue possible par la numérisation des paiements allait devenir l'un des risques les plus insidieux et les plus dangereux pour les libertés individuelles. Les années 2010 leur ont largement donné raison.

Enfin, sur le volet économique, malgré tous les efforts des institutions publiques pour cacher au grand public la réalité du fonctionnement des systèmes monétaires contemporaines (qui a appris à l'école comment est créée la monnaie ?), l'accumulation de désastres monétaires tout au long du XXème siècle (hyperinflation, augmentation du rythme et de la gravité des crises monétaires) a convaincu un nombre croissant d'économistes que, contrairement à l'idée reçue, **la monnaie est une chose trop importante pour être laissée à l'État**.

Comme l'ont démontré Mises et Hayek, **les cycles économiques sont essentiellement créés par les manipulations monétaires des autorités publiques**, avec des conséquences sociales et économiques catastrophiques. Depuis 1971, les monnaies étatiques ne reposent plus, comme on se plaît souvent à le croire, sur les

fondamentaux des économies et des États, mais tout simplement sur la seule coercition qui rend leur usage obligatoire. Depuis 2008, le roi est nu : d'une part, le grand public comprend que, grâce au privilège économique immense de la création monétaire par le crédit, les banques sont assurées du soutien ultime des États qui leur permet d'agir de manière excessivement risquée sans toujours en subir les conséquences ; d'autre part, les politiques monétaires ultra-expansionnistes créent de nouveaux risques et font peser des doutes croissants sur la capacité des monnaies étatiques à conserver la valeur et donc à jouer leur rôle de monnaie saine.

Dès 1984, **Hayek déclarait :** *"je ne crois pas au retour d'une monnaie saine tant que nous n'aurons pas retiré la monnaie des mains de l'État ; nous ne pouvons pas le faire violemment ; tout ce que nous pouvons faire, c'est, par quelque moyen indirect et rusé, introduire quelque chose qu'il ne peut pas stopper".* C'est chose faite avec Bitcoin.

Des conséquences vertigineuses

Cette rupture entraîne une série de conséquences potentiellement vertigineuses.

Premièrement, les progrès techniques en cours font que **les cryptomonnaies vont devenir plus faciles à utiliser, que leur nombre va probablement se multiplier dans des proportions aujourd'hui inimaginables, et qu'elles seront de plus en plus difficiles à contrôler par les États**. Leur qualité en tant que monnaie va augmenter grâce au fait qu'elles sont en concurrence les unes par rapport aux autres. C'est la fin du monopole de la production monétaire (qui empêchait cette concurrence au profit des utilisateurs), comme préconisé par Hayek en 1976 dans son ouvrage *The Denationalization of money*. Même avec le maintien du cours légal, l'essor des cryptomonnaies va créer un défi inédit pour les autorités. Des réglementations trop contraignantes ne feront qu'éloigner le capital et alimenter le marché noir, tout en diminuant la demande (et donc la valeur) de monnaies nationales. Avec une telle perspective, on peut se demander quel est l'avenir des politiques monétaires conduites par les États.

Deuxièmement, avec la décentralisation permise par les cryptomonnaies, on assiste à une éclosion historique d'expérimentations, de prises de risques et d'innovations technologiques dans un domaine qui en était jusqu'à présent largement dépourvu. Le caractère centralisé des systèmes monétaires et financiers, couplé à l'absence de concurrence, freinait le progrès technologique en matière de monnaie et de banque. C'est l'une des explications de certains aspects ridiculement archaïques du secteur bancaire quand on le compare à certains secteurs qui ont été révolutionnés par la transformation numérique. **Avec toutes les technologies issues de Bitcoin, la monnaie devient programmable, ce qui ouvre une nouvelle ère de décentralisation des institutions et d'autonomie pour les individus**.

C'est ainsi que de nouvelles blockchains comme Ethereum ont le potentiel de contribuer à transformer pratiquement tous les secteurs d'activité, en commençant par la banque, l'assurance et les objets connectés. Le financement de l'innovation est déjà révolutionné par les *initial coins offerings* (ICO). Ces opérations traversent actuellement une période d'excès et de frénésie spéculative, mais elles constituent une innovation objectivement intéressante et destinée à perdurer. Les différentes blockchains en cours d'expérimentation vont aussi permettre l'émergence de nouvelles formes d'organisation encore difficiles à appréhender aujourd'hui, comme les *decentralized autonomous organizations* (DAO), sans autorité centrale et sans assise nationale. Le défi posé au droit traditionnel reste largement à explorer. **Il ne s'agit donc pas d'un phénomène seulement économique mais aussi sociétal, culturel, presque civilisationnel**.

Accompagner l'innovation

Face à cette révolution issue de Bitcoin, les régulateurs devraient adopter une attitude raisonnable. Il convient de maintenir aussi faible que possible le poids de

la fiscalité et des obligations réglementaires pesant sur les entrepreneurs, les investisseurs, les créateurs et les consommateurs. Il est aussi important de faciliter l'activité des entreprises en clarifiant le traitement juridique et comptable de ces nouvelles activités et de ces nouveaux instruments. L'innovation est un processus suffisamment risqué pour que les pouvoirs publics n'y ajoutent pas du risque inutile à travers le flou ou les variations de la réglementation.

La compétition mondiale est engagée. Le capital et les talents sont largement mobiles. Impossible, à ce stade, de savoir combien d'emplois seront détruits et créés par cette révolution. Le dilemme qui s'offre à nous est identique à celui rencontré lors de chaque " grappe d'innovations " au sens de Schumpeter. D'un côté, nous focaliser sur les risques supposés de la technologie en refusant obstinément d'en reconnaître les côtés prometteurs, et laisser les pouvoirs publics céder à la " capture du régulateur " qui rend rentable pour les intérêts en place d'obtenir des " régulations " limitant l'émergence de nouveaux concurrents. De l'autre, **faire confiance aux mécanismes qui ont, depuis quelques siècles, permis la plus grande création de richesse et de prospérité au service de l'humanité** : recherche scientifique, innovation technologique, liberté d'entreprendre, respect de la propriété privée, accumulation du capital, libre échange, concurrence.

Introduction

En 1994, le rapport rédigé pour le premier ministre français par Gérard Théry, ingénieur général des télécommunications et créateur, en 1978, de Teletel, le réseau informatique du Minite (1) analysait Internet de la manière suivante : *" son mode de fonctionnement coopératif n'est pas conçu pour offrir des services commerciaux. Sa large ouverture à tous types d'utilisateurs et de services fait apparaître ses limites, notamment son inaptitude à offrir des services de qualité en temps réel de voix ou d'images. (...) Ce réseau est donc mal adapté à la fourniture de services commerciaux. Le chiffre d'affaires mondial sur les services qu'il engendre ne correspond qu'au douzième de celui du Minitel. Les limites d'Internet démontrent ainsi qu'il ne saurait, dans le long terme, constituer à lui tout seul, le réseau d'autoroutes mondial " (2).*

On pourrait multiplier à l'infini les exemples d'économistes, hauts-fonctionnaires, journalistes, scientifiques, chercheurs, professeurs qui ont, à l'époque, raillé les piètres performances d'Internet et juré qu'il ne se développerait jamais. Cette " *arrogance épistémique de ceux qui savent et se trompent* ", décrite par le chercheur Philippe Silberzahn (3) est une des raisons pour lesquelles la France est passée à côté de la révolution du web dans les années 1990 et qu'aucune des entreprises majeures dans ce domaine n'a été créée en France, alors que notre pays avait tous les atouts techniques, humains et financiers pour être un leader mondial.

1. Confier une réflexion sur internet à l'inventeur du minitel peut sembler paradoxal... tout comme confier une réflexion sur les cryptomonnaies à un ancien sous-gouverneur de la Banque de France.

2. THERY, Gérard, *Les Autoroutes de l'information*, rapport au premier ministre, 1994 http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000675.pdf

3. SILBERZAHN Philippe, *Bienvenue en incertitude ! Principes d'action pour un monde de surprises*, Natura Rerum Edition, 2017 (page 168)

Ces considérations n'impliquent aucunement que Bitcoin ne traverse pas une bulle, ni qu'il survivra aux péripéties actuelles. Mais cela incite à aborder ce sujet avec une certaine prudence.

L'idée que " ce qui compte, ce n'est pas le bitcoin, c'est la technologie derrière lui " a permis d'évacuer un peu trop rapidement le fait que, sans cryptomonnaie (4), les blockchains conteporaines n'existent pas. En négligeant Bitcoin (5), on se prive d'éléments précieux pour comprendre le phénomène plus global de la " blockchain ". La monnaie est à la fois la première " killer app " de la blockchain et son rouage indispensable.

L'objectif de cette étude est donc de revenir sur certaines caractéristiques trop peu connues de Bitcoin et d'explorer certaines dimensions et implications économiques, politiques et culturelles parfois vertigineuses de l'avènement du bitcoin et des cryptomonnaies en général.

L'idée n'est pas d'être exhaustif sur un sujet aussi complexe et foisonnant, ni de répondre aux multiples contre-arguments opposés à Bitcoin (qui oublient parfois que ce dernier ne prétend pas résoudre tous les maux de l'humanité), mais de fournir quelques pistes de réflexion pour alimenter un débat trop souvent biaisé. Parmi les multiples manières de décrire Bitcoin et la blockchain, de nombreuses peuvent être intéressantes, correctes et complémentaires. Celle proposée ici n'est que l'une des approches possibles et ne prétend aucunement à la vérité (6).

Après un rappel des principales caractéristiques techniques de Bitcoin (partie 1), nous approfondissons la question lancinante du " sous-jacent " du bitcoin, pour rappeler que ce dernier en est probablement moins dépourvu que les monnaies étatiques actuelles (partie 2).

Nous examinons ensuite la possibilité pour le bitcoin de devenir une véritable monnaie, et les conséquences économiques et politiques potentielles d'une telle évolution (partie 3), avant d'élargir l'analyse à la nouvelle ère de décentralisation et d'autonomie ouverte par les technologies liées au bitcoin et aux blokchains (partie 4).

4. Le mot " cybermonnaie ", préconisé par la commission d'enrichissement de la langue française en mai 2017, n'est pas dénué d'intérêt, malgré sa connotation un peu " années 1980 ". Nous préférons toutefois le terme qui a émergé à la suite d'un processus libre, décentralisé et concurrentiel, celui de " cryptomonnaie ". Ce terme nous parait préférable à l'expression vague de " monnaie virtuelle "

5. Précision de vocabulaire : nous utilisons le mot " Bitcoin " pour le réseau et le protocole, et " bitcoin " pour l'unité monétaire. Cette distinction est fondamentale. Le créateur d'Ethereum a d'ailleurs eu la présence d'esprit d'utiliser deux mots différents pour désigner ces deux objets : " Ethereum " et " l'ether ".

6. Par ailleurs, cette étude n'est pas un guide d'initiation, ne fournit pas de conseils (notamment en matière d'investissement) et ne fait pas de prédictions. Pour une initiation technique, on pourra se reporter à l'excellent guide publié par BitConseil (https://bitconseil.fr/produit/bitcoin-registres-blockchain-smart-contracts-guide-bitconseil/

Remerciements

Les auteurs tiennent à remercier, pour leur relecture attentive et leurs précieux conseils : David François, Jacques Favier, Jérôme de Tychey, Laurent Salat, Nicolas Bacca, Pierre-Louis Boitel, Pierre-Marie Padiou, Quentin de Beauchesne. Toute erreur ou imprécision subsistant reste bien sûr de la seule responsabilité des auteurs. Merci, également, à Tiphaine de Mombynes pour son œuvre qui illustre la couverture.

1. Une technologie idéaliste, révolutionnaire et évolutive

1.1 Les idéaux fondateurs

1.1.1 Les germes philosophiques

Le fait que Bitcoin ait été conçu en 2008 a laissé penser qu'il était une réaction à la grande crise financière mondiale de la même année. Il est vrai que Satoshi Nakamoto a inséré, dans le premier bloc de la blockchain Bitcoin, un message faisant référence à un nouveau sauvetage des banques par l'État : le titre d'un article du *Times* du 3 janvier 2009, " Chancellor on brink of second bailout for banks ". L'objectif de ce message était avant tout de prouver que la blockchain Bitcoin avait véritablement démarré le 3 janvier 2009, mais la concordance de la naissance de cette technologie avec la crise financière a souvent servi d'explication originelle.

Il faut pourtant remonter plusieurs décennies en arrière pour comprendre les origines véritables de cette technologie et de sa monnaie éponyme.

Dans les années 1990, alors qu'internet émerge véritablement pour le grand public, un groupe de mathématiciens, cryptographes, informaticiens et hackers se forme dans le but de militer pour la protection de la vie privée, en particulier par l'usage de la cryptographie. Les " cypherpunks ", parmi lesquels on retrouve les créateurs de Wikileaks, militent pour l'usage d'outils de chif-

frement afin d'écarter les risques grandissants d'intrusion des états ou de sociétés privées dans la vie privée des individus.

Timothy May est l'un des contributeurs majeurs de la mailing-list Cypherpunk, sur laquelle il diffusa en 1992 *Le Manifeste crypto-anarchiste* rédigé en 1988, texte fondateur et visionnaire à tendance libertaire, qui décrit brillamment la révolution numérique que nous vivons actuellement. Il est suivi par un autre manifeste, pubié en 1993 par Eric Hughes. Tous deux sont évoqués dans l'encadré suivant et figurent en intégralité en annexe (1).

1. Les textes majeurs de ce courant sont tous accessibles sur ce site : http://nakamotoinstitute.org/literature/

2. RODRIGUEZ, Philippe, *La Révolution blockchain*, Dunod, 2017

Les cypherpunks

" Les cypherpunks estiment que la vie privée est une bonne chose, écrit Tim May, et souhaitent qu'il y en ai davantage. Ils reconnaissent que ceux qui veulent une vie privée doivent s'en donner les moyens et ne pas simplement attendre des gouvernements, des entreprises ou d'autres organisations immenses et sans visage, qu'ils leur accordent une vie privée par bienveillance. Les cypherpunks savent que les peuples ont dû se créer leur propre vie privée pendant des siècles, avec des murmures, des enveloppes, des portes fermées et des courriers secrets " (...). Un an plus tard, Eric Hughes, l'un des membres du petit groupe désormais baptisé cypherpunk, publie un manifeste crypto-anarchiste, A Cypherpunk Manifesto. Il y reprend, à son tour, l'idée que la vie privée doit être préservée des possibles dérives du Net et que le système d'échanges anonymes doit êter généralisé. Il y appelle ainsi tous les cypherpunks à écrire des programmes de chiffrement pour se prémunir des écoutes opérées illégalement par les gouvernements ou les entreprises. " La vie privée est nécessaire dans une société ouverte à l'âge électronique, écrivait-il de manière prophétique. La vie privée n'est pas toutefois un secret. Une affaire privée est quelques chose dont on ne souhaite pas que tout le monde soit au courant, alors qu'une affaire secrète est quelque chose dont personne ne doit être au courant. La vie privée est donc le pouvoir de sélectionner ceux auxquels le monde sera révélé ". **Philippe RODRIGUEZ,** *La Révolution blockchain* **(2)**

Fondées sur des algorithmes publics, les solutions de chiffrement les plus célèbres sont nées dans les années 1990 et n'ont cessé de se développer et de gagner en légitimité. Parvenues à un stade de maturité mais encore insuffisamment adoptées du grand public, ces solutions peuvent permettre à quiconque de protéger ses correspondances et de signer électroniquement ses échanges, données ou documents. Une de leurs forces fondamentales repose sur leur indépendance de toute entité centrale. La confiance établie entre deux personnes ne repose que sur les mathématiques, ce qui permet de s'émanciper de tout tiers de confiance, étatique ou privé.

La confiance établie entre deux personnes ne repose que sur les mathématiques (...)

Parallèlement, Internet a vu apparaître de multiples innovations sur son réseau, tels que le web, l'email, la voix sur IP. Mises à la disposition de tous, ces technologies fondent en grande partie nos usages numériques et reposent toutes sur des protocoles technologiques libres. Mais, alors que les services de paiement électronique sont apparus dans les années 1980 avec les cartes bancaires à piste magnétique puis à puce, aucune technologie libre n'est quant à elle venue spécifiquement offrir d'alternative sur Internet à ces outils.

L'enjeu était d'ailleurs moins de créer un système de paiement libre que de concevoir un véritable système monétaire fonctionnant sur Internet. Un système de paiement ne peut être réellement libre tant que la monnaie qui y circule est contrôlée par les États et les banques. Les services tels que PayPal, même s'ils ont tenté de diffuser une image alternative par rapport au modèle des banques, interfèrent parfois dans la livraison des paiements. C'est ainsi qu'en 2010, Wikileaks a vu sa campagne de collecte de dons subitement stoppée par PayPal, puis Visa et Mastercard, ainsi que par les banques (3)

Les initiatives de systèmes monétaires et de paiement autonomes n'ont pas manqué depuis les années 2000, avec des propositions presque abouties comme B-money ou Bit Gold. Conçu par Nick Szabo en 1998, Bit Gold, est un projet de monnaie numérique décentralisée dont le fonctionnement est extrêmement proche de Bitcoin, mais qui n'a pas réussi à résoudre parfaitement le classique problème de la double dépense (Nick Szabo reste l'une des figures les plus écoutées de la communauté Bitcoin et est même souvent présenté comme le vrai Nakamoto (4)).

3. *Le Monde*, 24/12/10 - http://www.lemonde.fr/documents-wikileaks/article/2010/12/24/julian-assange-c-est-interessant-de-voir-la-censure-en-occident_1457331_1446239.html

4. *The New York Times,* 15/05/15 - https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html

1.1.2 Satoshi Nakamoto

Il fallut attendre la proposition technique de Satoshi Nakamoto en 2008 pour finalement découvrir le premier système monétaire libre et autonome. Bénéficiant du contexte de la crise financière de 2008 qui a renforcé le sentiment de défiance vis-à-vis du système bancaire et du rôle des États dans l'emballement de la création monétaire et du crédit, Bitcoin s'est imposé comme une solution inventive et totalement révolutionnaire par rapport aux environnements monétaires et financiers classiques.

Le texte de Nakamoto de 2008, *Bitcoin : A Peer-to-Peer Electronic Cash System* (cf. extrait en annexe), propose un protocole technique permettant de créer une monnaie aux caractéristiques radicalement nouvelles et le réseau d'échange autorisant son transfert de pair à pair, sans intervention d'un tiers de confiance.

> ***Le caractère universel de Bitcoin, la taille de sa communauté et l'absence d'autorité centrale, rendent cette technologie bien plus libre que celles animées par des leaders qui font souvent figure de gourou.***

Nakamoto (que ce pseudonyme représente une ou plusieurs personnes) a décidé de rester anonyme. Après avoir conçu et contribué à lancer le protocole, il s'est retiré publiquement en 2011, peu de temps après une réunion entre Gavin Andresen (son dauphin à l'époque) et la CIA. La majorité des auteurs de solutions cryptographiques a eu maille à partir avec les agences de renseignements des grands États : ce fait permet à lui seul de comprendre ce choix.

Le caractère universel de Bitcoin, la taille de sa communauté et l'absence d'autorité centrale et morale, rendent cette technologie et ce réseau bien plus libres et indépendants que ceux animé par des leaders qui font souvent figure de gourou. Ces créateurs identifiés représentent un point de vulnérabilité. Bitcoin n'est dirigé que par le consensus mathématique, sans dogme, même si les évolutions techniques réclament des manœuvres politiques de grande ampleur, et même si quelques personnalités comme les cryptographes et développeurs Gregory Maxwell, Nick Szabo ou Adam Back sont des références pour une grande partie de la communauté Bitcoin.

Cette invention est née sous forme d'un logiciel libre, fonctionne sur un réseau libre et est opérée selon des règles transparentes. Elle consacre l'émergence de la première monnaie numérique libre, autonome et résistante à la censure.

1.2 La mise en œuvre technique

1.2.1 Internet, machine à copier

Deux analogies peuvent être avancées pour appréhender Bitcoin de la meilleure façon.

La première s'appuie sur le déroulement d'une transaction. Lorsque Mario donne un billet de dix euros à Emmanuel, tout le monde s'accorde sur le fait que Mario ne détient plus le billet après la transaction. : il ne peut donc pas le dépenser à nouveau. Ce billet, théoriquement unique, peut être contrefait et l'analyse de son authenticité et de son unicité est compliquée : le receveur fait confiance au support de la monnaie (papier ou métallique). Si Mario fait un virement de dix euros à Emmanuel, son compte bancaire est le reflet de cette transaction et son solde est diminué du même montant. Emmanuel recevra ces fonds et verra son compte crédité du même montant.

Cette opération a été rendue possible par un système de compensation entre les deux banques teneurs des comptes. La banque contrôle le flux et est le garant de la bonne exécution de la transaction. L'opération réalisée directement entre deux individus avec un billet est impossible à reproduire numériquement sans faire appel à un tiers de confiance : la banque.

La seconde analogie rappelle qu'Internet étant une " machine à copier " l'information, seul un tiers peut garantir que l'argent ne peut être re-dépensé. La garantie qu'une transaction est unique (billet de banque ou transaction numérique) ne peut pas être constatée de manière simple. Sur Internet, l'intégrité de la transaction peut être garantie par la signature électronique mais l'unicité de la donnée est une notion inédite. Lorsqu'une photo numérique est envoyée à un destinataire, l'émetteur peut en conserver une copie. L'équivalent de l'invention de Nakamoto pour cette photo consiste à pouvoir certifier comme unique original cette photo auparavant si facilement duplicable.

La mise en œuvre de cette invention dans certains domaines artistiques et culturels ouvre de nouvelles perspectives en termes de titres de propriété, de rareté et de valeur économique. Mais, au-delà des enjeux de droit d'auteur et de propriété intellectuelle, c'est la problématique d'unicité ou d'exclusivité de la donnée numérique qui apparaît ici. C'est l'un des défis relevés par Bitcoin : rendre impossible la double dépense de la monnaie numérique.

Au-delà des notions de monnaie et de réseau de paiement, une manière complémentaire de comprendre le protocole Bitcoin est de le considérer comme une forme de messagerie sécurisée avec des messages signés numériquement sur une infrastructure comptable décentralisée.

1.2.2 Principales caractéristiques

Bitcoin est un réseau pair à pair. Les réseaux P2P sont principalement connus pour les services de partage de fichiers, mais aussi pour du calcul distribué ou des communications. Sur le réseau P2P de Bitcoin, circulent des messages signés numériquement dans lesquels sont enregistrées les informations relatives au transfert d'unités de compte appelées bitcoins (avec un b minuscule) de l'utilisateur A vers l'utilisateur B. Les messages ne sont pas chiffrés, ce qui signifie que chacun peut consulter l'intégralité des messages qui transitent sur ce réseau. A et B sont identifiés par des adresses Bitcoin. De façon raccourcie, on considèrera que A et B possèdent chacun une clé (dite privée) leur permettant de dépenser les bitcoins qu'ils ont reçus sur leur adresse grâce à la preuve de propriété que constitue la signature électronique. Il convient de souligner que, sur le réseau, ne circule aucun bitcoin, seulement des instructions comptables signées pour opérer le transfert de propriété d'un certain nombre de bitcoins de A vers B.

La deuxième brique de Bitcoin est sa blockchain. C'est une base de données dans laquelle sont enregistrées l'ensemble des opérations comptables échangées entre tous les utilisateurs depuis le démarrage du protocole. Chaque message ordonnant le déplacement d'une quantité de bitcoins est consigné dans ce grand registre. Selon le principe du " minage ", les transactions sont regroupées dans un bloc, chaque bloc validé étant ensuite scellé et enregistré dans la blockchain. Les transactions bitcoins sont toutes liées les unes aux autres car tout échange de A vers B est consigné dans le registre et tout nouveau mouvement de

B vers C sera également public. Chaque bloc de transactions est également lié au précédent par une empreinte cryptographique du bloc N-1 insérée dans le bloc N. Cette construction permet à chaque bloc de faire référence à tout l'historique, et non seulement au bloc précédent.

Cette base de données est distribuée sur l'ensemble des nœuds, ce qui signifie qu'elle est répliquée autant de fois qu'il y a de nœuds sur le réseau P2P. Chacun peut d'ailleurs décider de contribuer à la résilience de ce dernier en opérant une instance du registre général des transactions.

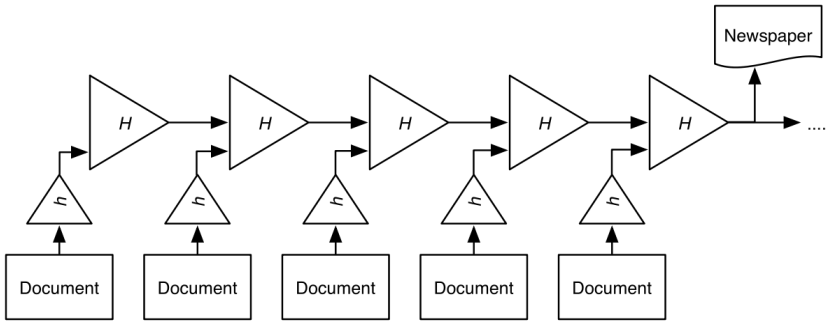
Si l'expression " block chain " (en deux mots) en référence à Bitcoin est postérieure au document de Nakamoto (5), il semble qu'elle ait été utilisée dès la fin des années 1990 dans des discussions sur des mailing lists de cryptographes.

Surtout, **la conception du type de base de données que nous appelons aujourd'hui " blockchain " date des travaux de deux chercheurs, Stuart Haber and W. Scott Stornetta, qui ont proposé, en 1991, un système de certification chaînée (chaîne d'horodatage, ou horodatage chaîné) (6).** Haber et Scott Stornetta sont d'ailleurs abondamment cités dans le white paper Bitcoin: ils font l'objet de trois de ses huit notes de bas de page. La ressemblance visuelle entre leur dispositif conçu dans les années 1990 et celui décrit par Nakamoto est frappante, comme le montrent les schémas suivants.

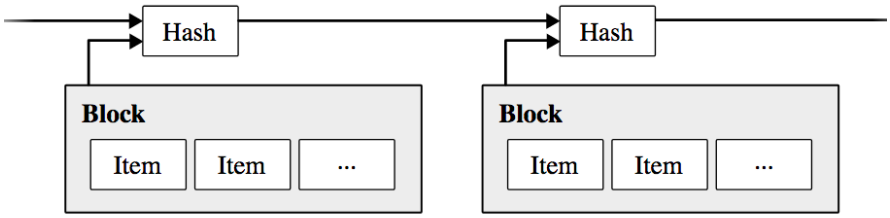
5. Il a été employé par Hal Finney en 2010 : http://satoshi.nakamotoinstitute.org/emails/cryptography/6/

6. https://en.wikipedia.org/wiki/Linked_timestamping Ce dispositif s'est affiné dans les années qui suivirent, au point de conduire à la création d'un standard ISO 18014 décrivant un mécanisme de tokens chainés : https://en.wikipedia.org/wiki/ISO/IEC_18014

Chaîne d'horodatage inventée dans les années 1990



Chaîne d'horodatage du white paper Bitcoin



7. " *Unspent Transaction Output* " (UTXO)

Le bitcoin est l'unité de compte numérique que l'on dépense dans les messages signés sur le réseau et dont les soldes sont représentés par les porte-monnaies qui font la somme des transactions dites " non-dépensées " (7) des adresses maintenues à jour dans la blockchain. Ce jeton est rare : sa création monétaire est limitée à 21 millions d'unités. Autre particularité, le bitcoin étant numérique, il est divisible et peut être échangé dans toutes les quotités désirées jusqu'au cent millionième (consensuellement nommé " Satoshi ").

Pour que ce bien numérique ne puisse être dépensé plusieurs fois s'il est copié, donc pour rendre le système absolument sécurisé, il faut que le registre comptable public des transactions soit inviolable. La blockchain peut être assimilée à une immense chambre forte transparente, composée d'un nombre presque infini de coffres transparents dont chaque utilisateur possède la clé pour en dépenser le contenu et dont les soldes sont vérifiables par tous.

Cette organisation comptable et sécuritaire est maintenue par le " minage ". Chaque transaction incluse dans un bloc est préalablement validée en vérifiant son historique traçable jusqu'à sa création. Ce bloc est ensuite scellé par un sceau numérique unique dont la valeur est le résultat d'une fonction (hash) unique dépendant de tous les éléments transactionnels contenu dans le bloc et lié au bloc N-1, et par extension à toute la blockchain.

> ***Bitcoin est le premier système monétaire autonome et résistant à la censure, complémentaire aux systèmes existants, fondé sur les mathématiques et la transparence.***

Tous les mineurs du réseau, observateurs des transactions, voient circuler quasiment les mêmes transactions au même moment. Les mineurs peuvent être des particuliers ou des professionnels ; seule compte la puissance de calcul qu'il vont consacrer à la réalisation de ce sceau numérique. Pour trouver ce sceau, tous sont en compétition pour résoudre une opération cryptographique qui est à la fois difficile à réaliser et est extrêmement facile à vérifier par les autres membres du réseau une fois qu'elle est achevée (cf. encadré suivant).

La difficulté du minage

Chaque bloc de transactions à miner constitue un ensemble de données. Certaines de ces informations (l'empreinte du bloc précédent, la date et l'heure de création du bloc, etc.) sont regroupées dans ce que l'on appelle " l'en-tête " du bloc. Cet en-tête comprend aussi une variable appelée " nonce ". Le minage consiste, pour le mineur à se livrer à des opérations de hachage (8) de l'en-tête avec un objectif : être le premier, parmi tous les mineurs, à trouver une valeur pour le " nonce " qui permette au hash obtenu de commencer par un certain nombre de zéros prévu par l'algorithme (ce nombre de zéros, ajusté toutes les deux semaines, détermine la difficulté de l'exercice).

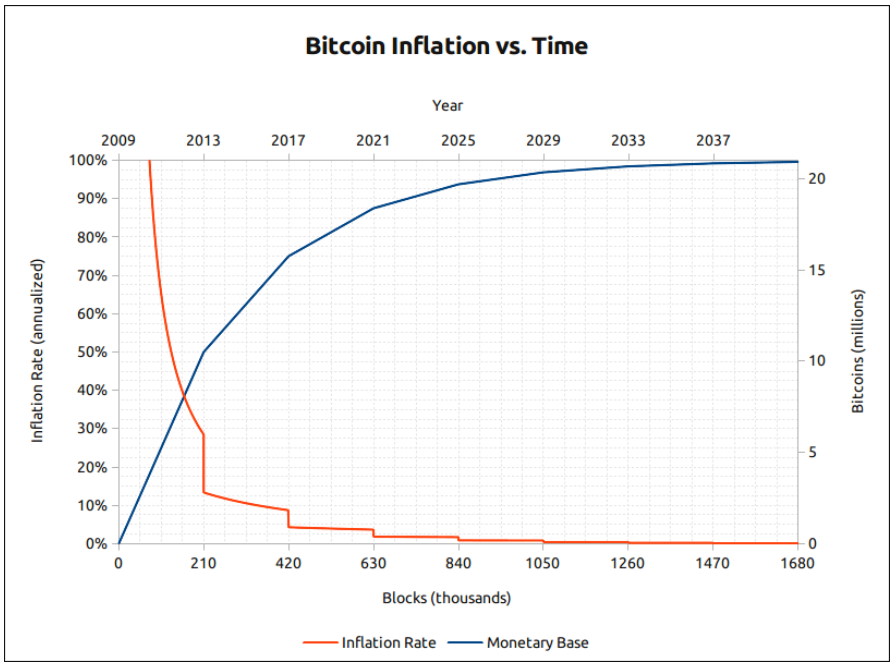
Pour cela, **le mineur n'a pas d'autre choix que d'essayer, aussi vite que possible, un maximum de valeurs pour ce nonce***, en refaisant à chaque fois le hachage, jusqu'à ce qu'il en trouve une qui permette de respecter la condition imposée. Voilà pourquoi cet exercice est difficile et nécessite une forte puissance informatique. Ensuite, pour vérifier instantanément le calcul du mineur qui affirme être le gagnant, il suffit au reste du réseau de refaire le calcul de hash en utilisant la valeur du nonce que le mineur a diffusée à tous. Toutes ces opérations sont bien sûr automatisées.*

Lorsqu'un premier mineur trouve la solution au challenge numérique imposé à tous, il le notifie instantanément au réseau. L'ensemble des nœuds accepte le nouveau bloc et le mineur est récompensé par les bitcoins créés à cet effet. La création monétaire n'est donc réalisée qu'en récompense du travail des mineurs pour sécuriser la blockchain. Le rythme de création monétaire défini dans le logiciel est connu dès le premier jour et tous les paramètres d'ajustement sont également prévus.

Plus il y a de mineurs en compétition, plus la puissance globale allouée à la résolution du challenge est élevée, et donc plus rapidement ce dernier sera-t-il remporté. Si cette fréquence augmente, le rythme de création monétaire augmentera également. Afin de de maintenir cette création à un rythme régulier, le logiciel adapte donc le niveau de difficulté requis tous les 2016 blocs (environ tous les 15 jours). Le niveau de la rémunération des mineur est, par ailleurs, divisé par deux tous les 210 000 blocs (environ tous les 4 ans). D'un montant de 50 bitcoins par bloc au démarrage du réseau, il est actuellement de 12,5 bitcoins par bloc.

8. Une fonction de hachage transforme n'importe quelle donnée numérique en une suite de caractères appelée " hash ", qui constitue une empreinte cryptographique. Une telle fonction a deux caractéristiques : d'une part elle est non réversible, on ne peut pas retrouver la donnée initiale à partir du hash final (en revanche on peut vérifier immédiatement si une empreinte est bien le hash d'une donnée spécifique : il suffit de hacher à nouveau cette dernière et de comparer les deux hashs qui doivent alors être identiques) ; d'autre part toute modification infime de la donnée initiale aboutit à une modification radicale du hash. Il existe plusieurs fonctions de hachage. Celle utilisée pour Bitcoin est SHA256.

La création de bitcoins atteindra sa limite asymptotique de 21 millions d'unités en 2140. Ce processus est représenté, en valeur et en pourcentage de progression, dans le graphique suivant.



En conclusion, **Bitcoin est un réseau en accès libre sur lequel quiconque peut réaliser des transactions infalsifiables, enregistrées publiquement dans un registre immuable grâce au travail d'une communauté incitée à allouer de la puissance de calcul pour percevoir la récompense que constitue la création monétaire**. Bitcoin peut s'apparenter à une forme de bien commun**,** actif patrimonial partagé par les membres d'une communauté, au sens spirituel et moral du mot " bien " comme au sens matériel et pratique. Il constitue le premier système monétaire et de paiement autonome et résistant à la censure, complémentaire aux systèmes existants, fondé sur les mathématiques et la transparence plutôt que sur la coercition et l'opacité. Bitcoin est libre et transparent, ne fait aucune promesse, n'oblige ni ne contraint personne, et permet à chacun de redevenir maitre de ses transactions et de son argent.

1.2.3 Evolution et gouvernance

Les premières années de Bitcoin ont été largement consacrées à la validation du modèle. Sa conception et sa sécurité ont été étudiées par tous les laboratoires de recherche des plus prestigieuses universités. Sa robustesse est continuellement mise à l'épreuve par tous les hackers du monde. Grâce à cet examen permanent, son modèle technologique a recueilli une validation assez générale du monde scientifique. Il est important de signaler que les analyses académiques ont quasiment toutes conduit à valider la rigueur de son protocole mathématique. **La robustesse de la technologie est acquise et n'est plus véritablement remise en cause** dans le flot d'articles à charge sur Bitcoin.

Les débats ont toujours été très animés dans la communauté Bitcoin. Ils concernent notamment le pilotage de ce logiciel libre, le choix des améliorations à y apporter, les héritages et interprétations des volontés du ou des créateurs. Dès les premières années de l'existence de Bitcoin, deux grandes voies d'évolution du protocole originel se sont ouvertes.

Tout d'abord, on a vu fleurir de nombreuses copies de Bitcoin. Les cryptomonnaies issues de Bitcoin, nommées " *altcoins* ", apportent au marché une richesse d'offres de monnaies, peut-être un peu trop abondante, mais aussi libre que Bitcoin. Certains altcoins font l'effort de proposer une technologie en certains points plus aboutie que Bitcoin, par exemple en termes d'anonymat (Monero est le plus connu).

La seconde voie consiste à faire évoluer Bitcoin afin qu'il puisse répondre aux exigences attendues en termes de sécurité et de passage à l'échelle (" scalabilité "). Le nombre de transactions possibles sur le réseau Bitcoin est encore très éloigné des capacités transactionnelles des réseaux de paiement privatifs tels que Visa ou Mastercard. Ce nombre est lié à la taille des blocs et à l'intervalle temporel séparant chacun d'entre eux. Actuellement, le réseau est en mesure de traiter approximativement 3 000 transactions par bloc, soit environ cinq transactions par seconde. Face à un usage croissant, le réseau arrive à saturation.

Cette limite n'est pas intrinsèque à la technologie. Elle résulte d'un choix consistant à privilégier la sécurité sur le volume des transactions. Chaque blockchain propose un compromis spécifique

entre ces deux paramètres, avec des implications différentes. Dans le cas de Bitcoin, la stratégie suivie jusqu'à présent consiste à essayer d'augmenter le volume possible sans diminuer le niveau de sécurité.

Plusieurs scénarios sont envisageables. Soit les efforts de recherche technique en cours dans l'écosystème aboutiront et permettront la scalabilité de Bitcoin. Soit d'autres cryptomonnaies, avec des caractéristiques différentes, s'imposeront. Quoi qu'il en soit, comme pour toute nouvelle technologie, il est important de ne pas analyser les limites actuelles de manière statique mais dynamique, en prenant en compte les progrès en cours et probables pour la suite.

S'agissant de l'amélioration de la scalabilité, le débat fait rage depuis plusieurs années au sein de la communauté des développeurs et cryptographes de Bitcoin. Dès 2010, Hal Finney, le premier développeur ayant travaillé avec Nakamoto, reconnaissait que " *Bitcoin lui-même ne peut atteindre une échelle permettant que chaque transaction dans le monde soit diffusée à chacun et inscrite dans la blockchain. On a besoin d'un niveau complémentaire de systèmes de paiement qui soit plus léger et plus efficace* " (9). Ce modèle de couches protocolaire est d'ailleurs celui qui compose aujourd'hui notre environnement numérique : HTTP (web), SMTP (mail), FTP (transfert de fichiers).

9. https://bitcoin.fr/verrouillage-de-segwit/

Une étape importante a été franchie avec l'optimisation qu'a représenté l'activation de Segwit en août 20173. Par ailleurs, la communauté ne s'étant pas mise d'accord sur les propositions d'augmentation de la taille des blocs, un *hard fork* a eu lieu le 1er août 2017, conduisant à la blockchain parallèle Bitcoin Cash. Le *hard fork* " Segit2X " prévoyant un doublement de la taille des blocs a finalement été abandonné en novembre 2017. Par ailleurs, au-delà de ces quelques épisodes emblématiques, des *hard forks* de moindre ampleur ont lieu très régulièrement, sans aucun impact sur le cours du bitcoin.

La priorité actuelle est le développement de solutions comme le *Lightning network* (10) (dont une condition technique préalable était la mise en œuvre de Segwit). Ce projet devrait permettre des paiements instantanés, sans tiers de confiance et avec pratiquement aucune limite de flux. Une des critiques cependant faites au réseau Lightning repose sur le caractère privatif et potentiellement centralisé des hubs de ce réseau, ces hubs devenant potentiellement de nouvelles banques. Dans ce schéma, le bitcoin fera figure de monnaie de réserve pour garantir un réseau

10. https://bitcoin.fr/video-2018-annee-lightning/

https://www.wired.com/story/the-lightning-network-could-make-bitcoin-faster-and-cheaper/amp?__twitter_impression=true

de paiement plus rapide (que certains appellent " *off chain* ", même si toutes les transactions de Lightning peuvent aussi passer "*on chain*"). L'une des trois principales startups en pointe dans le monde sur ce sujet est française : ACINQ (11).

C'est ainsi la perspective de centaines de milliers de transactions par seconde avec des frais réduits qui se dessine à plus ou moins brève échéance. Comme ces transactions pourront porter sur des micro-montants et avoir lieu successivement sur des micro-intervalles de temps, elles pourront, permettre des versements monétaires en flux continus et former, selon l'expression d'Andreas Antonopoulos, **des " cascades de paiements " ou de la " monnaie en streaming "** (12). Certains paiements comme des salaires ou une consommation de flux d'énergie ou d'information pourront être effectués en continu et non pas de manière ponctuelle. Les conséquences de cette évolution en matière organisationnelle, comptable, industrielle et même sociétale sont potentiellement considérables.

L'intense effort de recherche technologique en cours pour améliorer le réseau Bitcoin vise également à permettre la fongibilité du jeton numérique, faciliter les " smart contracts ", renforcer la confidentialité des transactions, et améliorer le respect de la vie privée4. Certains projets commencent à être connus, comme Rootstock (13) et TumbleBit (14). L'année 2018 devrait être riche en avancées dans tous ces domaines (15).

Beaucoup estiment ces progrès trop lents. Le choix clairement assumé par Bitcoin Core est d'œuvrer à une scalabilité qui ne crée pas d'effets pervers (diminution de la sécurité des transactions, concentration excessive du minage, etc.), quitte à accepter un progrès plus lent. Ce choix est contesté par certains : c'est l'intérêt des *hard forks* que de leur donner la possibilité de mettre en œuvre leur proposition et de la tester auprès des utilisateurs.

Ces événements témoignent du mode de gouvernance complexe et novateur de Bitcoin. Les décisions sont prises de manière consensuelle mais n'excluent pas des débats houleux, des stratégies d'influence, des jeux d'acteurs, des négociations. Tout l'enjeu est d'aligner des intérêts pas nécessairement concordants entre des acteurs et des communautés aussi différents que les mineurs, les plateformes d'échange, les développeurs historiques, les startups en création, etc. dont certains ont des activités très rentables en l'état (16).

11. Les deux autres sont Blockstream et Lightning Labs.

12. Les comptes rendus de la conférence internationale Scaling Bitcoin des 4-5 novembre 2017 à Stanford donnent une idée de la complexité et de la richesse des solutions en cours d'étude : https://bitconseil.fr/scaling-bitcoin-synthese-partie-1/ https://bitconseil.fr/scaling-bitcoin-synthese-2-scalabilite/

13. https://bitconseil.fr/rootstock-rsk-smart-contracts-bitcoin/

14. https://bitcoinmagazine.com/articles/bitcoin-privacy-all-breeze-wallet-about-bring-tumblebit-life/

15. https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/

16. Par exemple, une hypothèse consiste à supposer que l'équipe de Bitcoin Core conserve l'option d'un doublement de la taille des blocs comme instrument d'échange pour inciter les plateformes d'échange qui ne l'ont pas encore fait à implémenter Segwit

Cette gouvernance de Bitcoin est d'ailleurs très intriguante quand on la compare au fonctionnement des démocraties contemporaines. L'absence d'autorité centrale et la nécessité d'un très fort consensus entre ses utilisateurs pour toute modification importante rendent le système relativement conservateur : les règles ne sont modifiées que lorsqu'il y a une adhésion générale, une véritable conviction collective que le changement améliorera nettement le système. Cette caractéristique est très différente de la situation qui prévaut dans les démocraties modernes, où un pouvoir élu avec une médiocre proportion de l'électorat peut se permettre de transformer le droit dans tous les domaines, où chaque ministre tient à faire adopter " sa " grande loi, et où l'adaptation permanente du droit et de la fiscalité est politiquement valorisée alors qu'elle engendre une complexité et une insécurité juridiques désastreuses pour les équilibres sociaux et l'activité économique.

2. Un sous-jacent bien réel

2.1 Le bitcoin repose sur la technologie et la liberté

2.1.1 Bulle ou antifragilité ?

Le bitcoin et les cryptomonnaies constituent un terrain de jeu idéal pour les amateurs de prévisions, prédiction, pronostics et prophéties, surtout parmi les Prix Nobel d'économie, consultés par les médias comme la Pythie de Delphes. L'expérience prouve toutefois que cet exercice, concernant une technologie nouvelle, est particulièrement périlleux (cf. encadré suivant).

Le triste bilan de la prédiction

*En 1878, Robert Louis Stevenson prend la plume pour dissuader la ville de Londres d'adopter l'électricité pour son éclairage public : trop brillante, pas assez naturelle, dangereuse pour l'œil humain. En 1911, le général Foch écrit : " **les avions sont des jouets intéressants mais sans intérêt militaire** ". En 1962, le studio Decca Recording Co refuse de signer les Beatles : "**nous n'aimons pas leur son, et la guitare est déjà dépassée**". En 1977, trois ans après le choc pétrolier, Jimmy Carter déclare : " **chaque nouvel inventaire des réserves pétrolières est plus inquiétant que le précédent. La***

production mondiale peut probablement continuer à augmenter pendant encore six à huit ans. Mais à un moment dans les années 1980, elle n'augmentera plus. La demande dépassera la production ". En 1989, le Prix Nobel d'économie Paul A. Samuelson écrit : " contrairement à ce que de nombreux sceptiques ont longtemps cru, l'économie soviétique est la preuve qu'une économie socialiste dirigée peut fonctionner et même réussir ". En 2007, Steve Balmer, PDG de Microsoft, déclare : " il n'y a aucune chance que l'iPhone obtienne une part de marché significative ".

Philippe SILBERZAHN, *Bienvenue en incertitude !* **(1)**

1. Source : SILBERZAHN Philippe, *Bienvenue en incertitude ! Principes d'action pour un monde de surprises*, Natura Rerum Edition, 2017 (page 74)

2. " Le bitcoin, monnaie pour un monde fini ", blog *Le Nœud gordien*, 23/11/17 http://www.noeud-gordien.fr/index.php?post/2017/11/23/Le-Bitcoin%2C-monnaie-pour-un-monde-fini

Dans le débat public, il va de soi que le bitcoin traverse une bulle et qu'il n'a pas de sous-jacent. La réalité est plus compliquée, comme le suggère l'intéressante analyse d'**Alexis Toulet (2) :**

" Une véritable bulle n'a lieu qu'une fois, et lorsqu'elle a éclaté aucun nouvel engouement ne peut recommencer, surtout pas pour le même produit. On n'a jamais entendu parler d'une nouvelle bulle sur les valeurs Internet après le krach de 2000, ni sur les crédits subprime après le krach de 2007. Or, le bitcoin a déjà connu plusieurs bulles… et y a survécu. C'est ainsi que son cours :

- *A connu un pic supérieur à 20 € en juin 2011… avant de chuter de plus de moitié*
- *Nouvel emballement jusqu'à plus de 200 € en avril 2013… puis perte brutale de plus de 60% de cette valeur*
- *Encore une bulle jusqu'à frôler les 900 € en décembre 2013… suivie d'un effondrement dans les profondeurs, moins de 200 € en janvier 2015*
- *Enfin, augmentation plus ou moins continue à partir de début 2016 jusqu'à environ 1200 € au printemps 2017, suivie d'une montée en flèche à 7 000 € au 22 novembre 2017*

La structure est à l'évidence différente de celle d'une simple bulle. Des paliers successifs sont atteints, entrecoupés de bulles et d'effondrements, mais à chaque fois

la valeur du bitcoin finit par reprendre sa hausse. (…) Soit plusieurs millions de personnes sont en train de lourdement se tromper, et avec obstination encore, car ils recommencent et recommencent en permanence… soit il y a une vraie valeur sous-jacente au système Bitcoin ".

L'expression " valeur sous-jacente au système Bitcoin " est certainement plus appropriée que " le sous-jacent du bitcoin ". Dans le vocabulaire financier, un actif sous-jacent concerne un produit dérivé (3), ce que le bitcoin n'est pas. Toutefois, faute de terme plus adapté, et pour bien insister sur le fait que Bitcoins s'appuie bien sur un actif réel, nous l'utilisons ici.

Comment savoir si l'on est en présence d'une bulle ? Selon **Jean Tirole,** *" une bulle existe lorsque la valeur d'un actif financier excède le " fondamental " de l'actif, c'est-à-dire la valeur actualisée des dividendes, intérêts ou loyers qu'il rapportera aujourd'hui et dans le futur. En d'autres termes, l'actif est surévalué par rapport à sa valeur intrinsèque – la valeur actualisée des dividendes, coupons, loyers ou aménités associées à la détention de l'actif " (4).* Les nombreux commentateurs qui estiment que le bitcoin traverse une bulle n'ont jamais réussi à étayer leur affirmation par un calcul reposant sur cette définition.

On prétend souvent que le bitcoin ne " repose sur rien ". C'est ce qu'affirme notamment **Jean Tirole :** *" Si un jour le marché décide que Bitcoin n'a aucune valeur – si les investisseurs perdent confiance dans Bitcoin -, Bitcoin n'aura effectivement aucune valeur, car il n'y a pas de valeur fondamentale derrière Bitcoin, contrairement à une action ou à une propriété immobilière " (5).* Paul Krumgan, autre prix Nobel d'économie, s'est aussi montré très critique envers le bitcoin (il convient de rappeler qu'en 1998 il avait pronostiqué à tort un ralentissement d'Internet (6)).

Beaucoup estiment que la valeur du bitcoin ne réside que dans la confiance que les gens lui portent, contrairement à l'or qui a une valeur économique plus objective grâce à ses usages non monétaires (bijouterie et industrie). Comme le montrent les sections suivante, en réalité le bitcoin s'appuie sur un actif bien réel : un réseau sécurisé, un écosystème industriel et une communauté. Surtout, c'est oublier qu'il n'y a pas de valeur économique " fon-

3. Un actif sous-jacent est " *un actif sur lequel porte une option ou plus largement un produit dérivé. Il peut être financier (actions, obligations, bons du Trésor, contrats à terme, devises, indices boursiers…) ou physique (matières premières agricoles ou minérales…). L'actif sous-jacent est l'actif réel sur le prix contractuel duquel porte le produit dérivé concerné. Il désigne en effet l'instrument support d'un contrat à terme dont la qualité est strictement définie* " https://fr.wikipedia.org/wiki/Actif_sous-jacent

4. TIROLE, Jean, *Economie du bien commun*, PUF, 2016 (page 404)

5. *Ibid*. Tirole a réaffirmé cette thèse plus récemment, dans le *Financial Times*, en novembre 2017 : https://www.lesechos.fr/finance-marches/marches-financiers/030957836512-pour-jean-tirole-le-bitcoin-na-aucune-valeur-intrinseque-2134561.php

6. Krugman parlait de la technologie, non du cours des actions des startups internet. Il estimait notamment qu'en 2005, Internet n'aurait pas eu plus d'impact sur l'économie que le fax. www.digitaljournal.com/article/346996

damentale " ou " intrinsèque ". **La valeur des choses ne résulte que de l'appréciation subjective des individus** et des comparaisons qu'ils effectuent avec d'autres biens (ou avec d'autres moments pour mener leurs activités). C'est aussi le cas pour l'or, même dans ses usages non monétaires.

> *Ce qui permet à Bitcoin de survivre et de se développer, c'est parce qu'il a un triple sous-jacent : un réseau sécurisé, un écosystème industriel, et une communauté humaine.*

Les économistes " *mainstream* " ont du mal à dissimuler leur perplexité face à l'objet économique profondément nouveau qu'est Bitcoin. Par exemple, Robert Shiller, autre Prix Nobel, après avoir estimé en 2017 que le bitcoin était un exemple typique de bulle spéculative (7), a indiqué en janvier 2018 " *ne pas savoir que faire du bitcoin, en fin de compte* " : pour lui, s'il est probable que le bitcoin s'effondre complètement, il peut tout aussi bien " *survivre pendant 100 ans* " (8).

La présente étude ne prend pas position sur le fait de savoir si le bitcoin traverse (ou a traversé) une bulle ou non. En revanche, **les prix Nobel d'économie et autres " experts " ne sont probablement pas les mieux placés pour faire des prédictions sur ce sujet**. Bitcoin représente quelque chose de technologiquement totalement nouveau, largement en dehors de leur expertise habituelle : il constitue une réelle " discontinuité " (cf. encadré suivant).

7. *Cointelegraph*, 05/09/17 : https://cointelegraph.com/news/nobel-prize-winner-uses-bitcoin-as-example-of-irrational-exuberance

8. *Cointelegraph*, 19/01/18 : https://cointelegraph.com/news/yale-prof-shiller-thinks-bitcoins-bubble-could-actually-linger-100-years

Pourquoi les experts se trompent-ils plus souvent que les généralistes face à une discontinuité ?

> *" Premièrement parce que leur expertise est un stock de connaissance, et que la connaissance ne peut concerner que le passé, ce qui a marché précédemment (...). Par définition, une discontinuité remet en question ce qui a marché jusque-là, et donc* ***de facto*** *le savoir de l'expert.* ***La discontinuité est précisément le moment où le savoir de l'expert n'est plus valable. C'est la dernière personne à consulter en cette occasion !*** *Deuxièmement parce que la discontinuité surgit par définition en dehors du cadre de l'expertise. L'expert ne la voit donc pas, du moins initialement, et lorsqu'il la voit, peut avoir tendance à ne pas la prendre au sérieux. Ainsi, en 1876, un expert du télégraphe regardera les balbutiements du téléphone, qui au début est de très mauvaise qualité et ne va pas au-delà de quelques centaines de*

> *mètres, avec une bonne dose de scepticisme. C'est ce qui explique que la Western Union grand opérateur du télégraphe aux États-Unis au siècle dernier, ait écrit à cette époque : " ce téléphone a trop de limitations pour être sérieusement considéré comme un moyen de communication " ".* **Philippe Silberzahn,** *Bienvenue en incertitude !* **(9).**

De la même manière, les analogies historiques comme celle sur la crise des Tulipes sont généralement dénuées de toute rigueur et du moindre rapport avec un phénomène technologique comme Bitcoin. De nombreux travaux historiques récents ont démontré qu'il s'agissait d'un événement historique largement déformé (10). Comme le dit **Jacques Favier** (11) : *" la spéculation sur la tulipe en 1637 est sans doute le morceau choisi d'histoire le plus souvent invoqué par ceux qui veulent montrer la profondeur de leur ignorance concernant Bitcoin " (12).*

S'il existe aujourd'hui une bulle, c'est surtout autour de certains *altcoins*, de certaines *initial coin offerings* (ICO), et plus généralement de l'expression " technologie blockchain " (cf. partie 4). Mais même ces phénomènes spéculatifs, en apparence excessifs, déraisonnables et dangereux, peuvent garder un intérêt pour l'ensemble de la société et l'économie, comme le résume très bien **Nicolas Colin** : *" Bien sûr, en cas de succès, l'emballement attire des spéculateurs, qui accompagnent le mouvement de façon opportuniste sans éprouver d'intérêt pour le protocole lui-même. Mais leur irruption n'est pas inutile : ils contribuent à attirer l'attention de nouvelles générations d'utilisateurs. Comme l'a montré l'économiste Carlota Pérez, de tels emballements spéculatifs sont déterminants pour l'émergence des innovations de rupture. Les bulles ne sont toxiques que si elles contaminent le système bancaire, ce qui n'est pas le cas avec les cryptomonnaies " (13).*

On peut se demander si le discours permanent sur la " bulle ", qui semble fragiliser Bitcoin, ne contribue pas en fait à son caractère antifragile. **Bitcoin peut, en effet, être considéré comme une entité " antifragile " au sens de Taleb** (14) : à la différence de systèmes institutionnels classiques comme les systèmes monétaires ou bancaires, plus il est attaqué, plus il se renforce (15).

9. SILBERZAHN Philippe, *Bienvenue en incertitude ! Principes d'action pour un monde de surprises*, Natura Rerum Edition, 2017 (page 134)

10. https://www.smithsonianmag.com/history/there-never-was-real-tulip-fever-180964915/

11. Historien, ancien banquier et auteur, avec Adli Bataille, de l'excellent ouvrage *Bitcoin, la monnaie acéphale* (CNRS Editions, 2017).

12. FAVIER, Jacques, " Tulipes ", 19/09/17, blog *La Voie du Bitcoin* http://blog.lavoiedubitcoin.info/post/Tulipes

13. COLIN, Nicolas, " Cryptomonnaies, un peu de cohérence ", *L'Obs*, n°2777, 25/01/18

14. " *Certains objets tirent profit des chocs ; ils prospèrent et se développent quand ils sont exposés à la volatilité, au hasard, au désordre et au stress, et ils aiment l'aventure, le risque et l'incertitude (...). L'antifragilité dépasse la résistance et la solidité. Ce qui est résistant supporte les chocs et reste pareil ; ce qui est antifragile s'améliore. Cette qualité est propre à tout ce qui s'est modifié avec le temps ".* TALEB Nassim Nicholas, *Antifragile. Les bienfaits du désordre.* Les Belles Lettres, 2013 (page 13)

15. https://medium.com/@eranshir/bitcoin-as-the-first-anti-fragile-economical-entity-b52bc600ec91 https://medium.com/blockchannel/thoughts-on-the-antifragility-of-bitcoin-cryptocurrencies-2624b1bcaa87

Les flambées du cours le font connaître, mais les chutes ponctuelles attirent aussi les investisseurs regrettant de ne pas avoir acheté plus tôt. Même les campagnes médiatiques négatives sont finalement utiles au bitcoin, en le faisant découvrir à des publics qui l'ignoraient et qui décident ensuite d'en acheter. Plus les médias et les gouvernements communiquent sur les dangers du bitcoin et des cryptomonnaies et sur la nécessité de les encadrer strictement, plus les populations se rendent compte que le fonctionnement du système bancaire et monétaire ne leur garantit pas une pleine maîtrise de leur argent, et plus elles s'intéressent à Bitcoin.

Bitcoin satisfait probablement à la loi appelée "effet Lindy" : l'espérance de vie future de tout objet non périssable (technologie, idée, etc.) augmente avec le temps. Comme le résume **Taleb :** *" s'agissant du périssable, chaque jour de vie supplémentaire se traduit pas une espérance de vie plus courte. S'agissant du non périssable, chaque jour supplémentaire peut impliquer une espérance de vie plus longue "(16).* Taleb reconnaît que cette idée n'est pas aisée à comprendre et fournit l'exemple suivant : *" si un livre est encore publié quarante après, je peux m'attendre à ce qu'il le soit quarante ans de plus. Cependant (...), s'il survit une décennie de plus, l'on s'attendra alors à ce qu'il soit publié pendant encore cinquante ans ".* On peut faire le même raisonnement avec Bitcoin, objet technologique récent et révolutionnaire dont il est particulièrement difficile de prédire l'espérance de vie. Le fait qu'il ait fonctionné pendant huit ans et continue de se développer malgré l'accumulation d'obstacles apparemment insurmontables fournit une indication déterminante sur sa capacité à continuer d'exister sur une période au moins égale et croissante avec chaque jour qui passe.

Ce qui permet à Bitcoin de survivre et de se développer, c'est parce qu'il a un triple sous-jacent : un réseau sécurisé, un écosystème industriel, et une communauté humaine.

16. TALEB Nassim Nicholas, *Antifragile. Les bienfaits du désordre.* Les Belles Lettres, 2013 (page 385). Taleb précise bien que ses arguments " *ne concernent pas toutes les technologiques, mais l'espérance de vie, ce qui est seulement une moyenne résultant de probabilités* "

2.1.2 La sécurité du réseau

Le premier sous-jacent du bitcoin est la sécurité inégalée qu'offre son protocole. Grâce à la décentralisation du registre et au mécanisme de la preuve de travail, une transaction, une fois validée dans un bloc, est pratiquement impossible à falsifier. Avec l'enregistrement successif des blocs suivants, cette difficulté augmente de manière exponentielle. Au bout de quelques heures, la dépense d'énergie nécessaire représenterait des centaines de millions de dollars. A mesure que le temps passe, l'information inscrite dans cette transaction acquiert donc un caractère d'inviolabilité qui fait du bitcoin le premier actif numérique pratiquement inaltérable, et sa blockchain la première base de données impossible à modifier sans respecter les règles. Pour cette raison, il a été comparé aux plus grands et aux plus anciens monuments de la civilisation comme les pyramides d'Egypte (17). Cette inaltérabilité a une valeur en soi ; elle représente un véritable service. C'est sur cette valeur, sur ce service, qu'est assis le bitcoin.

Pour comprendre la valeur de ce réseau on peut essayer d'imaginer combien coûterait une tentative de recréer *ex nihilo* un réseau de paiement mondial offrant exactement les mêmes performances que Bitcoin, notamment en termes de sécurité et de résistance à la censure. Cela représenterait, pour la communauté qui souhaiterait réaliser ce chantier, une somme phénoménale, pratiquement impossible à évaluer, qui se compterait en milliards ou dizaines de milliards de dollars. D'ailleurs aucune entreprise ou consortium n'a tenté cette performance.

Le fait qu'une monnaie puisse avoir pour sous-jacent un réseau informatique est bien sûr une situation inédite. Après des millénaires pendant lesquels la monnaie était assise sur des biens matériels, puis une cinquantaine d'années pendant lesquelles elle ne reposait que sur une vague confiance dans l'économie des États et surtout sur la capacité de ces derniers à imposer leur monnaie par la force (cf. infra) une nouvelle forme de monnaie a pour sous-jacent un service fourni par un protocole informatique. C'est la déclinaison, au domaine de la monnaie, de la digitalisation progressive de toutes les activités économiques résumée par la formule célèbre de Marc Andreesen, " *software is eating the world* " (18).

17. " *Les pyramides se dressent aujourd'hui comme un témoignage de la preuve de travail de la civilisation égyptienne (...) Bitcoin est le premier monument digital de preuve de travail de dimension planétaire* ". In ANTONOPOULOS, Andreas, *The Internet of Money, volume two*, Merkle Bloom, 2017 (page 29)

18. The Wall Street Journal, 20/08/11 : https://a16z.com/2016/08/20/why-software-is-eating-the-world/

Ce qui sert à produire cet actif sous-jacent, c'est la forte la puissance de calcul totale consacrée par les mineurs au réseau Bitcoin, qui est parfaitement quantifiable (elle est mesurée par le *hash rate* : nombre de calculs de hashs par période de temps). Plus elle est élevée, plus la difficulté à falsifier une transaction est forte, et donc plus le réseau est sécurisé et plus le bitcoin a de la valeur aux yeux de ses utilisateurs. On pourrait très bien imaginer une autre blockchain offrant le même niveau de sécurité que Bitcoin, pour un même volume de transactions, mais avec un protocole différent, qui nécessiterait une puissance de calcul inférieure. Mais pour l'instant elle n'existe pas. La valeur de marché du bitcoin dépend en partie de ce *hash rate*. En cas de *hard fork* (comme, plus généralement, face à tout concurrent pouvant attirer des sociétés de minage), l'un des enjeux principaux pour le réseau Bitcoin est d'éviter que trop de mineurs mettent leur puissance de calcul au service de la nouvelle chaîne.

Par ailleurs, ce que l'on décrit comme la " spéculation " autour du bitcoin contribue indirectement à renforcer la puissance de calcul et la sécurité du réseau : l'augmentation du cours du bitcoin attire de nouveaux mineurs, ce qui entraîne une augmentation de la difficulté du minage (19), donc de la sécurité du réseau et donc de l'intérêt du public pour le bitcoin. Au-delà de la spéculation (dont les conséquences monétaires sont évoquées infra), il existe une particularité souvent ignorée du bitcoin : la hausse de sa valeur a un effet radicalement différent de celui observé pour les autres types de monnaies. Les efforts supplémentaires consacrés à la production en réponse à la progression du cours n'aboutissent pas à une stabilisation de ce dernier (comme c'est le cas pour les monnaies métalliques ou fiat) mais à un renforcement de la sécurité du réseau, et donc à une augmentation de sa demande et, toutes choses égales par ailleurs, de son cours (20).

Ce sous-jacent quantifiable en puissance de calcul est un déterminant indirect de la valeur de marché du bitcoin. Ce qui compte plus directement, c'est l'évaluation subjective, par les utilisateurs du bitcoin, de la sécurité ainsi offerte sur ce réseau. Si, pour eux, la possibilité d'utiliser ce protocole de confiance mondial qui n'a jamais été piraté a une forte valeur, cela contribuera, avec d'autres paramètres (facilité d'utilisation, rapidité, frais de transactions, etc.) à faire augmenter la demande et le cours du bitcoin.

Tout comme l'utilisation non monétaire de l'or est la bijouterie et quelques composants industriels, dans le cas du bitcoin, on peut considérer, en conclusion, que son utilisation non monétaire est

19. Cette difficulté étant ajustée automatiquement tous les 2016 blocs, soit environ deux semaines pour maintenir stable le rythme de validation des blocs et donc d'émission des nouveaux bitcoins (cf. partie 1).

20. Dans le cas d'une monnaie métallique, toute hausse de la valeur du métal précieux incite à consacrer plus de ressources pour en extraire davantage. Cela fait augmenter la production et conduit progressivement à une stabilisation puis une baisse du cours. Pour les monnaies nationales actuelles, une hausse du cours incite souvent les États à mener une politique monétaire permettant de maîtriser cette hausse, afin notamment de ne pas desservir les exportations nationales (ce qui se fait donc au détriment des détenteurs de cette monnaie). Pour Bitcoin, il en va tout autrement. Une hausse du cours entraîne, comme pour l'or, une augmentation des moyens consacrés à le produire : le minage devient plus rémunérateur donc les mineurs vont accroître leurs moyens pour miner davantage, et de nouvelles entreprises vont se lancer sur ce marché. Mais ce développement du minage ne créera pas plus de bitcoins puisque le rythme de production est figé dans l'algorithme fondateur : il entraînera, en revanche, une amélioration de la sécurité du réseau, à travers l'ajustement de la difficulté du minage évoquée plus haut. Ce mécanisme représente donc un cercle vertueux qu'on ne trouve dans aucun autre type de monnaie : plus le bitcoin s'apprécie, plus la sécurité de son réseau augmente, et plus cette monnaie devient attractive pour un public croissant, ce qui augmente sa demande.

un droit d'accès au système de transfert de valeur international le plus sécurisé et le plus résistant à la censure qui ait jamais existé.

On a l'habitude d'évaluer la puissance d'une institution (entreprise ou État) par sa production mais aussi par le niveau de ressources qu'elle est capable de consacrer à sa sécurité : ressources financières, humaines, militaires ou énergétiques. Pour Bitcoin, son niveau élevé de sécurité obtenu par la forte dépense énergétique est systématiquement décrit comme un inconvénient, une gabegie, une tare originelle, alors qu'il constitue en fait la preuve de l'importance de ce système. Cela provient de son important coût environnemental, qui est évoqué dans la section suivante, avant d'aborder les deux autres composantes du sous-jacent du bitcoin.

2.1.3 La question énergétique

La forte consommation énergétique du bitcoin est une question sérieuse. Or elle est rarement traitée de manière sérieuse dans les médias. Elle se résume souvent à un procès à charge, avec des données anciennes, peu précises, parfois non vérifiées, reposant sur des hypothèses douteuses, pas toujours explicites, et sans aucune prise en considération ni des coûts du système classique, ni des arguments de la " défense " du système Bitcoin.

Un rapport de Crédit Suisse de janvier 2018 a d'ailleurs reconnu que les prévisions apocalyptiques sur l'évolution future de la consommation énergétique de Bitcoin, souvent citées sans la moindre distance critique, étaient largement infondées (21).

21. https://www.bloomberg.com/news/articles/2018-01-16/bitcoin-s-power-needs-may-be-overblown-recalling-pot-growing

Quelle que soit la manière dont on la mesure, cette consommation est actuellement très élevée. Si elle devait augmenter avec le développement de Bitcoin, cela pourrait poser un problème réel qui nécessiterait des solutions qui n'existent pas encore. Mais, sans prétendre à l'exhaustivité sur un sujet aussi complexe, il convient également de prendre en compte les éléments suivants.

Tout d'abord, contrairement à une croyance trop répandue, **le débit sur le réseau Bitcoin n'est pas une fonction croissante de la puissance de calcul**. Cela signifie que les différents efforts techniques en cours pour améliorer le nombre de transactions par secondes, par exemple le réseau Lightning Network (cf. partie1), n'entraîneront pas en soi une augmentation de la consommation électrique. Cette dernière dépend d'autres paramètres, comme

le cours du bitcoin, le nombre de mineurs, le type de machines qu'ils utilisent, etc.

Une consommation importante est indispensable à la sécurité du réseau. Il s'agit d'un prix à payer pour un service objectivement important : un réseau d'échange ultra-sécurisé, mondial, décentralisé, résistant à la censure. La question de savoir si ce service " vaut " ce coût environnemental est faussée par le fait qu'actuellement, peu de gens comprennent l'avancée technologique et sociétale que représente Bitcoin. Toute leur attention est donc focalisée sur ce qui est perçu comme un inconvénient. Cette situation va sans doute évoluer : comme dans toute autre industrie, on comprendra progressivement que la production d'un service universellement recherché ne se fait pas sans coût.

> *La question de savoir si ce service " vaut " ce coût environnemental élevé est faussée par le fait qu'actuellement, peu de gens comprennent l'avancée technologique et sociétale que représente Bitcoin.*

Dans le cas du bitcoin, un coût significatif est nécessaire car la sécurité inégalée du réseau repose sur l'asymétrie extrême existant entre le coût de validation des transactions (presque nul (22)) et le coût d'inscription d'une transaction dans la blockchain (qui nécessite le minage et sa preuve de travail). Il est d'ailleurs intéressant de noter que cette asymétrie est l'inverse de celle en vigueur dans les systèmes de paiement classiques, où le coût de la validation est élevé (car il est centralisé) et celui de l'inscription dans le registre est négligeable (car il est automatisé).

Pour Bitcoin, ce coût énergétique n'est pas caché. Il est assumé, il est même ce sur quoi repose la qualité principale de système. L'électricité est en quelque sorte sa matière première. Il en va tout autrement de secteurs comme l'industrie bancaire, dont le coût énergétique est considérable mais jamais évalué, reconnu, ni publié. Il serait intéressant de calculer le coût énergétique du secteur bancaire : distributeurs de monnaie, transport de fonds, construction et entretien de bâtiments (agences bancaires, gratte-ciels), coûts associés aux millions d'employés (23) de ce secteur (transport pour se rendre à leur travail, chauffage, climatisation, etc.). Certes, ce secteur gère un volume d'activité bien supérieur à celui des cryptomonnaies, mais la scalabilité de ces dernières est possible sans augmentation de leur coût énergétique.

22. Il s'agit des quelques secondes de vérification simple et automatique effectuée par les milliers de nodes du réseau.

23. On peut penser que de nombreux employés seront progressivement remplacés par les outils issus de cette révolution technologique (smart contracts et cryptomonnaies). Les enjeux de cette évolution sont exactement les mêmes que ceux rencontrés depuis des siècles avec le progrès technique. Les reconversions seront d'autant plus difficiles socialement et humainement qu'elles auront été mal anticipées, voire freinées par certains acteurs institutionnels comme les syndicats ou l'État. En revanche, si elles sont gérées intelligemment, la ressource humaine rendue disponible pourra se consacrer à d'autres tâches d'une manière satisfaisante pour les individus et bénéfique pour la société.

S'agissant des autres cryptomonnaies, certaines prétendent se passer de la preuve de travail et de la consommation énergétique qui en découle. Mais elles doivent aussi assumer un compromis dans lequel le niveau de sécurité est lui aussi diminué. L'avenir dira si elles peuvent passer à l'échelle avec ce niveau réduit.

Enfin, les mineurs ne sont pas des organisations philanthropiques ou des administrations publiques : ce sont des entreprises commerciales en concurrence, qui doivent réduire leurs coûts autant que possible tout en assurant leur production et maximiser leur profit. Ils ont un intérêt objectif à maximiser leur efficacité énergétique. Or c'est exactement ce qu'ils font, et cela de deux manières.

D'une part, **ils recherchent des équipements moins énergivores.** Une industrie spécifique est en train de se créer pour répondre à cette demande.

D'autre part, **ils recherchent l'électricité là où elle est la plus abondante et la moins chère**, c'est-à-dire là où elle ne fait pas l'objet d'une demande concurrente. C'est la raison pour laquelle de nombreuses entreprises de minage sont installées dans des zones dépourvues de réseaux de distribution locale et utilisent de plus en plus les énergies non renouvelables. Certains pensent d'ailleurs que cette industrie pourrait encourager l'industrie verte en rendant rentables des sources d'énergie qui ne l'étaient pas auparavant (24). Au Canada, la société Hydro-Quebec souhaite, pour maintenir sa production hydroélectrique sous-utilisée et menacée par le développement de l'auto-production des particuliers, attirer des entreprises énergivores, dont des mineurs de cryptomonnaies (25).

D'ailleurs, les chiffres de l'évolution de la consommation mondiale d'énergie montrent que la consommation d'électricité du bitcoin ne s'est pas ajoutée à la consommation habituelle : elle s'est donc alimentée principalement d'une énergie qui aurait été perdue sans cette utilisation. Bitcoin n'a pas " volé " de l'énergie aux pays, aux entreprises et aux particuliers.

24. *Coincenter*, 14/12/17 : https://coincenter.org/entry/how-bitcoin-could-drive-the-clean-energy-revolution

25. " *La maison intelligente produisant une partie de son énergie pourrait être rentable au Québec à partir de 2025. Des propriétaires pourraient produire jusqu'à 15 % de leur consommation énergétique. La consommation d'électricité des Québécois plafonne depuis 2007. Elle pourrait maintenant décroître. (…) Si les Québécois consomment moins, Hydro-Québec devra nécessairement se tourner vers une autre clientèle pour écouler sa production et éviter la catastrophe. Le PDG Martel veut tout faire pour attirer au Québec des entreprises énergivores. Dans sa ligne de mire, les géants du web comme Facebook et Microsoft. Québec vend pour l'instant 450 MWh à des compagnies de serveurs informatiques. Dans quatre ans, l'objectif est de vendre 6 TWh, soit l'équivalent de près d'un million de foyers américains. (…). Avec l'arrivée des mineurs de cryptomonnaie, M. Martel estime qu'un autre 5 TWh pourrait s'ajouter* ". http://www.journaldequebec.com/2018/01/09/hydro-pourrait-se-lancer-dans-les-maisons-intelligentes

2.1.4 L'écosystème industriel et la communauté

L'écosystème industriel en cours de formation rapide dans le domaine des cryptomonnaies est aussi un élément majeur du sous-jacent du bitcoin. Loin des regards du grand public, de nombreuses sociétés se sont créées dans le monde entier depuis plusieurs années pour mettre en place les infrastructures et les services nécessaires au développement du bitcoin : entreprises de minage, plateformes d'échange, fabricant de *hardware wallets* (dont le leader mondial est la startup française Ledger (26)), cabinets de conseil, etc. Une des sociétés les plus en vue est Blockstream, qui regroupe certains des meilleurs développeurs et cryptographes au monde, et qui a réalisé en 2016 une levée de fonds de 55 M€ à laquelle a participé Axa (27). Cet écosystème crée des emplois, génère des revenus et stimule la recherche scientifique, effets qui sont systématiquement occultés dans les débats sur les cryptomonnaies.

Enfin, l'actif immatériel le plus difficile à percevoir, alors qu'il joue un rôle considérable pour constituer un réel sous-jacent du bitcoin, est **la communauté humaine qui s'est organisée en lien avec son écosystème industriel.** Il s'agit en premier lieu des " *early adopters* ", souvent des acteurs engagés qui voient dans Bitcoin un véritable projet de société et non pas seulement un support de spéculation. Alors que beaucoup d'entre eux sont devenus de potentiels multimillionnaires, leur mot d'ordre sur les réseaux sociaux est de ne pas vendre leurs bitcoins mais de les conserver (28), pour montrer leur confiance dans ce projet, alors même que le discours dominant dans les médias est que la " bulle " va s'effondrer.

Certains observateurs critiquent ces enrichissements soudains et estiment la distribution des bitcoins inégalitaire. Il est indéniable que l'avènement des cryptomonnaies et la hausse des cours entraînent un transfert de richesse en faveur des " *early adopters* ". Mais, d'une part, ce transfert n'est pas plus critiquable que les effets des politiques monétaires expansionnistes qui bénéficient à certaines catégories privilégiées, notamment à travers ce que la théorie économique désigne depuis longtemps comme " l'effet Cantillon " (du nom de l'économiste franco-irlandais du 17ème siècle) (29).

26. https://www.lesechos.fr/finance-marches/banque-assurances/0301165538086-bitcoin-ledger-leve-70-millions-de-dollars-2146015.php

27. *Les Echos*, 18/01/18 : https://www.blockstream.com/2016/02/02/blockstream-new-investors-55-million-series-a/

28. Ils emploient, de manière humoristique, l'expression " hodl ! ", en référence à un célèbre message de forum comportant une coquille dans son objet (" HODL " au lieu de " HOLD ").

29. Effet par lequel les premiers détenteurs de la monnaie nouvellement créée (les individus et entreprises bénéficiaires du crédit, les personnes rémunérées par la puissance publique et les titulaires de marchés publics) reçoivent cette monnaie avant l'élévation générale du niveau des prix qui découle de l'augmentation de la masse monétaire, ce qui améliore leur pouvoir d'achat relatif par rapport aux populations qui subissent par la suite cette inflation sans avoir perçu aussi tôt la monnaie nouvellement créée.

> ***Bitcoin est une plateforme : chacun peut s'y greffer, y entrer, y participer, l'enrichir ou en sortir sans contrainte. Il est comparable à des technologies comme Internet ou le mail***

D'autre part, les investisseurs précoces dans les cryptomonnaies ont pris un risque, ils ont réalisé un effort de compréhension dans un domaine complexe et nouveau. Les documents historiques déjà disponibles (30) montrent très bien que le développement du bitcoin a été très laborieux et précaire, et qu'il aurait très bien pu échouer rapidement, faute de soutien dans les premiers mois et les premières années. Ces *early adopters* ont même parfois connu des pertes financières importantes lors des piratages de plateformes qui ont rythmé les premières années du bitcoin (la plus spectaculaire étant Mt.Gox). Chacun de ces *hacks* a été l'occasion de faire évoluer les standards de l'écosystème Bitcoin et a contribué à améliorer sa sécurité, dont profitent aujourd'hui les nouveaux arrivants. Au total, l'investissement initial des *early adopters* a donc permis d'amorcer un processus qui bénéficie aujourd'hui à tous ceux qui souhaitent acheter des cryptomonnaies.

Outre ces particuliers passionnés, il faut aussi citer les développeurs qui entretiennent et mettent à jour le protocole, dans une gouvernance typique des logiciels libres et fort éloignée des structures centralisées et hiérarchisées des institutions traditionnelles. Cette communauté informelle, sans chef, fonctionnant sur la base du mérite et de la cooptation entre pairs qui ont démontré leur expertise et leur engagement, est habituellement appelée " Bitcoin Core ". Un de ses représentants les plus éminents est le cryptographe britannique Adam Back, PDG de Blockstream, et destinataire du premier message envoyé par Satoshi Nakamoto. Le recensement des contributions de chaque développeur au protocole Bitcoin (31) rappelle l'écrasante supériorité numérique et qualitative de cette communauté sur celles des autres cryptomonnaies.

Il existe, par ailleurs, une fondation Bitcoin, créée en 2012 pour promouvoir le bitcoin. Elle n'a toutefois absolument aucun pouvoir sur le système et son influence globale est limitée. La blockchain Ethereum bénéficie également d'une communauté très nombreuse et active, coordonnée par une fondation de droit suisse détentrice des fonds levés en 2014. Cette entité et ses principaux développeurs ont, eux, une forte influence sur le système Ethereum.

30. Par l'exemple l'excellent POPPER, Nathaniel, *Digital Gold*, HarperCollins, 2015

31. Notamment sur les sites suivants : https://github.com/bitcoin/bitcoin/graphs/contributors et https://bitcoin.team

Toutes choses égales par ailleurs, le développement des *altcoins* et les potentielles nouvelles *hard forks* pourraient, en théorie, affaiblir Bitcoin en détournant à leur profit une partie de cette communauté. Mais ce n'est pas ce qui a été observé jusqu'à présent. Il y a évidemment eu des transferts vers ces nouvelles blockchains, mais pas autant que certains avaient pu le craindre. S'il est relativement aisé de copier l'algorithme Bitcoin, de le modifier et de proposer une nouvelle cryptomonnaie, il est beaucoup plus difficile de convaincre cette vaste communauté de se détourner du bitcoin et d'adopter la nouvelle proposition. Non pas que cette communauté soit " captive " en raison de son investissement passé ou de contrainte techniques ou commerciales : Bitcoin est un système ouvert où entrer comme sortir est très facile. Outre la confiance dans une équipe de développeurs qui a fait ses preuves, il y a simplement une forme d'engagement profond, aux motifs variables (philosophiques, économiques, etc.), qui contribue très nettement à une forme de sous-jacent du bitcoin.

Il convient d'insister sur le fait que **Bitcoin est une plateforme : chacun peut s'y greffer, y entrer, y participer, l'enrichir ou en sortir sans contrainte**. Il est comparable à des technologies comme Internet, le mail (SMTP) ou voix sur IP (VoIP). Bitcoin n'est pas centralisé et ne possède pas d'entité de contrôle. Comme le résume l'un des meilleurs analystes mondiaux du bitcoin, *" Bitcoin introduit une plateforme sur laquelle vous pouvez faire fonctionner une monnaie comme une application, sur un réseau sans aucun point de contrôle central, un système complètement décentralisé comme Internet lui-même. Ce n'est pas une monnaie pour Internet, mais plutôt l'Internet de la monnaie " (32).*

D'ailleurs, à la différence de certaines de ses cryptomonnaies concurrentes, et surtout à la différence du système bancaire, **Bitcoin n'a ni budget de communication, ni plan marketing, ni stratégie d'influence, ni cabinet de lobbying (33).** Il doit l'essentiel de sa progression au travail intense, spontané et bénévole de nombreux développeurs, depuis des années. Certains d'entre eux possèdent des bitcoins et peuvent voir leurs efforts récompensés à long terme si le cours augmente, mais cette rémunération est indirecte, incertaine, et souvent secondaire dans leurs motivation (entre 2009 et 2016, rares furent ceux qui imaginaient que le cours progresserait autant que depuis mi-2017).

32. ANTONOPOULOS, Andreas, *The Internet of Money, volume two*, Merkle Bloom, 2017

33. Certes, la société Blockstream a des actionnaires, des moyens, une influence, mais son poids est maintenant relativement limité dans l'écosystème Bitcoin en expansion croissante.

Par ailleurs, comme Facebook, mais aussi comme Internet, **Bitcoin bénéficie d'un fort effet de réseau**, cette externalité économique positive qui fait que la valeur d'un système augmente de manière exponentielle avec le nombre de ses utilisateurs (34). Toutefois, la nouveauté majeure de Bitcoin par rapport à Internet est que chacun peut, en quelque sorte, acheter des parts de ce protocole, en anticipant le fait que ce réseau se développera, rendra des services à l'humanité et prendra donc de la valeur. Bitcoin est donc à la fois un logiciel libre et un réseau dont les unités de compte sont mises en vente et ont une valeur de marché.

En apparence, il s'agit d'une forme de " marchandisation ", mais l'intérêt essentiel de cette mise en vente est qu'elle permet à la multitude de s'approprier cet actif et d'éviter le sort d'Internet dont la technologie a été progressivement pillée et accaparée par les grands acteurs que sont les GAFA et les États. On peut espérer que l'équivalent de cette centralisation du web par les " serveurs sirènes " (35) (Google, Apple, etc.) ne se produise pas avec Bitcoin, même s'il convient de rester prudent : son réseau est encore très récent et il est inévitablement soumis à certaines tendances centralisatrices (économies d'échelle, spécialisation des tâches, effets réseau de certains acteurs comme les exchanges ou les sociétés de minage).

> ***Bitcoin bénéficie d'un fort effet de réseau, une externalité économique positive qui fait que la valeur d'un système augmente de manière exponentielle avec le nombre de ses utilisateurs***

En conclusion, ces éléments montrent que l'idée que " le bitcoin ne repose sur rien " ne repose elle-même sur… rien. En revanche, de nombreuses cryptomonnaies créées sans ce sous-jacent technologique, industriel et humain ne reposent, elles, sur pas grand-chose. Elles font d'ailleurs l'objet de tensions spéculatives bien plus intenses que le bitcoin. Quant aux monnaies étatiques, leur " sous-jacent " est surtout la contrainte.

34. La loi de Metcalfe, énonce notamment que l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs.

35. LANIER, Jaron, *Internet : qui possède le futur ?*, Le Pommier, 2014

2.2 Les monnaies étatiques ne reposent plus que sur l'autorité

36. Zweig, Stefan, *Le Monde d'hier. Souvenirs d'un européen*, Belfond, 1982

Dès la première page de sa célèbre autobiographie, Stefan Zweig se souvient avec nostalgie de la quiétude qui caractérisait toute la société avant la Première Guerre Mondiale. Il n'hésite pas à inclure, dans les causes de ce qu'il appelle " l'âge d'or de la sécurité ", la solidité du système monétaire : "*notre monnaie, la couronne autrichienne, circulait en brillantes pièces d'or et nous assurait ainsi de son immutabilité* ". A contrario, il cite, dans sa préface, l'altération de la qualité de la monnaie parmi les pires maux qui puissent affecter l'humanité : " *tous les chevaux livides de l'Apocalypse se sont rués à travers mon existence : révolution et famine, dévalorisation de la monnaie et terreur, épidémies et émigration* " (36). Quelle est la qualité des monnaies régaliennes contemporaines et quel sort les attend ? Depuis 1971, elles ne reposent fondamentalement sur rien à part la contrainte, et depuis 2008 les politiques monétaires créent des risques préoccupants qui ne font que dégrader la confiance dans les monnaies nationales et renforcer l'intérêt pour le bitcoin et les cryptomonnaies.

2.2.1 Depuis 1971, les monnaies nationales n'ont pas de réel sous-jacent

Si la monnaie est une des institutions les plus anciennes de la civilisation et l'un des objets les plus courants de la vie quotidienne, qui peut être certain de bien comprendre ce qu'elle est fondamentalement ? Et n'est-il pas étonnant que les règles régissant sa création ne soient jamais enseignées à l'école, et que même de nombreux étudiants en économie ou banquiers ne les connaissent pas ?

Une monnaie ayant cours légal ne peut être refusée en règlement d'une dette : tout créancier ou commerçant a le devoir de l'accepter. Le droit positif détermine quelle unique monnaie est autorisée pour le règlement des impôts. **Dans nos sociétés qui se disent libres, la monnaie est imposée par la loi : les individus ne sont pas libres de choisir dans quelle monnaie ils peuvent effectuer leurs transactions**. La contrefaçon ou falsi-

fication de pièces ou billets est d'ailleurs souvent beaucoup plus lourdement punie que des crimes comme le viol, la torture ou les actes de barbarie (37).

Indépendamment de cet aspect juridique (et outre certains aspects symboliques et anthropologiques également intéressants), il y existe une essence économique de la monnaie. Pour la comprendre, il faut recourir aux instruments de la science économique.

Les conditions historiques de l'émergence de la monnaie font encore l'objet de débats académiques. Les manuels d'économie expliquent presque systématiquement que les hommes ont d'abord recouru à l'échange par le troc, puis ont inventé la monnaie comme intermédiaire d'échange pour surmonter ses deux limitations que les économistes appellent aujourd'hui la " non-coïncidence des besoins " et la " non-divisibilité des biens ". Cette vision des choses a été contestée avec certains arguments intéressants (38).

Deux éléments fondamentaux semblent toutefois certains. D'une part, en dehors du rôle joué ponctuellement par certains États, notamment pour organiser l'économie de leurs armées, **l'apparition et le développement de la monnaie ont constitué un processus social spontané**. D'autre part, l'existence d'un intermédiaire d'échange a permis le développement du commerce entre personnes ne se connaissant pas (39), puis une spécialisation économique progressive et une division du travail sans lesquelles le décollage économique exceptionnel des derniers siècles n'aurait jamais eu lieu.

Pour choisir ces intermédiaires d'échanges, les hommes ont recherché en priorité des biens possédant certaines qualités : solidité, divisibilité, transportabilité, homogénéité, relative rareté, etc. Ils ont d'abord utilisé toutes sortes d'objets et de matières : galets, grains de maïs, plumes, tabac, coquillages, pierres précieuses, etc. Ce sont les métaux précieux qui se sont ensuite naturellement imposés car ils étaient les seuls à réunir un maximum des qualités nécessaires. Pendant des siècles, pratiquement toutes les monnaies du monde ont été reliées, d'une manière ou d'une autre, à des métaux précieux. La valeur de chaque monnaie nationale était directement liée aux stocks d'or présents dans chaque pays, eux-mêmes dépendant à la fois du rythme d'extraction et de l'évolution de la balance commerciale.

37. C'est le cas en France, où le code pénal prévoit les condamnations suivantes : " *la contrefaçon ou la falsification des pièces de monnaie ou des billets de banque ayant cours légal en France ou émis par les institutions étrangères ou internationales habilitées à cette fin est punie de trente ans de réclusion criminelle et de 450 000 euros d'amende* " (article 442-1) ; " *le viol est puni de quinze ans de réclusion criminelle* " (article 222-23) ; " *le fait de soumettre une personne à des tortures ou à des actes de barbarie est puni de quinze ans de réclusion criminelle* " (article 222-1)

38. GRAEBER, David, *Dette, 5 000 d'histoire*, Babel, 2013

39. " *Le scénario du troc cher aux économistes est peut-être absurde quand on l'applique aux transactions entre voisins dans un petit village rural, mais s'il s'agit d'une transaction entre un habitant d'un de ces villages et un mercenaire de passage, il devient soudain tout à fait sensé* ". Graeber, David, *Dette, 5 000 d'histoire*, Babel, 2013 (page 262)

La situation a radicalement changé quand, le 15 août 1971, le président américain Nixon a suspendu la convertibilité du dollar en or (40). Depuis cette date, les monnaies n'ont plus aucun " sous-jacent " au sens strict. En suspendant la convertibilité en or du dollar, Nixon a mis fin au système appelé " étalon de change-or " issu de Bretton Woods en 1944. Comme le résume l'économiste **Pascal Salin,** *" désormais on se trouvait, pour la première fois dans l'histoire, dans une situation où la monnaie n'avait plus de définition en termes réels (en or ou en argent ou en termes de tout autre bien) ! 1 dollar n'avait plus d'autre définition que d'être un dollar, 1 livre une livre, 1 franc un franc, etc. Il devenait clair que l'expansion monétaire n'avait plus aucune limite et que la politique monétaire pouvait évoluer au gré des décisions des autorités monétaires " (41).*

Aujourd'hui, la valeur de la monnaie au sens général (non son cours quotidien) ne dépend plus fondamentalement que de la confiance du public. Celle-ci se fonde sur une perception diffuse de la " puissance économique " des États, notamment leur capacité de lever l'impôt, mais elle est en réalité extrêmement fragile. **L'affirmation souvent répétée dans les médias, selon lesquelles les monnaies étatiques ont au moins pour sous-jacent l'économie de leurs États est en réalité extrêmement vague** et n'est d'ailleurs jamais expliquée et étayée en détails.

40. Décision complétée par les accords de la Jamaïque, qui ont fait suite à la réunion des 7 et 8 janvier 1976 du comité intérimaire du Fond monétaire International à Kingston

41. SALIN, Pascal, *Les Systèmes monétaires, des besoins individuels aux réalités internationales*, Odile Jacob, 2016

2.2.2 Depuis 2008, les politiques monétaires créent de nouveaux risques

Depuis 2008, la monnaie est créée pratiquement sans limites. Les politiques monétaires ultra-expansionnistes du *quantitative easing* ont fait exploser les masses monétaires dans des proportions jamais vues en temps de paix. Elles font penser à ce que Milton Friedman avait appelé, pour dénigrer les politiques de relances monétaires keynésiennes, de l'" *helicopter money* ", c'est-à-dire des tombereaux de monnaie déversés sans limites sur la planète.

Ces politiques répondent à une tentation permanente du pouvoir politique, déjà mise en évidence avec humour par le grand économiste français **Frédéric Bastiat** en 1849 : *" Quand les législateurs, après avoir ruiné les hommes par la guerre et l'impôt, persévèrent dans leur idée, ils se disent : " Si le peuple souffre, c'est qu'il n'a pas assez d'argent. Il en faut faire. " Et comme il n'est pas aisé de multiplier les métaux précieux, surtout quand on a épuisé les prétendues ressources de la prohibition, " nous ferons du numéraire fictif, ajoutent-ils, rien n'est plus aisé, et chaque citoyen en aura plein son portefeuille ! ils seront tous riches " (42).*

Elles ont, de nos jours, facilité une explosion de l'endettement dans le monde. La dette brute mondiale est passée de 210% du PIB mondial avant la crise de 2008 à 250%, un niveau que beaucoup d'économiste pensent insoutenable, surtout dans la perspective d'une possible remontée des taux d'intérêt (43).

En attendant, la banalisation des taux d'intérêt négatifs a des conséquences dangereuses pour l'économie, comme le résume l'économiste **Cécile Philippe :** *" l'aplatissement/déformation de la courbe des taux rend illisible le risque lié à l'investissement pour les entreprises ; l'accoutumance à l'endettement public reporte le problème vers le futur avec des entreprises qui dépendent de plus en plus du soutien public et s'éloignent du service rendu aux consommateurs dans le cadre d'un calcul économique sain ; les taux faibles rendent très fragiles des industries spécialisées dans la protection conte les aléas de la vie,*

42. BASTIAT, Frédéric, " Maudit Argent ", in *Journal des Economistes*, 15 avril 1849 http://bastiat.org/fr/maudit_argent.html

43. World Economic Forum, 20/12/17 : https://www.weforum.org/agenda/2017/12/we-could-be-facing-a-major-debt-crisis?utm_content=bufferb3f05&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

44. Institut Economique Moliari, 06/04/16 : http://www.institutmolinari.org/banalisation-des-taux-d-interets,2551.html

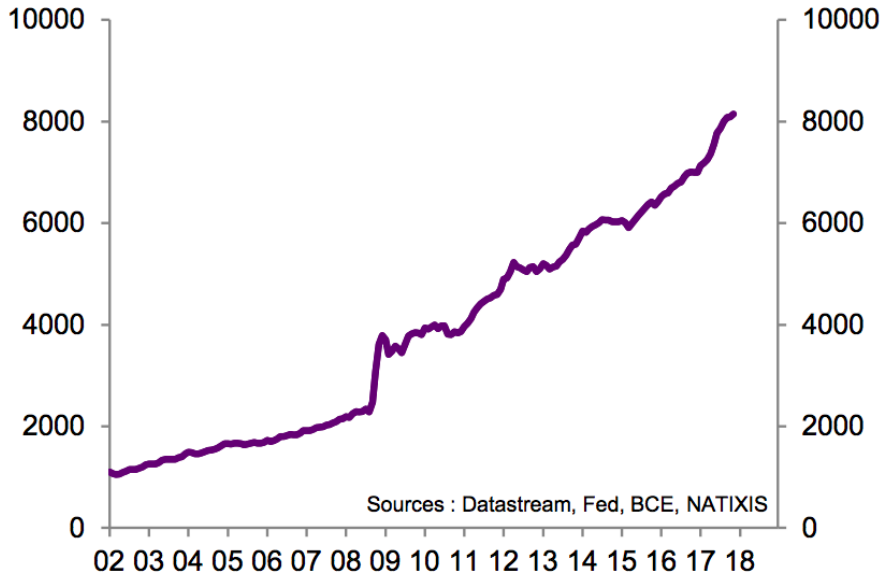
45. Natixis, *Le Monde n'arrive pas à discipliner sa liquidité : ça pourrait mal finir*, Flash Economie 02/01/18

46. Cité par Pascal Salin, *Contrepoints*, 10/12/14 : https://www.contrepoints.org/2014/12/10/190838-prix-nobel-deconomie-40-ans-apres-hayek-et-la-monnaie

en particulier, les assureurs ; c'est la japonisation de nos économies " (44).

Depuis le début des années 2000, la base monétaire des États-Unis et de la zone Euro a atteint des niveaux exceptionnels en valeur, comme le montre le graphique suivant. La base monétaire mondiale est passée d'environ 12% du PIB en 2002 à 32% aujourd'hui (45). Ce graphique est à comparer avec celui, apparaissant dans la partie 1, du rythme d'émission du bitcoin, qui est exactement inverse, avec une production monétaire qui plafonne en volume, et un taux de croissance monétaire qui chute au cours du temps.

États-Unis + Zone euro : base monétaire (Mds de $)



Source : Natixis, Flash Economie 02/01/18

Hayek et les théoriciens de l'école autrichienne ont depuis longtemps analysé en détails les conséquences négatives des tentatives de relance de l'économie par la politique monétaire : " combattre la dépression par une expansion forcée de crédit, c'est essayer de guérir un mal par les moyens mêmes qui l'ont provoqué; parce qu'on souffre d'une mauvaise orientation de la production, on veut renforcer celle-ci : cette manière de procéder ne peut conduire qu'à une crise beaucoup plus sévère dès que l'expansion de crédit vient à s'arrêter " (Hayek) (46).

> *Nul besoin d'avoir reçu un prix Nobel d'économie pour pressentir que, lorsque l'argent ne coûte rien, on ne peut faire que des bêtises*

Même de plus en plus d'économistes contemporains étrangers à ce courant d'idées s'inquiètent aussi des multiples effets pervers engendrés par ces politiques monétaires : bulles sur les marchés d'actifs, spéculation, risques d'inflation, perturbation du calcul économique des entreprise, déclenchement cycles économiques artificiels.

Par exemple : *" l'excès de liquidité mondiale continue à s'aggraver, avec l'incapacité des Banques Centrales à le résorber. Les conséquences de l'excès de liquidité annoncent les crises futures : bulles sur les prix des actifs en particulier bulle obligataire de grande taille qu'un choc inflationniste pourrait faire exploser ; accumulation d'actifs risqués dans les portefeuilles des investisseurs, ce qui pourrait conduire à une crise de ces investisseurs en cas de récession faisant apparaître une réévaluation des primes de risque " (47).* La politique monétaire de la Banque Centrale Européenne est particulièrement critiquable : en restant expansionniste alors que l'économie s'améliore, elle crée de nouveaux déséquilibres et de nouveaux risques particulièrement inquiétants (48).

S'agissant des conséquences inflationnistes des politiques monétaires contemporaines, même si elles sont souvent niées, elles sont bien réelles (cf. encadré suivant).

47. Natixis, *Le Monde n'arrive pas à discipliner sa liquidité : ça pourrait mal finir*, Flash Economie 02/01/18

48. Natixis, *Les cinq raisons pour lesquelles on peut critiquer la politique monétaire restée expansionniste de la BCE*, Flash Economie 03/01/18

Les conséquences inflationnistes du Quantitative Easing

> *" L'inflation s'observe à travers la hausse généralisée des prix mais* ***quid*** *de l'inflation, résultat de la non-déflation ou inflation négative ? En effet, ce thème n'est jamais abordé par les spécialistes, pourtant il mériterait qu'on y accorde une attention particulière.* ***Les politiques monétaires de Quantitative Easing ont eu comme principal résultat d'empêcher la baisse massive du prix des actifs sous-jacents à la crise des subprimes et par conséquent de limiter la baisse du niveau général des prix*** *atténuant la gravité de la récession. En effet, au regard de la sévérité de la crise, la déflation n'a presque pas eu lieu aux États-Unis. Le soutien artificiel apporté par ces politiques n'a pas permis " la purge " de l'économie US. Le problème est que des ressources " mal employées " le sont restées au lieu d'être libérées pour d'autres utilisations.*
>
> *De même,* **le maintien de la politique de *Quantitative Easing* a aggravé la mauvaise allocation des ressources** *puisqu'elle maintient le taux d'intérêt à des niveaux artificiellement bas et le prix des actifs artificiellement élevés. Le processus de désendettement à l'œuvre aujourd'hui est justement une tentative graduelle des entreprises d'assainir leurs bilans qu'elles savent surévalués du fait de la politique monétaire ".* **Institut Economique Molinari, 18/04/16 (49)**

49. http://www.institutmolinari.org/l-helicopter-money-jusqu-ou-ira-le,2553.html

50. ARTUS, Patrick, VIRARD, Marie-Paule, *La Folie des banques centrales*, Fayard, 2017

L'essor des cryptomonnaies se nourrit en partie des inquiétudes macroéconomiques causées par la perte de contrôle des politiques monétaires contemporaines dont les effets ont jusqu'ici été beaucoup plus favorables aux marchés financiers qu'à la croissance économique et à l'emploi. Plutôt que de bulle des cryptomonnaies, on devrait parler de bulle sur les marchés financiers et d'effondrement des monnaies étatiques par rapport à leurs concurrentes des différentes blockchains.

Comme le résume un livre dénonçant *La Folie des banques centrales*, *" nul besoin d'avoir reçu un prix Nobel d'économie pour pressentir que, lorsque l'argent ne coûte rien, on ne peut faire que des bêtises " (50).* Les auteurs concluent d'ailleurs leur ouvrage par une question cruciale : " en démocratie, est-il vraiment raisonnable de concentrer autant de pouvoirs entre les mains d'une institution exempte de tout contrôle démocratique réel et sérieux sur ses décisions ? ".

La réponse des promoteurs du bitcoin est que la monnaie est une affaire trop sérieuse pour être confiée à quelques bureaucrates irresponsables.

2.2.3 Quelle pérennité pour les monnaies nationales ?

Dans les économies développées, on a aujourd'hui largement perdu de vue une notion pourtant classique en science économique, celle de " monnaie saine " (" sound money "). La monnaie peut pourtant être de plus ou moins bonne qualité, c'est-à-dire réunir plus ou moins de caractéristiques propres à satisfaire les besoins de ses utilisateurs ; et le monopole dans ce domaine produit les mêmes effets pervers, au détriment du consommateur, que dans tout autre secteur (51).

La qualité des monnaies nationales est en diminution constante. Alors qu'elles ne reposent sur rien depuis 1971, qu'elles sont produites sans limites depuis 2008, et donc que leur fonction de réserve de valeur de long terme est sérieusement compromise, qu'est-ce qui leur permet de se maintenir ?

Comme le résume l'économiste **Pascal Salin,** *" jamais, dans toute l'histoire humaine, la monnaie n'a été aussi mal gérée, jamais elle n'a perdu aussi rapidement de sa valeur, jamais il n'y a eu autant de crises monétaires et de crises de change qu'au XXème siècle, siècle au cours duquel la monnaie a été nationalisée, où elle a été produite par des monopoles nationaux et publics. Devant une telle évidence, il est stupéfiant que l'on puisse continuer à dire qu'il est, par nature, du rôle de l'État de veiller à la stabilité monétaire et que la production monétaire constitue nécessairement un attribut de la souveraineté ! " (52).*

Ce paradoxe peut s'expliquer par les quatre faits suivants.

Premièrement, les gouvernements imposent l'emploi de leur monnaie *fiat* pour le paiement des impôts. En quelque sorte, ces monnaies sont les seules à permettre d'acheter la possibilité de ne pas être poursuivi par l'administration fiscale. Cela leur confère presque un sous-jacent symbolique ou juridique. Mais ce dernier ne garantit en rien le maintien de leur valeur : toute l'histoire

51. La monnaie est un bien économique qui fait l'objet d'une production, plus ou moins coûteuse, et d'une demande. Sa différence majeure par rapport à un bien économique standard est que l'augmentation de sa production ne contribue pas à une augmentation du bien-être social : en diminuant la valeur relative de chaque unité, cette augmentation dégrade la fonction de réserve de valeur de la monnaie. En revanche, comme pour tout autre bien économique, la monopolisation de sa production risque d'entraîner une baisse de sa qualité – ce qui arrive notamment si la production est accrue pour des raisons politiques ou sur la base de raisonnements économiques erronés – tandis que la concurrence a les mêmes effets que dans tout autre domaine : baisse du coût de production et augmentation de la qualité.

52. SALIN, Pascal, Libéralisme, Odile Jacob, 2000 (page 435)

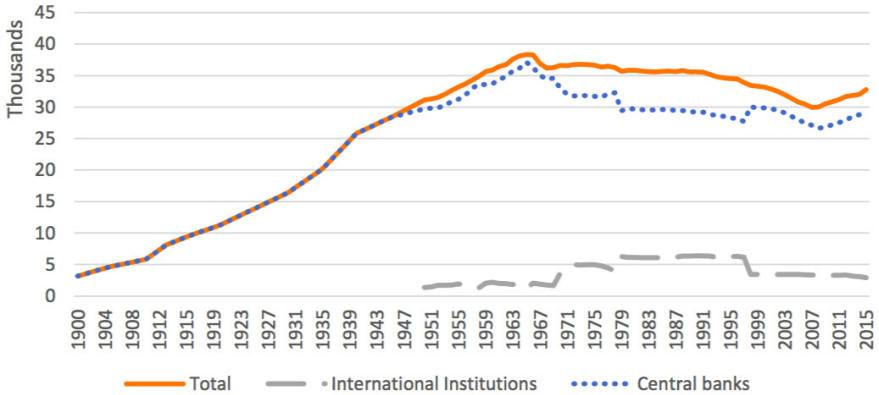
monétaire du 20ème siècle montre que des monnaies nationales peuvent brusquement perdre leur valeur dans des proportions considérables et ruiner des millions d'épargnants sans que les pouvoirs publics ne puissent rien y faire. Le fait qu'elles servent à payer l'impôt ne les protège pas du risque d'effondrement.

Deuxièmement, les États régulent étroitement les systèmes bancaires et imposent aux banques de n'ouvrir des comptes et de n'effectuer des transactions que dans ces monnaies nationales, ce qui confère à ces dernières un avantage compétitif par rapport à n'importe quel autre type de monnaie.

Troisièmement, dans la plupart des pays, le cours légal implique que personne ne peut refuser un paiement de dette effectué avec une monnaie nationale.

Enfin, et c'est assez paradoxal, les États, à travers leurs banques centrales, conservent d'importants stocks d'or pour maintenir la valeur de leur monnaie en cas de crise majeure, alors même que nous avons quitté l'étalon de change-or il y a presque un demi-siècle. Les réserves officielles des banques centrales et institutions internationales ont même tendance à remonter depuis 2008, après avoir diminué depuis le milieu des années 1960, comme le montre le graphique suivant.

Réserves officielles d'or, 1900-2015 (en tonnes)



Source : World Gold Council, Reserve Statistics (53)

L'or est désormais presque unanimement considéré chez les économistes comme une " relique barbare ", selon l'expression de Keynes. Il n'a aucun rôle officiel dans le système monétaire international actuel. Il n'y a aucun lien entre les réserves d'or et les monnaies nationales. Pourtant, les banques centrales éprouvent toujours le besoin de conserver ces stocks, comme pour donner une apparence de sous-jacent ou de garantie à des monnaies qui en sont largement dépourvues. Et une partie de l'opinon publique et des commentateurs se laisse piéger par cette apparence.

53. https://www.gold.org/data/gold-reserves. Cité in AMMOUS Saifedean, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley, 2018

La perception par le grand public de la qualité de la monnaie

> *“ Si le grand public parvenait à comprendre le prix qu'il paie en termes d'inflation récurrente et d'instabilité pour le seul bénéfice que confère la facilité d'une monnaie unique dans les transactions ordinaires, et pour ne pas avoir à envisager de temps à autre l'usage d'une monnaie non familière, il trouverait certainement ce prix fort excessif (...).*
>
> ***De tout temps, les gouvernements ont eu intérêt à persuader le grand public que le droit d'émettre la monnaie leur appartenait en exclusivité.*** *Aussi longtemps que, pour des raisons pratiques, cela impliquait l'émission de pièces d'or, d'argent ou de cuivre, cela n'avait pas autant d'importance que cela en a aujourd'hui, à l'heure où nous savons qu'il existe bien d'autres types de supports monétaires, le papier en premier lieu, que les gouvernements sont moins aptes à gérer, et plus prompts à en abuser que des monnaies métalliques ”.*
>
> **Friedrich Hayek,** *Pour une vraie concurrence des monnaies (The Denationalization of Money, 1976)* **(54)**

54. HAYEK, Friedrich, *Pour une vraie concurrence des monnaies*, PUF, 2015 (page 33)

En conclusion, s'il existe aujourd'hui des monnaies que l'on peut qualifier de “ virtuelles ”, les monnaies étatiques sont sans doute les plus qualifiées pour mériter ce titre. Elles sont créées à partir de rien et leur production semble ne plus avoir aucune borne, ce qui inquiète d'ailleurs un nombre croissant d'économistes dans le monde entier. Il en va tout autrement du bitcoin, en dépit des contre-vérités forgées et colportées sur ce sujet.

Une partie de l'explosion de son cours s'explique d'ailleurs probablement par cette double prise de conscience du grand public et de quelques grands acteurs de la finance : tandis que les monnaies nationales sont fragilisées par leur sous-jacent incertain et par les politiques monétaires actuelles qui menacent leur pérennité, le bitcoin possède un sous-jacent solide, issu de la sécurité fournie par son protocole et de l'écosystème industriel et humain qui le soutient, et son rythme de création est prévisible et décroissant.

3. Une monnaie en devenir

3.1 De réserve de valeur à moyen d'échange

Les progrès technologiques nécessaires pour permettre au bitcoin de devenir une monnaie " normale " seront probablement plus longs que certains ne l'espéraient, et les défis à relever sont sérieux. Mais l'innovation dans ce domaine est permanente ; c'est son rythme qui doit être pris en compte, et non simplement la situation actuelle du bitcoin, encore monnaie en devenir.

3.1.1 Réserve de valeur et spéculation

Certains économistes estiment que le bitcoin ne peut pas être une monnaie car il ne satisfait pas au " théorème de régression " énoncé par Ludwig von Mises, qui prouve qu'une monnaie, avant d'avoir une valeur d'échange, a nécessairement une valeur d'usage (1) (cf. encadré suivant).

1. Il ne s'agit pas d'une hypothèse historique mais d'une décomposition analytique fondée sur la logique, et dont la réfutation ne peut donc être tentée que par la logique. https://fee.org/articles/what-gave-bitcoin-its-value/

Le théorème de régression de Mises

> *“ Considérons d’abord une monnaie marchandise, comme l’or. J’accepte de l’or comme paiement à un instant t si à l’instantt-1, j’ai constaté le pouvoir d’achat qu’il possédait. Les personnes qui l’ont accepté comme paiement à l’instant t-1 l’ont fait parce qu’ils ont constaté qu’à l’instant t-2, l’or avait un pouvoir d’achat. Ainsi de suite, en remontant jusqu’à la première utilisation de l’or comme monnaie, on trouve que la première personne qui l’a accepté comme paiement ne l’a fait que parce qu’elle avait constaté que l’or servait à un certain nombre d’usages valorisés par d’autres personnes. Ainsi, le théorème de régression affirme que toute monnaie tire sa valeur de son utilisation non monétaire. Ceci est aussi valable pour les monnaies décrétées : l’euro vient du franc, de la lire, etc. qui eux-mêmes étaient grosso modo échangeables contre de l’or jusqu’en 1971 ”.*
>
> **Brice Rothschild,** *Contrepoints*, **06/11/13 (2)**

2. https://www.contrepoints.org/2013/11/06/145305-theoreme-de-regression-et-bitcoin

En réalité, on peut considérer que le bitcoin satisfait bien à ce critère. Les premiers bitcoins ont été émis le 9 janvier 2009. Le premier prix en bitcoin a été posté neuf mois plus tard, le 5 octobre 2009 (1 dollar pour 1 309,03 bitcoins). Que s’est-il passé entre ces deux dates ? Pendant ces quelques mois, des passionnés, informaticiens, cryptographes, entrepreneurs, libertariens, cypherpunks et activistes en tous genres se sont emparé de ce réseau, s’y sont intéressés, y ont trouvé une valeur technique et philosophique, et ont échangé entre eux des bitcoins de manière gratuite. A mesure que le nombre de ces utilisateurs augmentait, la demande de bitcoins s’est renforcée jusqu’à atteindre un niveau permettant à ce jeton numérique d’être échangé contre des biens réels, lui conférant ainsi un rôle d’intermédiaire d’échanges et une valeur monétaire. Cette reconstitution montre qu’avant d’avoir une valeur d’échange, il a bien eu une valeur d’usage.

En revanche, qu’en est-il de son utilisation actuelle ? **Le bitcoin sert encore très peu d’unité de compte**. Il a cette fonction pour les ICO qui sont libellées en bitcoins. Et le fait que certaines entreprises commencent à proposer à leurs salariés d’être payés en bitcoins va sans doute contribuer à développer cette fonction.

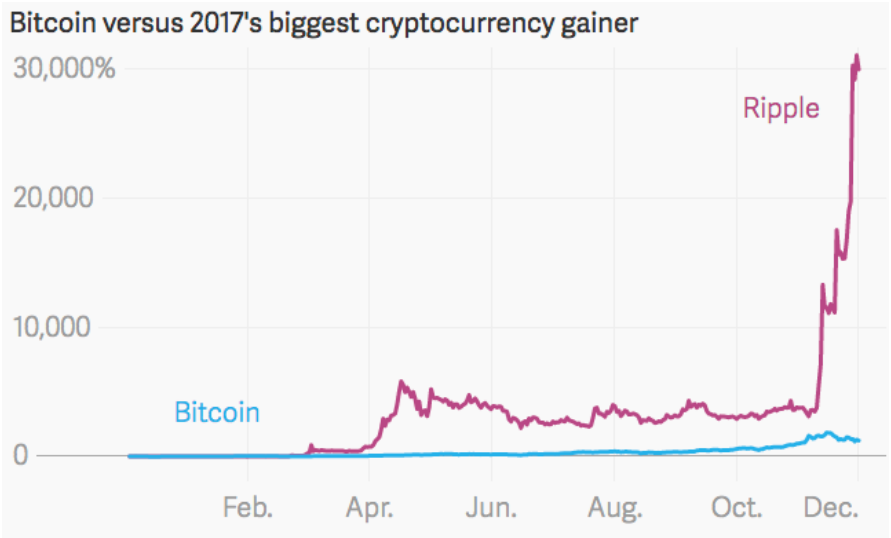
Le bitcoin est encore très peu utilisé comme moyen d’échange, surtout depuis l’explosion de son cours et des frais de transaction qui incitent à le thésauriser, même si le nombre

de commerce (physiques ou en ligne) qui l'acceptent ne cesse de progresser (3) : par exemple, au Japon, où le bitcoin a reçu un statut de moyen de paiement officiel, des dizaines de milliers de commerce sont prêts à l'accepter, dès que les frais de transaction auront diminué.

Depuis quelques années, certains analystes annoncent que l'usage du bitcoin et des cryptomonnaies se répandra en priorité dans les pays en développement, où les systèmes politiques, bancaires et monétaires sont particulièrement défaillants. D'après eux, avec la prévisible explosion du nombre de smartphones dans ces régions, plusieurs milliards de personnes supplémentaires auront bientôt, la possibilité, grâce aux cryptomonnaies, de devenir leur propre banque ; l'essor fulgurant de M-Pesa au Kenya (4) préfigurerait ce type d'évolution. Ce phénomène ne s'est pas encore produit, notamment en raison des limites actuelles du réseau Bitcoin. Il figure toujours parmi les scenarios possibles pour l'avenir.

Le bitcoin sert, en revanche, de plus en plus comme réserve de valeur, et cela malgré sa forte volatilité. Le fait que, sur longue période, et malgré des chutes brutales, son cours ait tendance à s'apprécier encourage de plus en plus d'utilisateurs à stocker de la valeur en bitcoins. Contrairement aux autres monnaies, la production du bitcoin est totalement inélastique à la demande ; les effets des variations de cette dernière sur son cours ne peuvent donc pas facilement être lissés. Sa volatilité de court terme est donc, en quelque sorte, un prix à payer pour son appréciation sur le long terme.

A titre de comparaison, la volatilité considérable du cours du Ripple, cryptomonnaie largement centralisée (5), n'a suscité chez les commentateurs aucune des critiques, alertes et préoccupations exprimées au sujet du bitcoin, alors qu'elle a été incomparablement plus forte, comme le montre le graphique suivant (6).



3. Des sites listent ces commerces, un peu comme, au début du web, au milieu des années 1990, Yahoo tenait à jour des listes de sites par catégories. Par exemple, pour la France : https://bitcoin.fr/depenser-ses-bitcoins/

4. *Jeune Afrique*, 03/04/17 : http://www.jeuneafrique.com/mag/421063/economie/mobile-banking-success-story-nommee-m-pesa/

5. *The New York Times*, 04/01/18 : https://www.nytimes.com/2018/01/04/technology/bitcoin-ripple.html

6. *Cointelegraph*. https://cointelegraph.com/news/the-cream-of-the-crypto-crop-10-best-performing-assets-in-2017

7. MALBRANQUE, Benoit, " Spéculations et marchés financiers ", in *Libres ! 100 auteurs, 100 idées*, Rouget, 2012 https://www.catallaxia.org/wiki/Beno%C3%AEt_Malbranque:Sp%C3%A9culation_et_March%C3%A9s_Financiers

Plus généralement, la spéculation est un phénomène plus positif que ce que l'on croit souvent : outre son impact positif pour le renforcement de la sécurité du réseau et pour le financement de l'innovation en matière de protocole (cf. partie 2), elle a aussi des vertus insoupçonnées de stabilisation économique, comme l'ont rappelé de nombreux économistes à travers les siècles (cf. encadré suivant).

Les vertus de la spéculation

> *« C'est souvent à l'occasion des bulles ou des hausses spectaculaires du prix de certains actifs qu'on incrimine la spéculation. En réalité, par le mécanisme qu'elle induit, la spéculation provoque précisément l'effet inverse, de sorte qu'en des temps difficiles, les hommes politiques devraient davantage encourager que contraindre la spéculation. Ainsi, alors que le spéculateur est toujours désigné comme le coupable des hausses fulgurantes des prix, celles-ci auraient été bien plus importantes en son absence. (...)*
>
> *En " profitant ", par " égoïsme ", des opportunités " d'enrichissement personnel " qui se présentent à lui, en achetant le bien ou l'actif lorsqu'il est excessivement bon marché (donc peu demandé et fortement offert) et en le revendant lorsque son prix atteint des sommets (et qu'il est devenu très demandé et peu offert), le spéculateur agit comme un régulateur naturel, plus efficace qu'aucun gouvernement ne saura jamais l'être. En aplanissant les fluctuations des prix, il réalise une action éminemment vertueuse : il permet de stocker les biens pendant l'abondance, et de les distribuer lors de pénuries. Des vaches grasses puis des vaches maigres : tel est le monde sans les spéculateurs ".*
>
> **Benoit Malbranque,** *Libres,* **2011 (7)**

3.1.2 Limite des 21 millions et caractère déflationniste

Il convient tout d'abord d'écarter un " faux inconvénient », celui de la limitation du volume de bitcoins émis. Dans un scénario très hypothétique, si le bitcoin devait être utilisé comme monnaie universelle, le fait que son volume total soit limité ne perturberait en rien le fonctionnement des échanges. La science économique prouve que n'importe quel volume de monnaie peut convenir pour assurer le fonctionnement des échanges. L'ajustement se fait par les prix. Ce qui

compte, c'est que cette monnaie soit suffisamment divisible, pour le cas où sa valeur unitaire augmenterait beaucoup : ainsi, des échanges de petits montants restent possibles. Or le bitcoin est un million de fois plus divisible que le Dollar ou l'Euro. Si sa valeur continue de progresser (et donc que les prix libellés en bitcoin continuent à baisser), sa plus petite unité, le Satoshi, pourra servir pour les achats de petits montants. Et il sera très facile, si nécessaire, d'accroître cette divisibilité par une modification bénigne du protocole : contrairement à une éventuelle modification de la limite des 21 millions, ce changement n'aurait aucun impact sur le cours et serait donc largement accepté par la communauté.

Par ailleurs, ce volume limité est aussi un retour à une caractéristique normalement essentielle de toute monnaie, qui a été totalement perdue de vue avec les monnaies nationales contemporaines. Dans toutes les civilisations, chaque fois que de nouvelles monnaies ont été expérimentées, celles qui se sont imposées sont celles dont la relative rareté permettait de garantir que leur valeur pourrait se maintenir dans le temps (en évitant toute production ou découverte majeure soudaine).

De ce point de vue, la " politique monétaire " du bitcoin est particulièrement bien pensée. Elle reproduit le modèle des métaux précieux qui a démontré son utilité pendant des siècles, et notamment au 19ème siècle qui a connu une croissance mondiale majeure avec une très grande stabilité des monnaies, organisées autour de l'étalon or. Pour le bitcoin comme pour un métal précieux, le volume total est limité et l'extraction coûteuse et progressive. Cette extraction se fait selon un rythme régulier et prévisible. Dans le cas du bitcoin, ce rythme est même parfaitement régulier et prévisible puisqu'il est inscrit dans l'algorithme fondateur. Il peut d'ailleurs être modifié mais il est très peu probable qu'un consensus puisse être formé en ce sens puisque cela diminuerait la valeur des bitcoins des acteurs impliqués.

Toutes choses égales par ailleurs, si la demande de bitcoins augmente plus que son rythme d'émission (qui est de plus en plus lent), sa valeur unitaire continuera d'augmenter. Le bitcoin est donc une monnaie en quelque sorte " déflationniste " (mais sans l'origine de la déflation que constitue normalement la réduction de monnaie et de substituts monétaires).

> ***Une monnaie comme le bitcoin, qui ne se déprécie pas avec le temps, peut contribuer à augmenter le niveau moyen de ce qui est appelé en économie la préférence temporelle pour le futur***

Or, **contrairement à une idée très répandue, la déflation n'est pas mauvaise en soi**. Tout dépend de ses causes et de ses circonstances historiques, qui peuvent être de natures très différentes (8). Si la déflation est causée par des faillites en série et une perte de confiance généralisée dans l'économie, elle peut être dévastatrice. Si, en revanche, elle résulte d'une concurrence accrue entre producteur et/ou d'une accélération du progrès technique, elle n'a rien de problématique : elle est même au contraire un immense avantage pour les consommateurs.

Selon l'économiste **Jesus Huerta de Soto,** l'un des principaux représentants contemporains de l'école autrichienne, la déflation *" est particulièrement salutaire lorsqu'elle naît de la conjonction d'une offre monétaire stable et d'une augmentation de la productivité. Un exemple : l'étalon-or au XIXº siècle. À cette époque, la quantité d'or augmentait seulement d'1% à 2% par an. À la même période, les entreprises du secteur industriel générèrent les augmentations de richesse les plus importantes de l'histoire " (9).*

Par ailleurs, la déflation peut, dans certaines configurations, avoir des effets positifs en termes économiques mais aussi politiques et moraux. D'après **Guido Hülsmann,** autre économiste du courant autrichien, *" la déflation est plutôt un grand promoteur de la liberté. Elle stoppe l'inflation et détruit les institutions qui la produisent. Elle abolit l'avantage relatif dont jouissent les financements à crédit, sous un régime d'inflation, par rapport aux investissement financés par de l'épargne. Par conséquent, elle décentralise le processus d'investissement et rend les banques, les entreprises, et les individus plus prudents et plus autonomes qu'ils ne l'auraient été sous un régime inflationniste " (10).*

Dans le cas du bitcoin, la baisse des prix nominaux n'aurait aucune cause récessioniste. La question pourrait en revanche se poser de savoir si elle ne favoriserait pas la thésaurisation. En réalité, les besoins des individus ne sont pas les mêmes en même temps, et

8. SALIN, Pascal, *Les Systèmes monétaires, des besoins individuels aux réalités internationales*, Odile Jacob, 2016

9. Institut Economique Molinari, 10/06/15 : http://www.institutmolinari.org/comme-l-etalon-or-entretien-avec,2138.html

10. HULSMANN, Guido, *Déflation et liberté*, Thomas Editions, 2015. Texte intégral : https://www.institutcoppet.org/2011/08/15/guido-hulsmann-deflation-et-liberte-2008

il n'y a aucune raison de pré-supposer que tous seraient prêts à reporter leur demande de consommation en même temps pour attendre une hausse du cours du bitcoin.

Par ailleurs, si cette caractéristique déflationniste du bitcoin amène certains à moins consommer, cela devrait réjouir ceux qui estiment que notre société consomme trop, au détriment des équilibres naturels ou de certaines valeurs traditionnelles. Les adeptes des théories de la décroissance pourraient être intéressés par le fait que le bitcoin semble rendre impossible une partie des mécanismes qu'ils critiquent, fondés sur la multiplication du crédit et la recherche permanente de croissance économique (11).

11. En revanche, ce qu'on appelle les politiques économiques de " relance par la consommation " (parfois revendiquées par les mêmes qui critiquent la " société de consommation ") seront plus difficiles à réaliser dans un monde où le bitcoin serait la monnaie universelle.

Une telle analyse serait pourtant fausse.

Premièrement, la thésaurisation n'empêche en rien la création de richesses et l'apparition de nouveaux biens et services. En effet, ce qui crée la richesse n'est pas la monnaie (n'importe quelle quantité de monnaie pouvant suffire à n'importe quelle économie, aussi développée soit-elle) : ce sont les moyens de production au sens large, ressources humaines incluses, et la manière dont ils sont utilisés. Si une majorité de détenteurs de monnaie thésaurisent, cela ne fait que donner une influence relative supérieure à ceux qui ne thésaurisent pas. Comme si les premiers déléguaient leur pouvoir économique aux seconds. La puissance productive globale reste inchangée, tout comme le niveau de consommation, même si cette dernière porte sur des produits de nature différente.

Deuxièmement, on peut très bien imaginer que des banques détenant des bitcoins émettent des crédits libellés dans une nouvelle (crypto)monnaie, tout en gardant un système de réserves fractionnaires leur permettant une expansion massive du crédit (cf. infra).

Enfin, en termes théoriques, **une monnaie comme le bitcoin, qui ne se déprécie pas avec le temps, peut contribuer à augmenter le niveau moyen de ce qui est appelé en économie la " préférence temporelle pour le futur " (12).** Une monnaie qui se déprécie incite, avec d'autres facteurs (comme l'instabilité juridique, la pression fiscale, les guerres, etc.) à épargner peu et à consommer du capital. Au contraire, une monnaie stable sur le long terme incite à l'investissement et à la construction du futur.

12. https://www.wikiberal.org/wiki/Pr%C3%A9f%C3%A9rence_temporelle

Le 19ème siècle illustre bien cette idée: c'est, dans l'histoire de l'humanité, l'une des périodes les plus fertiles en développement économique et social, en progrès scientifique et médical, en

réalisations industrielles, artistiques, etc. Et c'est aussi un siècle au cours duquel, à quelques exceptions près, causées par des interventions étatiques intempestives, les monnaies, fondées sur l'étalon or, ont conservé une valeur remarquablement stable (13). Cette dimension est peu comprise dans les sociétés contemporaines, largement influencées par la croyance issue de Keynes, prétendant que le développement économique est fondé davantage sur la consommation que sur l'épargne et l'accumulation du capital (14).

13. AMMOUS Saifedean, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley, 2018

14. Croyance réfutée par les travaux des économistes de l'école autrichienne, en particulier HAZLITT Henry, *The Failure of The New economics, An Analysis of the Keynesian fallacies*, D. Van Nostrand Company Inc., 1965 et HAYEK, Friedrich, *Contra Keynes And Cambridge: Essays, Correspondence.* University of Chicago Press, 2012

3.2 Les conséquences insoupçonnées de la liberté monétaire

3.2.1 Vers un nouveau paradigme monétaire ?

À mesure que de grands acteurs financiers entrent sur les marchés des cryptomonnaies, jusqu'ici essentiellement frequentés par des particuliers, le développement de ces instruments connaît une progression de plus en plus rapide. Deux bourses américaines ont déjà commencé à lister des dérivés sur le bitcoin en décembre 2017 (le Chicago Mercantile Exchange, CMO, et Chicago Board Options Exchange, CBOE). Il est trop tôt pour tirer un bilan de ces outils (15). De même, la bourse de New York envisage de plus en plus sérieusement de mettre en place des instruments liés au bitcoin (16).

Soit sur la blockchain bitcoin, soit sur une blockchain concurrente, la probabilité pour qu'une cryptomonnaie accède à un statut de moyen de paiement couramment utilisé grâce à une sécurité élevée et à un passage à l'échelle réussi ne cesse d'augmenter et relève de moins en moins de la science-fiction. Indépendamment de la réponse juridique qui sera apportée par les pouvoirs publics, l'évolution des conditions techniques et économiques fait qu'il se peut même qu'on assiste à une multiplication des cryptomonnaies, un grand nombre d'entre elles étant susceptibles de servir de moyen de paiement dans la vie courante.

Une des définitions les plus simples et les plus efficaces du concept de monnaie est celle de Ludwig von Mises : " un moyen d'échange couramment utilisé **"** (*L'Action Humaine*, 1949).

15. D'un côté, l'offre de futures sur bitcoin pourrait avoir plusieurs conséquences positives : améliorer l'image de la devise, en réduire la volatilité et disposer d'instruments de couverture. De l'autre, l'opportunité donnée aux investisseurs professionnels de " shorter " le bitcoin pourrait affecter l'ensemble de l'écosystème des cryptomonnaies. Cf. l'analyse d'Ambra Moschini, 11/01/18. https://bitcoin.fr/institutionnalisation-des-contrats-a-terme-sur-le-bitcoin-speculation-ou-opportunite-de-normalisation/

16. *Cointelegraph*, 07/01/18. https://cointelegraph.com/news/new-york-stock-exchange-moves-on-bitcoin-etfs

Le terme " couramment " est à la fois vague et utile : il n'implique pas que cette utilisation puisse avoir lieu dans le monde entier, auprès de tout interlocuteur. Une utilisation courante peut avoir lieu dans une zone géographique précise ou dans une certaine communauté. C'est la raison pour laquelle un grand nombre de cryptomonnaies peuvent émerger, chacune avec des caractéristiques différentes, les rendant propres à servir des besoins différents (avec par exemple des niveaux de sécurité ou des temps de validation différents, selon les montants échangés).

Ces cryptomonnaies ne remplaceront pas nécessairement les monnaies nationales. Elles peuvent coexister en remplissant des usages différents. Dans certains pays, toutefois, et dans certaines circonstances, on pourra assister à une forme de " fuite " devant les monnaies nationales, quand leur valeur aux yeux des utilisateurs sera devenue beaucoup trop faible ou trop risquée (17). Ces phénomènes ne sont pas nouveaux et ont rythmé toutes les grandes crises monétaires du 20ème siècle. La nouveauté réside dans le type de support alternatif offert, par les blockchains, aux personnes souhaitant se débarrasser de leurs monnaies nationales.

Par ailleurs, deux caractéristiques technologiques vont probablement appuyer le développement des cryptomonnaies. D'une part, elles permettent de réaliser des transactions programmables (cf. partie 4). D'autre part, elles vont permettre d'accompagner l'une des principales révolutions industrielles de notre époque : le développement des objets connectés, l'avènement des robots et l'essor de l'intelligence artificielle : pour la première fois, des entités non humaines vont prendre des décisions de stockage et d'échange de valeur. Elles devront donc procéder à des transactions monétaires. Elles vont aussi s'échanger des informations, des données, des instructions. Pour toutes ces tâches, les cryptomonnaies vont offrir des solutions plus sûres, plus rapides et moins coûteuses que bon nombre de systèmes existants.

17. Fuites qui n'ont rien à voir avec la loi de Gresham, selon laquelle la " mauvaise " monnaie chasse la " bonne " : cette loi " *ne joue que dans le cas où il existe un prix " officiel " entre deux monnaies, différent du prix qui équilibrerait les offres et demandes. Les détenteurs de monnaies, conscients du fait que le prix imposé ne permet pas les ajustements du marché, essaient de se débarrasser de la " mauvaise " monnaie et de garder la " bonne " monnaie. Ils pensent d'ailleurs très probablement que le prix de la " bonne monnaie " va augmenter dans le futur pour refléter les raretés relatives véritables* ". SALIN, Pascal, *La Vérité sur la monnaie*, Odile Jacob, 1990 (page 55)

3.2.2 Une monnaie dénationalisée

L'essentiel de l'histoire de la monnaie à travers les siècles, et même les millénaires, est l'histoire d'une appropriation très progressive, par l'État, de cette institution qui, à l'origine, était une création spontanée. Cette appropriation s'est faite au prix, d'une part, d'une réduction croissante de la liberté des utilisateurs des monnaies et des services bancaires, et, d'autre part, de désordres monétaires de plus en plus violents, conduisant eux-mêmes à une intervention croissante des États dans ce domaine (18).

Cette évolution a été extrêmement progressive. Elle s'est étalée sur plusieurs millénaires avec plusieurs étapes clés. Les monarques ont notamment imposé un nom aux pièces d'or (généralement le leur). Ils ont accru la réglementation sur les modalités de production des pièces d'or. Ils ont usé de leur droit de seigneuriage, consistant à diminuer le contenu en or des pièces tout en gardant leur valeur nominale, afin d'empocher un profit leur permettant de financer des dépenses massives. Cette forme de spoliation a d'ailleurs été dénoncée très tôt, notamment dans ce qui est probablement la première grande œuvre économique, le *Traité sur la monnaie* rédigé en 1355 par Oresme.

18. DE SOTO, Jesus, Huerta, *Monnaie, crédit bancaire et cycles économiques*, L'Harmattan, 2011

> ***L'usage des cryptomonnaies pourra être encadré et l'est déjà. Mais il sera impossible techniquement de les interdire. On ne supprimera pas les cryptomonnaies, pas plus qu'on ne peut " faire revenir le dentifrice dans le tube***

Plus tard, les États ont encadré de plus en plus étroitement l'activité des banques. Tout en accroissant, par certains aspects, leurs obligations, ils leur ont octroyé divers privilèges qui servaient leurs propres fins. Ils ont ainsi autorisé le système des réserves fractionnaires (19) et la " suspension du paiement en espèces " en période de tension bancaire (20), afin de favoriser l'activité de création monétaire des banques par le crédit, qui contribuait à alléger le coût du financement de l'État. Ces pratiques étaient auparavant minoritaires, interdites et souvent sévèrement punies (21) ; mais elles ont progressivement été implicitement tolérées par les autorités puis admises officiellement.

Enfin, **les États ont conféré des privilèges à certaines banques, par la suite consacrées banques centrales et prêteurs en dernier ressort** (cf. encadré suivant). Par exemple, en France, Napoléon a offert progressivement, à partir de 1803, le privilège de l'émission de billets à la Banque de France, qui avait notamment pour actionnaires… Napoléon et sa famille.

19. Le terme de "système de réserves fractionnaires" (on parle aussi de "couverture partielle") désigne le droit pour une banque commerciale de prêter, par des jeux d'écritures, de l'argent qu'elle n'a pas - en apparence - et sur lequel, outre le remboursement par le débiteur, elle touchera des intérêts. Cette création de monnaie scripturale est tempérée par l'obligation de déposer un pourcentage des encours de crédit de la banque auprès de la banque centrale ("réserves obligatoires"), pourcentage relativement faible en pratique (quelques pourcents). De la même façon, la transformation bancaire consiste à prêter des ressources à court terme (celles des épargnants) pour financer des crédits à long terme (ceux des emprunteurs). On parle dans ce cadre d'effet multiplicateur du crédit, le multiplicateur désignant le rapport entre la base monétaire (monnaie centrale) et la quantité de monnaie issue du crédit accordé par les banques. Ce sont "les crédits qui font les dépôts". Les avis des différents théoriciens sont très tranchés, les uns estimant que le système de réserves fractionnaires est une escroquerie, les autres que c'est une innovation capitale en matière de monnaie et de système bancaire. Source : https://www.wikiberal.org/wiki/R%C3%A9serves_fractionnaires

20. " *Alors que chacun doit payer ses dettes ou bien être condamné à faire faillite, les banques peuvent refuser de convertir leurs billets, tout en exigeant de leurs débiteurs qu'ils paient à une date spécifiée. Ceci est généralement appelé " suspension du paiement en espèces. " Permis de voler " serait plus exact, car comment appeler autrement une autorisation gouvernementale de continuer ses affaires sans respecter ses contrats ?* ". ROTHBARD, Murray, *État, qu'as-tu fait de notre monnaie ?* Institut Coppet, 2011 (page 83). Texte complet : https://www.institutcoppet.org/wp-content/uploads/2011/01/État-quas-tu-fait-de-notre-monnaie.pdf

21. Par exemple, en Catalogne, à partir de 1321, un banquier ne parvenant pas à honorer ses obligations parce qu'il aurait utilisé indûment une partie des dépôts à vue reçus pour accorder des prêts pouvait être décapité. Cf. DE SOTO, Jesus, Huerta, *Monnaie, crédit bancaire et cycles économiques*, L'Harmattan, 2011 (page 67).

Qu'est-ce qu'une banque centrale ?

> *" Une banque centrale accède à sa position dominante grâce à un monopole du monnayage octroyé par l'État. Ce secret de leur pouvoir est rarement crié sur les toits. Invariablement, on interdit aux banques privées d'émettre des billets et ce privilège est réservé à la banque centrale. Les banques privées ne peuvent offrir que des comptes courants. Si leurs clients souhaitent effectuer des retraits en espèces, par conséquent, les banques doivent s'adresser à la banque centrale ; d'où son titre imposant de « banque des banques ». Elle est une banque des banques parce que les autres banques sont forcées de traiter avec elle.*
>
> *Ainsi, les comptes courants deviennent des dépôts contenant des billets émis par la banque centrale et plus seulement de l'or. Et ces billets ne sont pas des billets ordinaires. Ce sont des créances sur la banque centrale, une institution auréolée de toute l'autorité de l'État lui-même. Après tout, c'est l'État qui nomme les dirigeants de la banque centrale et il coordonne avec eux ses autres politiques publiques. Il perçoit ces billets en paiement de l'impôt et décrète qu'ils ont cours légal "*
>
> **Murray Rothbard,** *État, qu'as-tu fait de notre monnaie ?* **(22).**

22. ROTHBARD, Murray, *État, qu'as-tu fait de notre monnaie ?* Institut Coppet, 2011 (page 85)

En général, après avoir octroyé à une banque le monopole de l'émission des billets, le gouvernement procédait, plusieurs années plus tard, à sa nationalisation, au motif qu'elle risquait d'abuser de sa position de monopole. Au 20ème siècle, l'activité de production monétaire dévolue aux banques commerciales à travers le mécanisme du crédit mais finement piloté par les banques centrales a permis aux États d'essayer d'orienter autant que possible l'activité économique, notamment sous l'influence des idées keynésiennes, et de financer le poids croissant des États Providence. Ce pouvoir s'est traduit par une tendance inflationniste généralisée et inédite, conduisant ensuite souvent à des politiques de stabilisation aux conséquences économiques et sociales douloureuses, puis un cercle vicieux de politiques de " relance " et de " stabilisation ".

Une des motivations des créateurs de cryptomonnaies est de libérer les populations de ces travers. Elle s'appuie sur les analyses des économistes ayant théorisé, depuis plusieurs décennies, la nécessité de privatiser la monnaie.

Comme le résume **Pascal Salin :** *" certes, c'est parce qu'il s'est emparé du monopole de la production de monnaie que l'État est le seul à pouvoir lutter contre l'inflation, mais il est le seul à créer de l'inflation et il est le plus apte à le faire (...). Il n'y aurait pas besoin de politique de stabilisation monétaire si l'État n'avait pas d'abord créé de l'instabilité monétaire ! La succession des phases d'inflation et de désinflation est l'expression même d'une instabilité monétaire. Elle est le pur produit de l'interventionnisme étatique dans le domaine monétaire. Pour supprimer l'instabilité monétaire il n'y a pas d'autre solution que de retirer de l'État toute décision concernant la production et la circulation de la monnaie. Il faut donc privatiser la monnaie " (23).*

23. SALIN, Pascal, Libéralisme, Odile Jacob, 2000 (page 436)

Dès 1976, dans *The Denationalization of Money*, **Hayek** proposait de suspendre le monopole de l'émission monétaire : *" le secteur privé, s'il n'en avait pas été empêché par l'État, aurait depuis fort longtemps fourni au public un choix de monnaies diverses, et celles qui auraient prévalu grâce au processus de concurrence auraient fondamentalement eu un pouvoir d'achat stable et auraient empêché tant la stimulation excessive de l'investissement que les récessions qui leur sont consécutives " (24).*

24. HAYEK, Friedrich, *Pour une vraie concurrence des monnaies*, PUF, 2015 (page 15)

Quelques années plus tard, en 1984, il déclarait, avec une expression presque prophétique si on la relie à l'apparition du bitcoin : *"je ne crois pas au retour d'une monnaie saine tant que nous n'aurons pas retiré la monnaie des mains de l'État ; nous ne pouvons pas le faire violemment ; tout ce que nous pouvons faire, c'est, par quelque moyen indirect et rusé, introduire quelque chose qu'il ne peut pas stopper " (25).*

25. *" I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop "*. Interview avec James U. Blanchard, Université de Fribourg, 1984 : https://www.youtube.com/watch?v=EYhEDxFwFRU&t=4s (minute 19.22)

A l'époque, sa proposition avait suscité un intérêt qui n'était toutefois resté qu'académique. Personne n'envisageait sa mise en œuvre concrète à court terme (26). Avec l'essor des cryptomonnaies, cette concurrence est désormais une réalité. Les utilisateurs de monnaie peuvent choisir librement les monnaies les mieux à même de répondre à leurs besoins. Exactement comme cela a longtemps été le cas dans de nombreuses régions du monde

26. Ce dont Hayek était parfaitement conscient ; il précisait, en introduction de son ouvrage : *" je suis convaincu que la tâche principale d'un théoricien de l'économie ou d'un philosophe politique doit être d'influencer l'opinion publique afin de rendre politiquement faisable ce qui semble impossible aujourd'hui "*.

et à de nombreuses périodes de l'histoire. Cette concurrence est encore embryonnaire mais elle est appelée à se développer. Même si le cours légal existera probablement encore longtemps, elle crée une situation qui n'était pas prévue par les autorités monétaires et dont les conséquences sont encore difficiles à mesurer.

Si les inventeurs du bitcoin et de ses petites sœurs cryptomonnaies avaient demandé la permission pour le faire, elle ne leur aurait jamais été accordée. C'est d'ailleurs ce qui explique l'explosion d'innovation que l'on constate en ce moment dans ce secteur. Chacun peut s'approprier la technologie et la compléter, ce qui ouvre au domaine de la monnaie un potentiel d'innovation qui lui était auparavant totalement interdit.

L'usage des cryptomonnaies pourra être encadré et l'est déjà. Mais il sera impossible techniquement de les interdire. Le génie technologique et monétaire s'est échappé de la lampe, et rien ne l'y fera rentrer. **On ne supprimera pas les cryptomonnaies, pas plus qu'on ne peut " faire revenir le dentifrice dans le tube "** (pour reprendre la célèbre métaphore, à propos de l'inflation, d'un ancien patron de la Bundesbank). Des mesures d'interdiction seront probablement prises, sur des motifs souvent légitimes (lutte contre le blanchiment et le terrorisme, etc.) mais leur mise en œuvre sera difficile.

De manière schématique, le seul moyen vraiment efficace d'empêcher l'utilisation d'une cryptomonnaie serait de bloquer tout accès à Internet. Les interdictions légales éventuelles ralentiront l'essor des cryptomonnaies, pourront faire chuter les cours mais se traduiront rapidement par un déplacement des acteurs et des capitaux vers des zones géographiques plus accueillantes et vers d'autres cryptomonnaies plus adaptées techniquement. Les régulations excessives auront aussi pour effet de faire basculer dans le marché noir une plus grande proportion d'activités économiques.

3.2.3 Quel avenir pour les politiques monétaires et le secteur bancaire ?

Les politiques et systèmes monétaires

Quelle politique monétaire si les agents économiques souhaitent régler une partie croissante de leurs transactions en cryptomonnaies plutôt qu'en monnaies nationales ?

Le pouvoir de battre monnaie est parfois présenté comme une fonction régalienne. Cette affirmation est pourtant largement arbitraire. Elle n'est acceptée que parce qu'elle est répétée *ad nauseum*, sans grande justification (27). Ce pouvoir est en tout cas *de facto* retiré aux États par l'apparition des cryptomonnaies. Quelques États ont des velléités de création de cryptomonnaies étatiques mais tant que ces dernières resteront créées et gérées par des organismes centralisés, elles n'auront aucune chance de concurrencer celles fondées sur des blockchains véritablement libres et décentralisées.

Dans les économies contemporaines, la politique monétaire reste un outil de politique publique pour influencer le niveau des taux d'intérêt en pilotant l'évolution de la masse monétaire. Elle poursuit divers types d'objectifs macro-économiques selon les pays (maîtrise du niveau général des prix, activité économique, etc.). Cet outil est totalement inopérant avec des cryptomonnaies émises de manière décentralisée par un algorithme dont les concepteurs et la communauté ont décidé des caractéristiques. C'est donc un pan majeur des politiques publiques qui pourrait être remis en question.

Pour les économistes qui croient dans l'efficacité des politiques monétaires pour stabiliser l'économie (opinion largement dominante aujourd'hui), c'est une évolution extrêmement préoccupante.

En revanche, elle est positive pour ceux qui estiment que le monopole de l'émission de la monnaie par la puissance publique a eu des effets économiques globalement négatifs (28). D'après eux, le nombre et l'ampleur des catastrophes monétaires au 20ème siècle a augmenté avec l'emprise croissante des États sur la monnaie. Et, de leur point de vue, **les manipulations monétaires effectuées par les banques centrales sont la cause principale des cycles**

27. La " justification " typique est : les fonctions de l'État incluent la sécurité, la diplomatie,... la monnaie ; donc la production de monnaie est une fonction régalienne qui doit être assurée de manière monopolistique par la puissance publique.

28. C'est notamment le cas de l'école autrichienne, fondée par Carl Menger, Eugen von Böhm-Bawerk et Ludwig von Mises. Hayek a obtenu le prix Nobel d'économie pour cette analyse. Cf. ROTHBARD, Murray, *État, qu'as-tu fait de notre monnaie ?* Institut Coppet, 2011 et DE SOTO, Jesus, Huerta, *Monnaie, crédit bancaire et cycles économiques*, L'Harmattan, 2011

économiques, avec leur succession de phases de croissance artificielle et de crises aux conséquences dévastatrices (cf. annexe 5).

Le scenario selon lequel les banques centrales pourraient commencer à acheter des cryptomonnaies pour prendre en compte la hausse considérable de leurs cours et diversifier leurs actifs paraît encore difficile à imaginer. Pourtant, il commence à être évoqué par des acteurs crédibles (29). La directrice du FMI, Christine Lagarde, s'est exprimée sur le bitcoin et les cryptomonnaies d'une manière inhabituellement positive (30).

Et l'économiste Saifedean Ammous estime que **le bitcoin pourrait servir de socle à un nouveau système monétaire international** dans lequel les banques centrales pourraient trouver un intérêt à l'utiliser à la fois comme monnaie de réserve et comme système de règlement interbancaire (31). Pour lui, ce serait possible en raison du fait que le bitcoin est, avec l'or, la seule monnaie dénuée de risque de contrepartie. Il considère qu'une telle évolution pourrait même se produire bien avant que le progrès technologique ne permette au bitcoin d'être couramment utilisé pour des achats de petits montants.

Hal Finney estimait également, dès 2010, que les banques pourraient posséder des bitcoins et ne les utiliser que pour leurs échanges interbancaires et pour servir d'actif sous-jacent à l'émission de prêts (32). Il citait l'économiste Georges Selgin, théoricien de la banque libre (indice parmi d'autres de l'impressionnante culture économique des concepteurs de Bitcoin), qui estime qu'un système de réserves fractionnaire serait possible. Ce dernier aspect fait toutefois débat parmi les économistes qui estiment que la monnaie pourrait et devrait être soustraite au monopole public. Par exemple, **Saifedean Ammous** estime que *" sans un prêteur en dernier ressort, le système de réserves fractionnaires devient extrêmement dangereux, et les seules banques qui survivront sur le long terme seraient celles s'appuyant sur une monnaie saine et offrant des instruments financiers 100% appuyé sur Bitcoin " (33).*

29. *Coindesk*, 17/12/17. https://www.coindesk.com/2018-year-central-banks-begin-buying-cryptocurrency/

30. *La Tribune*, 29/09/17. https://www.latribune.fr/entreprises-finance/banques-finance/le-fmi-pret-a-discuter-des-monnaies-virtuelles-et-de-la-blockchain-752355.html

31. AMMOUS Saifedean, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley, 2018

32. Forum Bitcoin, 30/12/10 : https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211

33. https://thesaifhouse.wordpress.com/2017/05/19/economics-of-bitcoin-as-a-settlement-network/

L'industrie bancaire

L'expert de Bitcoin Andreas Antonopoulos estime que les banques ne disparaîtront pas mais qu'elles seront bientôt réduites au même statut que les bureaux de poste à l'ère de l'e-mail.

Au-delà, quel rôle pour les banques de détails si chaque individu peut devenir sa propre banque en gérant lui-même ses crypto-monnaies ? Depuis des siècles, les banques étaient chargées de stoker les avoirs des particuliers et des entreprises, et de leur octroyer des crédits. Ces dernières années, avec les progrès fulgurants d'Internet et de la numérisation, on pouvait légitimement se demander à quoi pourraient encore servir la banque physique.

> ***le bitcoin pourrait servir de socle à un nouveau système monétaire international***

Une partie considérable du profit des banques actuelles vient du pouvoir de création monétaire qu'elles tirent de leur activité de crédit. Avec les cryptomonnaies privées, il va devenir de plus en plus facile de conserver soi-même ses avoirs, mais également de les prêter en tirant profit de plateformes décentralisées qui se substitueront à la fonction d'intermédiation du crédit assurée par les banques. Ces activités sont étroitement régulées mais le fonctionnement des blockchains étant transnational et résistant à la censure, il risque de permettre d'esquiver ces régulations et d'obtenir ainsi un avantage comparatif décisif.

L'industrie bancaire, protégée par des normes innombrables qui limitent artificiellement la concurrence dans ce secteur, est une des dernières à ne pas avoir intégré massivement les progrès technologiques contemporains pour améliorer la qualité de ses services et en diminuer le coût. Dans ce contexte, l'avènement des cryptomonnaies ne devrait pas représenter un problème nouveau pour elle mais plutôt la solution de substitution, pour remplacer une industrie qui n'aura pas su se réformer à temps, selon le schéma désormais classique de " dilemme de l'innovateur " du chercheur Clayton Christenson (34). Certaines banques auront aussi l'intelligence de s'adapter à cette révolution en proposant des services utiles aux consommateurs. Par exemple, des clients souhaiteront peut-être faire assurer la garde sécurisée de leurs cryptomonnaies par des établissements comme les banques ; mais l'essentiel des nouveaux services dans ce domaine restent à inventer.

34. CHRISTENSEN, Clayton, *The Innovator's Dilemma*, Harper Business, 2011

3.2.4 La protection des individus

Dans les pays soumis à la dictature, les cryptomonnaies représentent déjà un outil indéniable de protection contre l'arbitraire et l'oppression.

Au-delà de ces cas particuliers, **le développement des cryptomonnaies va sans doute offrir aux individus un outil de résistance particulièrement efficace non seulement contre l'inflation et la surveillance, mais aussi contre la guerre contre le cash** qui semble s'intensifier dans le monde entier depuis quelques années. De nombreux gouvernement tentent de réduire l'usage du cash, généralement en invoquant des motifs apparemment légitimes (lutte contre la corruption, contre le terrorisme, contre le marché noir, etc.). Mais l'argent liquide est un instrument de protection de la vie privée, et le supprimer rapprocherait d'une société de surveillance et de contrôle éloignée des principes d'une société de liberté (35).

Un récent épisode de cette guerre contre le cash a été particulièrement révélateur : la réforme monétaire indienne décidée par le gouvernement en novembre 2016, consistant à démonétiser les billets de 500 et 1 000 roupies, a tourné au désastre en créant d'immenses problèmes sans atteindre aucun de ses objectifs (36) et a eu pour effet de faire exploser l'intérêt de la population pour le bitcoin (37). Si l'argent liquide vient à être supprimé, les cryptomonnaies le remplaceront et une forme de cash électronique sera disponible. Le bitcoin se voulait, d'ailleurs, dans l'esprit de son créateur, un " système de cash électronique pair-à-pair ".

> ***Il est indéniable que les cryptomonnaies offrent une protection contre l'oppression fiscale***

Il est tentant de ne voir derrière tout détenteur de cryptomonnaie qu'un délinquant fiscal en puissance. On n'éprouve pourtant pas la même méfiance pour tout utilisateur d'argent liquide. Les professions qui utilisent fréquemment ce type de monnaie (certains commerçants, membres de professions libérales, etc.) ne font pas l'objet d'une telle suspicion. Cette présomption de culpabilité fiscale est injuste et traduit une autre forme de réaction plus émotive que rationnelle contre la révolution numérique qui atteint le domaine monétaire. Quoiqu'il en soit, il est indéniable que **les cryptomonnaies offrent une protection contre l'op-**

35. Ronald-Peter Stöferle, "Myths Behind the War on Cash", Mises Institute, 06/28/2017. https://mises.org/library/myths-behind-war-cash

36. BBC, 30/08/17. http://www.bbc.com/news/world-asia-india-41100610

37. *Cointelegraph*, 01/12/17. https://cointelegraph.com/news/bitcoin-boom-draws-record-number-of-indian-investors-according-to-exchanges

pression fiscale qui atteint souvent des proportions de plus en plus incompatibles avec l'idéal d'une société libre et pacifique (38).

En revanche, la transition peut créer des risques non négligeables pour les utilisateurs mal informés. De plus en plus de gens souhaitent épargner en cryptomonnaies mais maîtrisent mal les règles et savoirs techniques pour protéger leurs avoirs. Ils ne sont généralement pas conscients du niveau de risque induit par la nouveauté de ces instruments financiers et par leur volatilité. Les communautés d'utilisateurs plus avertis sont sensibles à ces problèmes et font tout pour alerter le public, notamment en répétant quelques conseils importants : ne pas stocker ses cryptomonnaies sur des plateformes d'échange (où l'on ne possède qu'un PIN, tandis que ce sont ces plateformes qui conservent les clés privées et sont donc hackables de ce fait) ; ou encore, n'investir en cryptomonnaies que ce que l'on peut se permettre de perdre totalement.

L'utilisation des cryptomonnaies a un effet responsabilisant : en cas de perte des clés privées, absolument aucun recours n'est possible. Aucune garantie d'État ne peut être sollicitée.

En même temps, la garantie des États sur les monnaies nationales n'est pas toujours aussi rassurante que prévu. Pour s'en convaincre, inutile d'aller jusqu'au Venezuela : à Chypre, en 2013, fait inédit dans un État de droit, membre de l'Union européenne, une loi d'exception a spolié les épargnants au mépris des droits les plus élémentaires. A la suite de la directive relative au redressement des banques et à la résolution de leurs défaillances (BRRD), de nouvelles dispositions prévoient de faciliter ce type d'opération en cas de besoin dans toute l'Union européenne (39). Et, dans le même ordre d'idée, en France, la loi Sapin 2 prévoit qu'en cas de crise financière, la liquidation de contrats d'assurance vie pourra être bloquée (40).

38. Comme le souligne l'historien des idées politiques Philippe Nemo,: " *l'impôt socialisant détruit la notion de consentement à l'impôt et viole le contrat social qui est censé fonder les démocraties modernes (...). L'arbitraire fiscal est largement responsable du climat de défiance, de fuite et généralement de mécontentement rageur qui caractérise les pays comme la France (...). Le transfert aux collectivités publiques d'une trop grande part de la richesse nationale est un facteur favorisant l'arbitraire, l'irrationalité, l'immoralité et le caractère partisan des décisions publiques, ce qui stupéfie les assujettis lorsqu'ils en prennent conscience, minant plus encore le lien social* ". NEMO, Philippe, *Philosophie de l'impôt*, PUF, 2017 (page 17)

39. *Le Revenu*, 10/01/16 : http://www.lerevenu.com/est-il-vrai-qua-partir-du-01012016-les-comptes-clients-de-plus-de-100-000-eu-de-depots-pourront-etre

40. Eric Verhaghe, blog *Jusqu'ici tout va bien*, 30/09/16. http://eric-verhaeghe.entreprise.news/2016/09/30/assurance-vie-prets-spoliation/

3.2.5 Quel avenir pour l'État-Providence ?

Quel avenir pour le financement des États, si une part croissante de l'économie bascule dans l'univers des cryptomonnaies et échappe ainsi à leur pouvoir de lever l'impôt ?

En matière de taxation des cryptomonnaies (sur la détention ou sur les plus-values), les États sont déjà largement dépendants du bon vouloir des déclarations fiscales des utilisateurs et ont très peu de moyens de vérifier leur exactitude. Ils pourront essayer d'avoir accès aux données des plateformes d'échange pour taxer d'office les détenteurs mais ces plateformes se délocaliseront alors dans des pays plus accueillants, et le progrès technique se poursuivra dans le sens d'une anonymisation croissante des cryptomonnaies.

Pour financer leurs dépenses, certains États pourront essayer de se procurer des cryptomonnaies autrement que par la fiscalité, s'ils estiment que c'est utile pour eux. Ils pourront essayer d'en acheter sur le marché contre des devises. Ils pourront aussi essayer de s'en procurer en échange de biens ou services (par exemple en vendant des actifs publics : infrastructures, biens immobiliers, parts dans des entreprises publiques, etc.). Enfin, ils pourront devenir producteurs en entrant dans l'industrie du minage. Ces solutions auront un coût économique et/ou politique majeur. Et s'ils ne parviennent pas à se procurer des cryptomonnaies alors que leur usage se répand, on peut prévoir que cela les obligera à diminuer drastiquement leurs dépenses car ils n'auront plus les moyens de les financer à la même hauteur avec des monnaies étatiques dévalorisées par cette concurrence.

De manière plus prospective, on peut estimer que si l'usage des cryptomonnaies par les États se développe (que cela soit par une utilisation monétaire ou pour le recours à des fonctionnalités annexes de la blockchain comme l'horodatage ou l'enregistrement de preuves et titres juridiques), un problème de souveraineté finira par se poser: les États ne pourront pas se permettre de devenir trop dépendant de mineurs installés dans d'autres États. Ils pourront alors être tentés de participer eux-mêmes au minage.

Enfin, quel avenir pour les systèmes d'assurances sociales centralisées et peu efficientes des États-Providence, dans un contexte où l'assurance peut être révolutionnée par les transactions programmables sur les blockchains et les réseaux de *smart contracts* ?

Ces nouveaux outils peuvent progressivement se substituer à un grand nombre d'assurances, le tout d'une manière plus fiable et moins coûteuse que n'importe quel système centralisé (cf. partie 4). Si des offres privées se développent et s'avèrent nettement plus performantes que celles offertes par les États-Providence, la légitimité de ces dernières sera remise en question.

Il sera tentant pour les États d'essayer de tirer profit des technologies issues de Bitcoin pour moderniser leurs propres processus et organisations. De nombreux domaines de l'action publique peuvent s'y prêter : identité digitale, modalités de vote, gestion des données publiques, commande publique, etc. (41) Mais on peut craindre qu'ils tardent à le faire, par rapport au rythme extrêmement rapide des changements à l'œuvre dans le secteur privé.

Ces différents éléments suggèrent que **des révisions complètes de doctrine sur le rôle de l'État dans une économie de marché pourraient découler de l'avènement des cryptomonnaies**. Force est de constater que ces aspects sont négligés dans le débat public alors qu'ils pourraient devenir d'actualité plus vite que prévu.

41. FABRIZI-RACINE, Nina, " La blockchain : (R)évolution d'État ? ", *La Semaine Juridique*, n°49, 11/12/17

4. Une nouvelle ère de décentralisation et d'autonomie

4.1 La multiplication des blockchains

Bitcoin ouvre la voie à de multiples innovations induites par la liberté et l'autonomie qu'offre sa technologie. Véritable " argent programmable ", il permet la conception de services où le flux financier est automatiquement réalisé sans intervention humaine ou de tiers de confiance comme les banques.

Pour permettre la mise en œuvre d'un de ces programmes (ou smart contract), on recourt à des " oracles ". Ce sont des sources d'information externes qui fournissent des éléments déclencheurs de la réalisation de la transaction. Par exemple l'assureur A indemnise un bitcoin à l'agriculteur B à condition que la température descende en-dessous de 0°C pendant deux jours. La transaction est scellée dans un contrat et elle sera exécutée lorsque le ou les oracles auront validé que la température locale aura bien été inférieure à 0°C. Afin de ne pas avoir de litiges, et de ne pas être juge et partie, l'assureur et l'agriculteur s'entendent pour choisir trois oracles : Météo France, une autre société disposant de thermomètres connectés sur l'ensemble du territoire, et un syndicat agricole. Le consensus convenu entre les parties valide la transaction si deux oracles sur trois donnent un verdict positif. Dans ce cas, la transaction est exécutée sans possibilité pour l'assureur de faire machine arrière. C'est ainsi la garantie,

pour l'agriculteur, que l'assureur n'invoquera pas des circonstances particulières pour retarder ou annuler l'indemnisation.

Le métier d'oracle est celui d'un tiers de confiance. Il est possible de multiplier les oracles pour ne pas devoir faire confiance à un seul juge. C'est d'ailleurs dans ce contexte que se développent des oracles décentralisés, qui permettent de s'affranchir d'une société commerciale que l'on pourrait potentiellement compromettre. L'oracle est un potentiel nouveau métier pour les banques et assurances… mais demain on ne voudra plus faire confiance à des entités, mais à la multitude, décentralisée.

On peut distinguer plusieurs échelles d'automatisation et de décentralisation de ce cas d'usage. Dans un premier temps, seul le paiement, encapsulé dans une transaction programmée, est réalisé automatiquement. C'est l'exécution du contrat (l'indemnisation) qui est automatisée. Dans un second temps, c'est tout le processus contractuel allant de la souscription à l'indemnisation qui peut être automatisé et déporté dans une application décentralisée. Dans ce cas, l'assureur est l'éditeur de cette application et celle-ci peut acquérir un cycle de vie autonome.

Mais finalement, la personne morale éditrice et tiers de confiance du contrat d'assurance pourrait être amenée à disparaitre au profit de la communauté. La DAO (*decentralized autonomous organization*) serait composée des souscripteurs des contrats assurances et de ses actionnaires, et deviendrait l'organisation remplaçant l'assurance telle que nous la connaissons aujourd'hui : la foule organise elle-même le système d'assurance au travers de règles écrites dans des (smart) contrats incensurables et dont l'exécution est automatisée.

Cette vision illustre la fameuse citation de Lawrence Lessig, " *code is Law* " (1), par laquelle il décrit un environnement numérique où les règles voire les régulations sont inscrites directement dans le code informatique. Ici, la liberté offerte aux développeurs les conduira à proposer au marché des solutions redéfinissant les concepts historiques de l'assurance et de la solidarité, par exemple. C'est peut-être la tendance vers laquelle nous glissons avec l'avènement des applications autonomes décentralisées.

La proposition technologique la plus visionnaire, construite dans le sillage de Bitcoin, est sans doute Ethereum. Conceptualisée en 2013 et lancée en 2015 par le précoce Vitalik Buterin, cette blockchain propose une architecture permettant de décentraliser des applications Internet. Ethereum est souvent

1. LESSIG, Lawrence , " Code is Law - On Liberty in Cyberspace " https://harvardmagazine.com/2000/01/code-is-law-html - traduction française: https://framablog.org/2010/05/22/code-is-law-lessig/

assimilé à un grand ordinateur mondial. Schématiquement, ce système tente de supprimer tous les tiers de confiance centralisés au moyen de programmes autonomes intelligents (smart contracts) dont le fonctionnement est garanti par un système d'incitation monétaire comparable à Bitcoin, l'Ether. Un nœud du réseau Ethereum choisit des applications à héberger (décentralisation et résilience) en contrepartie du paiement. A l'heure actuelle, l'écosystème Ethereum fourmille d'initiatives passionnantes et suscite beaucoup d'intérêt pour sa proposition de valeur.

Le mécanisme d'assurance décentralisée décrit plus haut a été expérimenté dans le cadre d'un projet sur la blockchain Ethereum (TheDAO) qui visait à créer un fond d'investissement décentralisé régi par des règles communautaires. Ce projet extrêmement ambitieux et sûrement un peu prématuré a connu une issue dommageable : l'utilisation d'une faille dans le code informatique de cette application décentralisée a permis le siphonage de près de 50 millions de dollars en cryptomonnaie Ether (5% des ethers en circulation).

Afin de préserver la communauté lésée, un vote communautaire a conduit réaliser un " fork " de la chaine Ethereum, consistant en la création d'une nouvelle branche de la chaîne, sur laquelle le fraudeur a été " effacé ". Ce fork a donc entrainé la création de deux chaînes Ethereum : la principale et nouvelle, soutenue par la majorité de l'écosystème dont l'unité de compte demeure l'Ether (ETH), et une chaine dite " classique " sur laquelle le siphonage est toujours visible et dont le token est l'Ether Classic (ETC) (2).

2. POLROT, Simon, "The DAO : post-mortem", 24/01/17 https://www.ethereum-france.com/the-dao-post-mortem/

Ainsi, alors que la " simple " décentralisation de la monnaie et du système de paiement proposée par Bitcoin s'avère être un chantier pharaonique, l'exécution de la vision globale d'Ethereum commence à heurter le mur des réalités souvent opposé à son grand frère. Le chemin à parcourir promet d'être aussi long que passionnant pour parvenir à la réalisation de cette promesse.

Quoi qu'il en soit, la communauté de développeurs et de toutes les intelligences qui travaillent à l'éclosion de ces écosystèmes a franchi une étape cruciale pour l'avenir de la société : **on peut désormais imaginer des services, et pourquoi pas des produits, qui seraient proposés par des sociétés autonomes décentralisées** : plus clairement, des services offerts par des applications n'appartenant pas à des sociétés commerciales.

Les exemples les plus souvent cités concernent les géants Uber et Amazon : il s'agirait de concevoir un service comme Uber, mais sans la société Uber. Ce service pourrait exister dans une forme accessible à tous, indépendante d'une politique tarifaire à géométrie variable, indépendante également de politiques protectionnistes de certains gouvernements : libre, transparent sans censure possible.

L'interdiction en France en 2015 d'Uberpop pour des motifs discutables ne serait plus aussi aisée à effectuer si ce type de service fonctionnait sur des applications décentralisées où aucune société ne puisse être incriminée. Utopique ou irréaliste pour certains, cette perspective se rapproche toutefois car c'est dans cette direction que toute cette nouvelle économie travaille. Dans le domaine du commerce, la startup Openbazaar fait partie des pionnières en œuvrant au développement d'une place de marché décentralisée, sans intervention d'un tiers de confiance. Il ne s'agit plus d'innovation mais de révolution : ces outils permettent de construire une monde numérique avec des adhérences les plus infimes possibles avec l'existant.

Une parfaite illustration de ce défi laborieux concerne à nouveau Bitcoin. Afin d'être résistant à la plus ultime des censures numériques – couper Internet-, ce qui aurait pour effet d'empêcher la diffusion des transactions, et le maintien de la blockchain, les chercheurs testent des alternatives permettant de diffuser les transactions sur des réseaux d'ondes radio (3). La société Blockstream propose quant à elle une diffusion satellitaire de la Blockchain Bitcoin depuis mi-2017 (4).

3. Avec notamment une proposition de Nick Szabo à la conference Scaling Bitcoin en novembre 2017 : https://bitconseil.fr/scaling-bitcoin-7-frais-transaction-resistance-censure/

4. *Bitcoin Magazine*, 24/08/16 : https://bitcoinmagazine.com/articles/how-blockstream-satellite-will-drive-bitcoin-adoption-interview-adam-back-and-chris-cook/

4.2 Le phénomène des ICO

La mode de la " blockchain " repose souvent sur une incompréhension du phénomène Bitcoin et une vision erronée d'Ethereum. De nombreux projets utilisant ce mot fourre-tout prétendent proposer des innovations technologiques qui en réalité n'en sont guère. Tous annoncent que " LA Blockchain " va bouleverser le marché du " [*insérer ce que vous voulez*] ", mais rares sont ceux qui fournissent une explication claire de leur blockchain.

La " blockchain " n'est pas la technologie sur laquelle est fondée Bitcoin, c'est exactement l'inverse. Bitcoin est une invention de 2008, dont le concept a été repris afin d'imaginer une technologie magique, au point que chaque entreprise cherche un problème dont la solution pourrait être " la blockchain ". " Ce qui est intéressant dans Bitcoin, c'est la technologie, pas la monnaie " : cette sentence tant de fois entendue illustre le profond déficit de compréhension de la technologie. Car Bitcoin sans bitcoins n'est rien d'autre qu'une infrastructure de signature électronique centralisée. S'il y a bien une bulle actuellement, elle concerne probablement plus la " blockchain " que Bitcoin.

Comme nous l'avons vu dans la partie 2, Bitcoin est fondé sur un protocole technique, un réseau qui a fait la preuve de son concept depuis bientôt 10 ans et dont la valeur repose en particulier sur ses caractéristiques d'autonomie et de résistance à la censure. La réussite de cette cryptomonnaie aiguise tous les appétits, que de nombreux gourmands tentent de reproduire afin de profiter de l'effet d'aubaine de ces nouveaux tokens/jetons. Le foisonnement de projets auquel nous assistons actuellement est fascinant. Il est primordial de rappeler que ces projets sont souvent expérimentaux et risqués, mais aussi que certains sont de possibles arnaques.

Depuis 2016 apparaissent sur le marché du financement des entreprises un modèle innovant de collecte de fonds en échange de l'émission d'un jeton : les Initial Coin Offerings (ICO).

Initialement, dans la philosophie des blockchains publiques, les ICO servaient des projets pour lesquels le jeton numérique (ou la monnaie) émis avait un rôle indispensable à la vie de la blockchain nouvellement créée. C'est sur ce principe que fut amorcé le projet Ethereum, pour lequel l'autonomie du système ne peut être assu-

rée que par l'existence d'une incitation monétaire. Le token émis est rapidement échangeable sur des bourses en ligne, partout dans le monde, faisant ainsi démarrer la spéculation mais aussi la valorisation de ce nouveau système.

De nombreux observateurs ont vu dans cette démarche de financement une occasion rêvée de collecter des fonds facilement (en termes de calendrier et de contrainte réglementaire) puisque le financement est réalisé en cryptomonnaie. Ainsi démarrait le nouveau tournant de la création et du financement de l'entreprise : imaginer une activité pouvant être " tokenisée ", et pour laquelle le succès se matérialiserait non seulement par le développement structurel de l'entreprise mais aussi par la valorisation d'un jeton, les deux étant idéalement liés.

L'équation est difficile à résoudre et beaucoup de projets s'intéressent à cette nouvelle forme de financement et de modèle économique. La tentation, pour une entreprise, de recourir à ce type de financement est certaine. Il permet d'atteindre et convaincre une communauté sensible à son projet, de l'inciter à devenir actrice du développement du produit ou service en devenant ambassadeur et financeur. Et ce mode de financement apporte d'autres avantages non négligeables : non dilution capitalistique, financement mondial auprès de particuliers ou d'entreprises par des voies rapides, en cryptomonnaie et sans contrainte réglementaire.

> ***La " blockchain " n'est pas la technologie sur laquelle est fondée Bitcoin, c'est exactement l'inverse.***

Les incitations des particuliers sont protéiformes : tout d'abord, ce financement peut être réalisé de façon impulsive, alors qu'un financement de type " crowdfunding " nécessite le passage par un formalisme rebutant avant d'être rassurant. Ensuite, l'attrait pour des gains financiers importants peut venir fausser certaines prises de décision, en espérant des performances futures similaires aux performances passées de certaines ICO. Enfin, et en particulier selon la qualification du token, le souscripteur dispose d'une méthode simple de participation au succès d'une entreprise, dont le token est complètement liquide sur le second marché et offert par toutes les bourses d'échange mondiales.

Si ce mode de financement naissant est scruté par les régulateurs et les fonds d'investissement, il n'en est qu'à son démarrage. Les projets actuellement financés pourraient l'être par les investisseurs traditionnels s'ils étaient moins averses au risque et à ces

modèles technologiques. En revanche, les prochaines années verront l'émergence de projets à nouveau décentralisés, à l'image de TheDAO, et qui ne seront pas représentés sous forme de société commerciale mais sous la forme plus virtuelle d'application décentralisée. Ces applications pourront lever des fonds, opérer des services et distribuer des dividendes à leurs actionnaires...en cryptomonnaie.

4.3 Vers une décentralisation généralisée ?

Une trentaine d'années après Internet, Bitcoin amène progressivement les individus à s'interroger sur la centralisation des pouvoirs et sur la liberté de chacun, avec le corolaire du respect de la vie privée. On ne peut qu'être impressionné par l'intelligence et la puissance des questions qui sont soulevées pour débattre de Bitcoin. Il reste à imaginer que les mêmes questions soient posées sur la création monétaire, le rôle des banques et des États.

Le développement de Bitcoin s'inscrit dans une tendance contemporaine plus globale consistant à s'affranchir du pouvoir ordonné par les traditions séculaires, à se libérer des croyances accumulées avec le temps, à contester les formes d'autorité considérées comme non légitimes. Le scepticisme à l'égard de la démocratie, décrit par Lawrence Lessig en 2000, amène les citoyens à rechercher de nouvelles formes d'organisation plus émancipatrices.

Cet élan de liberté se traduit socialement de diverses manières : augmentation du nombre de créations d'entreprises, avec l'idéal de s'épanouir plus librement, de créer de la valeur par des produits ou services et de s'affranchir du système salarial ; liberté de parole de plus en plus revendiquée, à mesure qu'elle est de plus en plus contrôlée, etc. De plus en plus d'outils sont à disposition pour entreprendre, réaliser, faire, sans demander la permission. S'il fallait attendre l'approbation des régulateurs pour réaliser la vision des inventeurs, toute la création serait censurée au nom du principe de précaution.

Cet élan se manifeste aussi dans la recherche d'un meilleur respect de la vie privée. La dissémination des données sur toutes

formes d'applications, leur utilisation à des fins plus ou moins consenties, et parfois même leur surveillance, sont autant de manifestations de l'empiètement des puissances d'Internet sur la vie privée des individus. Les scientifiques et les cypherpunks avaient déjà identifé ces risques il y a bientôt 30 ans.

Le respect de la vie privée passe par une meilleure maîtrise des données produites par chacun. Le règlement européen sur la protection des données (RGDP), qui entrera en vigueur en mai 2018, reconnait le droit de l'utilisateur à maitriser les données qu'il produit, *a minima* en l'informant de leur existence et de leur traitement.

Le stockage, le partage et valorisation des données personnelles s'appuieront probablement sur des dispositifs inspirés de Bitcoin. Ce dernier permet à chacun de devenir réellement maitre de ses « données monétaires » personnelles en contrôlant les clés privées. On peut très bien envisager que les données personnelles deviennent une nouvelle forme de monnaie numérique dont la valorisation permettra de rééquilibrer le rapport de richesse entre les individus et les grandes plateformes exploitant ces données.

> ***Le développement de Bitcoin s'inscrit dans une tendance contemporaine plus globale consistant à s'affranchir du pouvoir ordonné par les traditions séculaires***

Finalement, Bitcoin ne résulte pas d'un désir infantile de supprimer toute règle : il offre simplement la possibilité (non l'obligation) d'expérimenter un nouveau modèle de monnaie, de réserve de valeur et de protection de la vie privée. Il existe, fonctionne, et réalise cette expérimentation grandeur nature depuis des années.

Certes, une partie importante de l'engouement actuel résulte des hausses des cours des cryptomonnaies. Une partie non négligeable de cette attention repose sur la simple cupidité. Mais la compréhension des enjeux profonds progresse et les populations y sont de plus en plus sensibles. Pour les États, comment réagir face à cette révolution, comment accompagner ces mouvements de liberté et de protection de la vie privée, et comment préparer l'avenir avec clairvoyance et imagination ? Face à une telle révolution technologique et culturelle, les défis qui se posent à eux sont immenses.

4.4 Un défi lancé au droit

4.4.1 Quelle régulation ? Quelle réglementation ?

Combien de temps faudra-t-il encore entendre dire parler de schéma de Ponzi à propos de Bitcoin ?

Dans le système Bitcoin, aucune entité ne promet de rendement quelconque, et le mécanisme est complètement auditable (5). Les réactions premières face à Bitcoin sont très émotionnelles. Le percevant comme un danger ou une menace, certains tentent d'évacuer rapidement la question. Ce schéma de réactions a été observé dans le monde entier, où la valse-hésitation des régulateurs et autres bras armé des États ne fait qu'accélérer dans la frénésie actuelle.

Personne ne peut techniquement arrêter Bitcoin mais tout le monde peut formuler le vœu pieux de l'interdire (il n'est d'ailleurs pas certain que Bitcoin aurait le même succès si soudainement tous les États et régulateurs l'adoubaient).

L'industrie née avec Bitcoin est en pleine explosion, créant entreprises, emplois, pôles de recherche, nouveaux vecteurs éducatifs. En 2015, l'état de New York a été l'un des premiers à encadrer strictement les activités Bitcoin, entrainant rapidement le départ de toutes les initiatives vers d'autres états ou pays. Aujourd'hui, certains états comme Monaco (cf. infra) se positionnent de façon très ouverte et incitative pour le développement des activités liées aux cryptomonnaies. Le Japon avait ouvert la voie à ces initiatives en reconnaissant Bitcoin comme un moyen de paiement légal (6).

Un précédent en matière de régulation d'un système P2P existe : le protocole de partage de fichiers Bittorrent, né en 2001. Un des usages de ce protocole est le partage d'œuvre artistiques protégées. Depuis son lancement, le réseau Bittorrent est voué aux gémonies par toute une industrie. Sans entrer dans le débat du droit d'auteur et de sa rémunération, on peut se demander comment cette industrie aurait évolué si elle s'était emparé de la technologie dans les années 2000, et si elle avait tenté de l'utiliser à son avantage, plutôt que de l'ignorer ou de la combattre. Elle a obtenu des régulateurs qu'ils interdisent le téléchargement

5. Face à cette accusation particulièrement absurde, une simple réponse devrait suffire : a-t-on jamais vu un système de Ponzi *open source* ?

6. http://www.conseil-national.mc/index.php/textes-et-lois/propositions-de-loi/les-propositions-de-loi-en-cours/item/600-237-proposition-de-loi-relative-a-la-blockchain

7. Bien entendu, pour une explication de ces idées, il convient de se reporter au travail magistral effectué par les économistes de " l'école autrichienne ", en particulier Friedrich Hayek (" The Use of knowledge in society ", The *American Economic Review*, XXXV, n°4, septembre 1945 ; *Droit, législation et liberté*, vol. I, Paris, PUF, 1980) ou Ludwig von Mises (*L'Action humaine*, Paris, PUF, 1985).

" illégal " et qu'ils s'efforcent de limiter le développement de cette technologie rendant pourtant un service de grande valeur et résistant à la censure. On a vu le résultat.

Pour ce domaine nouveau que représentent les technologies et activités héritées de Bitcoin, comme pour beaucoup d'autres sujets, le débat sur la " régulation " est souvent faussé par l'ambiguïté qui entoure cette notion : régulation ne devrait pas être synonyme de réglementation (cf. encadré suivant).

La confusion régulation / réglementation

> *" Par régulation, on entend en général et à tort " règlementation ". Ce faisant on est une victime - consentante - d'une confusion linguistique :* ***en anglais en effet, le terme régulation veut dire " réglementation " et la contagion des langues conduit naturellement à assimiler régulation à " réglementation " et à laisser entendre que la déréglementation entraîne une dérégulation, c'est-à-dire le désordre.*** *C'est oublier que la régulation d'un système humain se réalise au mieux par des processus de coordination spontanés entre individus libres, et donc motivés pour agir de la manière la mieux adaptée à la poursuite de leurs objectifs, en tenant compte de leur interdépendance avec autrui, telle qu'elle se manifeste par le système de prix, par les moyens d'information, par les règles juridiques ou par la tradition.*
>
> *Le recours à un système décentralisé permet de mobiliser au mieux toutes les informations détenues – et surtout créées – par les individus membres d'une société (7). Certes en laissant la liberté à chacun d'agir en fonction de ses propres objectifs et de ses informations - mais surtout en respectant les droits légitimes d'autrui -, on n'aboutit pas à une société parfaite car la perfection n'existe pas et elle est d'ailleurs indéfinissable. Mais on arrive en tout cas à une société plus juste et plus conforme aux aspirations des uns et des autres ".*
>
> **Pascal Salin, Français,** *N'ayez pas peur du libéralisme* **(2007) (8)**

8. SALIN, Pascal, *Français, N'ayez pas peur du libéralisme*, Odile Jacob, 2007

Face à la révolution issue de Bitcoin, les régulateurs devraient adopter une attitude raisonnable. Il convient de maintenir aussi faible que possible le poids de la fiscalité et des obligations réglementaires pesant sur les entrepreneurs, les investisseurs, les créateurs et les consommateurs. Il est aussi important de facili-

ter l'activité des entreprises en clarifiant le traitement juridique et comptable de ces nouvelles activités et de ces nouveaux instruments : l'innovation est un processus suffisamment risqué pour que les pouvoirs publics n'y ajoutent pas du risque inutile à travers le flou ou les variations de la réglementation.

Des réglementations trop strictes ou inadaptées passeraient à côté de l'une des dimensions majeures du phénomène des cryptomonnaies et des ICO : elles offrent des outils de financement et d'incitation novateurs particulièrement précieux pour l'innovation en matière protocoles réseau (cf. encadré suivant).

Cryptomonnaies et innovation en matière de protocoles réseau

> " ***C'est ainsi qu'il faut regarder les cryptomonnaies : une tentative de relancer l'innovation dans le domaine des protocoles réseau, aujourd'hui délaissés par les géants d'internet.*** *La principale fonctionnalité d'une cryptomonnaie, c'est en effet d'intéresser les premiers utilisateurs d'un nouveau protocole à son déploiement à plus grande échelle. Plus nombreux sont les individus qui achètent les cryptomonnaies (comme le bitcoin) liées à un protocole, plus ils contrinuent à augmenter son échelle d'opération ; et plus ce protocole est utilisé, plus la valeur des cryptomonnaies augmente, ce qui permet de rémunérer les premiers utilisateurs pour le rôle crucial qu'ils ont joué à l'amorçage. (...)*
>
> *Les créateurs de protocoles ont compris cette dynamique. Ils ont imaginé les cryptomonnaies non pour spéculer, mais pour orchestrer l'émergence et le déploiement d'une nouvelle génération de protocoles réseau et ainsi combcler les lacunes du Code de la Route sur internet ".*
>
> **Nicolas Colin, "** *Cryptomonnaies, un peu de cohérence* **", L'Obs, 25/01/18**

La compétition mondiale est engagée. Le capital et les talents sont largement mobiles. Impossible, à ce stade, de savoir combien d'emplois seront détruits et créés par cette révolution. **Le dilemme qui s'offre à nous est identique à celui rencontré lors de chaque " grappe d'innovations " au sens de Schumpeter**.

D'un côté, nous focaliser sur les risques supposés de la technologie en refusant obstinément d'en reconnaître les côtés

prometteurs et laisser les pouvoirs publics céder à la " capture du régulateur " théorisée par le prix Nobel d'économie George Stigler (9) qui rend rentable pour les intérêts en place d'obtenir des " régulations " limitant l'émergence de nouveaux concurrents.

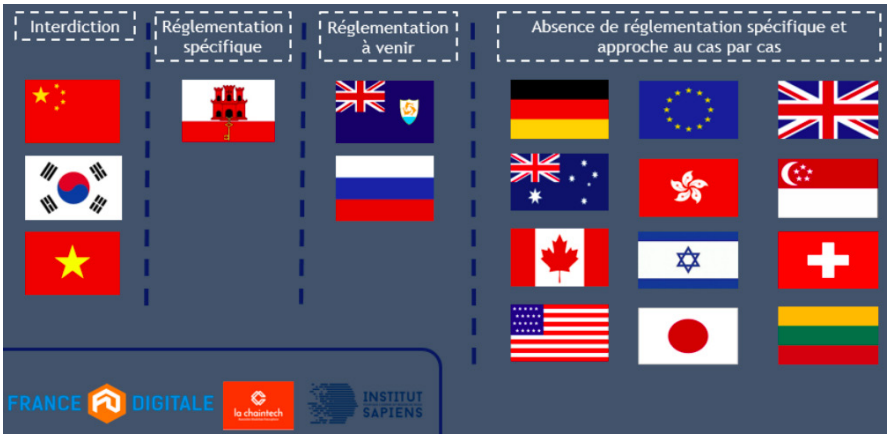
Ou, de l'autre, faire confiance aux mécanismes qui ont, depuis quelques siècles, permis la plus grande création de richesse et de prospérité au service de l'humanité : recherche scientifique, innovation technologique, liberté d'entreprendre et d'expérimenter, respect de la propriété privée, accumulation du capital, libre échange, concurrence.

9. https://www.wikiberal.org/wiki/George_Stigler#La_th.C3.A9orie_de_la_capture

4.4.2 L'exemple des ICO

Les réglementations sur les ICO dans le monde sont encore balbutiantes et chaque pays expérimente sa propre voie, comme le montre le schéma suivant.

Les différentes approches des régulateurs nationaux en matière d'ICO



Source : France Digitale, Chaintech, Institut Sapiens, janvier 2018

Il serait souhaitable que la France adopte une position remarquable pour renforcer l'attractivité de son territoire. Les propositions de France Digitale et la Chaintech, en partenariat avec l'Institut Sapiens (cf. encadré suivant) (10) sont raisonnables et intéressantes mais **il serait possible d'envisager un cadre plus ambitieux, offrant plus de souplesse, et permettant une meilleure responsabilisation des acteurs**.

10. *Réglementation des Initial Coin Offerings (ICO): un oxymore?* Etude réalisée par France Digitale et la Chaintech, en partenariat avec l'Institut Sapiens, janvier 2018. https://www.institutsapiens.fr/reglementation-des-initial-coin-offerings-ico-un-oxymore/

Principales propositions de France Digitale et de la Chaintech en matière d'ICO

- Ne pas limiter le nombre d'acquéreurs, qui rendrait caduque les effets de réseau.

- Limiter les risques que les ICOs servent au blanchiment d'argent ou au financement du terrorisme, en instaurant une politique de KYC (« know your customer »). Cependant, ce processus doit être suffisamment souple pour ne pas brider l'innovation, tout en fournissant les garanties nécessaires pour protéger l'acquéreur.

- Editer un white paper actualisé chaque année est nécessaire. Cette documentation juridique doit comprendre les conditions générales, la description du projet, les modalités juridiques et une information technique pour informer l'investisseur.

- Sécuriser les opérations ICOs en créant un compte de séquestre permettant de bloquer les fonds collectés et en développant des procédures de gouvernance au moyen de plusieurs signatures simultanées (" multi-sig wallet ").

- Définir un modèle comptable et le traitement fiscal des jetons (les plus-valus liées à ces investissements sont aujourd'hui imposé à 66,2%).

Toute contrainte non indispensable imposée aux start-tups et aux investisseurs aura des effets négatifs non nécessairement visibles mais contreproductifs, qui diminueront l'attractivité de la France sur ce marché totalement internationalisé. **Si toute nouvelle réglementation est toujours justifiée explicitement par les effets positifs recherchés, elle suscite néanmoins nécessairement des effets invisibles, indirects, progressifs, souvent négatifs, dont l'anticipation et l'analyse sont systématiquement négligés lors de la conception des réglementations**. Ce phénomène, qui est une constante historique de l'action publique, a été particulièrement bien mis en lumière en 1850 par Frédéric Bastiat dans son magistral *Ce qu'on voit et ce qu'on ne voit pas* (11).

Une voie courageuse pourrait être d'instaurer un bac à sable (" sandbox ") au sein duquel les projets d'ICO bénéficieraient d'une liberté juridique forte, permettant par exemple de proposer de nouvelles formes d'actions au porteur, librement

11. " *Dans la sphère économique, un acte, une habitude, une institution, une loi n'engendrent pas seulement un effet, mais une série d'effets. De ces effets, le premier seul est immédiat ; il se manifeste simultanément avec sa cause, on le voit. Les autres ne se déroulent que successivement, on ne les voit pas ; heureux si on les prévoit. Entre un mauvais et un bon Économiste, voici toute la différence : l'un s'en tient à l'effet visible ; l'autre tient compte et de l'effet qu'on voit et de ceux qu'il faut prévoir. Mais cette différence est énorme, car il arrive presque toujours que, lorsque la conséquence immédiate est favorable, les conséquences ultérieures sont funestes, et vice versa. — D'où il suit que le mauvais Économiste poursuit un petit bien actuel qui sera suivi d'un grand mal à venir, tandis que le vrai économiste poursuit un grand bien à venir, au risque d'une petit mal actuel* ". Frederic Bastiat, *Ce Qu'on voit et ce qu'on ne voit pas* (1850). Texte intégral : http://bastiat.org/fr/cqovecqonvp.html

échangeables. Dans ce cadre, la question épineuse de la connaissance du client doit être affrontée avec réalisme : une procédure lourde de KYC (connaissance du client lors de l'entrée en relation commerciale - Know Your Customer) est-elle cohérente avec le fait que le token soit échangeable sur des plate-formes parfois décentralisées ?

Le sujet fiscal sur ces tokens s'avère également d'une redoutable complexité. Les tokens (d'utilité ou quasi-actions) comme les cryptomonnaies ne sont actuellement pas qualifiés. Ce désert conduit à appliquer la pire fiscalité qui existe, avec une imposition supérieure à 60% des plus-values réalisées sur ces nouveaux actifs. Qualifier trop rapidement des tokens peut être préjudiciable pour le développement rapide de cette économie. En même temps, ne pas le qualifier entraîne l'application d'une fiscalité qui fait déjà fuir les premiers entrepreneurs et financiers de cette économie.

Face à autant de nouveautés, notre pays a l'opportunité de promouvoir des positions ambitieuses, d'adopter des postures et des réglementations progressives, d'imaginer une fiscalité qui lui permettra d'attirer des entreprises et des talents du monde entier.

Il peut s'inspirer de l'exemple de la principauté de Monaco, dont le Conseil National a adopté en décembre une remarquable " proposition de loi relative à la blockchain ", particulièrement volontariste et attractive (cf. encadré suivant) (12).

L'exposé des motifs souligne qu'*" un argument de stratégie économique internationale milite fortement en faveur de l'adoption d'un cadre juridique large, ouvert à toutes les blockchains, financières et non financières. La Principauté, si elle était le premier État au monde à promouvoir et à sécuriser l'activité des blockchains, ne manquerait pas d'attirer vers son territoire une activité économique prometteuse et à très haute valeur ajoutée ".* De même, le rapport de **M. Thierry Poyet** au nom de la Commission de Législation indique clairement que *" ce qui importe, c'est d'imaginer les utilisations qui pourront être faites, ou du moins d'essayer de construire un cadre législatif novateur, favorisant la venue sur notre territoire de sociétés innovantes, à très haute valeur ajoutée, pouvant demain contribuer au développement du Pays, à son attractivité et à sa notoriété ".*

12. Elle a six mois pour être validée par le gouvernement. http://www.conseil-national.mc/index.php/textes-et-lois/propositions-de-loi/les-propositions-de-loi-en-cours/item/600-237-proposition-de-loi-relative-a-la-blockchain

Article 7 de la proposition de loi relative à la blockchain adoptée le 21/12/17 à Monaco

" La Principauté de Monaco encourage l'expérimentation en matière de blockchain (chaîne de blocs), de smart contracts (contrats intelligents), de processus algorithmiques et de monnaies cryptographiques afin que les innovations prometteuses puissent se concrétiser, être testées sur le marché et avoir la possibilité d'être adoptées largement, tant à Monaco qu'à l'étranger.

La Principauté de Monaco organise à cet effet l'expérimentation pour une durée de trois années, par les entreprises qui le souhaitent, de manière à favoriser le développement de toutes solutions s'appuyant sur les blockchains (chaînes de blocs), les smart contracts (contrats intelligents), les processus algorithmiques ou les monnaies cryptographiques. Elle peut mettre ainsi à disposition desdites entreprises les moyens matériels nécessaires à cette expérimentation, ***en les assurant durant la période susmentionnée, de l'absence de contraintes d'ordre réglementaire ".***

5. Conclusion

En 2005, le controversé Ray Kurzweil publiait un livre qui allait poser les bases de pratiquement tout le débat mondial sur les nouvelles technologies jusqu'à aujourd'hui, notamment en matière d'intelligence artificielle : *The Singularity is near*. Ce qu'il appelle " singularité " est ce moment à venir où le progrès technologique exponentiel deviendra si rapide que nos esprits d'aujourd'hui sont incapables d'en penser toutes les conséquences.

Aujourd'hui, une forme de singularité se rapproche aussi en matière monétaire. Le bitcoin et les cryptomonnaies s'apprêtent à nous faire changer de monde, avec des conséquences particulièrement difficiles à imaginer.

Une prise de conscience est urgente.

Face au web dans les années 1990, la France a connu une forme de " marginalisation paradoxale " : alors qu'elle avait tous les atouts pour devenir un leader de cette révolution économique et culturelle, elle s'est laissée distancer, évincer de la compétition mondiale. Elle et l'Europe ont ensuite reproduit le même schéma avec l'intelligence artificielle. Aujourd'hui, notre pays risque de subir le même sort avec le bitcoin et les technologies qui en découlent.

Les cryptomonnaies vont devenir plus faciles à utiliser, leur nombre va probablement se multiplier dans des proportions aujourd'hui inimaginables, et elles seront de plus en plus difficiles à contrôler par les États. Avec toutes les technologies issues

de Bitcoin, la monnaie devient programmable, ce qui ouvre une nouvelle ère de décentralisation des institutions et d'autonomie pour les individus. Il ne s'agit pas d'un phénomène seulement économique mais aussi sociétal, culturel, presque civilisationnel.

Face à cette révolution, les régulateurs devraient adopter une attitude raisonnable. Il convient de maintenir aussi faible que possible le poids de la fiscalité et des obligations réglementaires pesant sur les entrepreneurs, les investisseurs, les créateurs et les consommateurs. Il est aussi important de faciliter l'activité des entreprises en clarifiant le traitement juridique et comptable de ces nouvelles activités et de ces nouveaux instruments.

La compétition mondiale est engagée. Le capital et les talents sont largement mobiles. Impossible, à ce stade, de savoir combien d'emplois seront détruits et créés par cette révolution. Le dilemme qui s'offre à nous est identique à celui rencontré lors de chaque " grappe d'innovations " au sens de Schumpeter : d'un côté, nous focaliser sur les risques supposés de la technologie en refusant obstinément d'en reconnaître les côtés prometteurs et laisser les pouvoirs publics céder à la " capture du régulateur " qui rend rentable pour les intérêts en place d'obtenir des " régulations " limitant l'émergence de nouveaux concurrents ; ou, de l'autre, faire confiance aux mécanismes qui ont, depuis quelques siècles, permis la plus grande création de richesse et de prospérité au service de l'humanité : recherche scientifique, innovation technologique, liberté d'entreprendre et d'expérimenter, respect de la propriété privée, accumulation du capital, libre échange, concurrence.

6. Annexes

6.1 The Crypto Anarchist Manifesto (Timothy May, 1988)

Texte intégral. Source : http://nakamotoinstitute.org/crypto-anarchist-manifesto/

“ A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the

past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences! ”

6.2 A Cypherpunk's Manifesto (Eric Hughes, 1993)

Texte intégral. Source : http://nakamotoinstitute.org/cypherpunk-manifesto/

" Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must _always_ reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward ".

6.3 Extrait du white paper Bitcoin (Satoshi Nakamoto, 2008)

Traduit de l'anglais. Source : https://bitcoin.fr/bitcoin-explique-par-son-inventeur/

Texte original : https://bitcoin.org/bitcoin.pdf

" **Résumé.** Un système de monnaie électronique entièrement en pair-à-pair permettrait d'effectuer des paiements en ligne directement d'un tiers à un autre sans passer par une institution financière. Les signatures numériques offrent une telle solution, mais perdent leur intérêt dès lors qu'un tiers de confiance est requis pour empêcher le double paiement. Nous proposons une solution au problème du double paiement en utilisant un réseau pair-à-pair. Le réseau horodate les transactions à l'aide d'une fonction de hachage qui les traduit en une chaîne continue de preuves de travail (des empreintes), formant un enregistrement qui ne peut être modifié sans ré-effectuer la preuve de travail. La plus longue chaîne (d'empreintes) sert non seulement de preuve du déroulement des évènements constatés, mais également de preuve qu'elle provient du plus grand regroupement de puissance de calcul. Aussi longtemps que la majorité de la puissance de calcul (CPU) est contrôlée par des nœuds qui ne coopèrent pas pour attaquer le réseau, ils généreront la plus longue chaîne et surpasseront les attaquants. Le réseau en lui-même ne requiert qu'une structure réduite. Les messages sont diffusés au mieux, et les nœuds peuvent quitter ou rejoindre le réseau à leur gré, en acceptant à leur retour la chaîne de preuve de travail la plus longue comme preuve de ce qui s'est déroulé pendant leur absence.

6.3.1 1. Introduction

Le commerce sur Internet dépend aujourd'hui presque exclusivement d'institutions financières qui servent de tiers de confiance pour traiter les paiements électroniques. Bien que ce système fonctionne plutôt bien pour la plupart des transactions, il écope toujours des faiblesses inhérentes à son modèle basé sur la confiance. Les transactions totalement irréversibles n'y sont pas vraiment possibles, puisque les institutions financières doivent gérer la médiation de conflits. Le coût de cette médiation augmente les coûts des transactions, limitant en pratique la taille minimale d'une transaction et empêchant la possibilité d'avoir des petites transactions peu coûteuses. L'impossibilité d'avoir des paiements non réversibles pour des services non réversibles engendre un coût encore plus important. Avec la possibilité d'inverser les transactions, le besoin de confiance augmente. Les marchands doivent se méfier de leurs clients, en les harcelant pour obtenir plus d'informations que nécessaire. Une certaine part de fraudes est acceptée comme inévitable. Tous ces coûts et incertitudes de paiement peuvent être évités par l'utilisation d'une monnaie physique, mais aucun mécanisme n'existe pour réaliser des paiements à travers un système de communication sans avoir recours à un tiers de confiance.

Ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur des preuves cryptographiques au lieu d'un modèle basé sur la confiance, qui permettrait à deux parties qui le souhaitent de réaliser des transactions directement entre elles sans avoir recours à un tiers de confiance. Les transactions qui sont informatiquement impossibles à annuler protégeraient les vendeurs de fraudes éventuelles, et un système de compte séquestre pourrait facilement être implémenté pour protéger les acheteurs. Dans ce document, nous proposons une solution au problème de double-dépense en utilisant un serveur horodaté distribué en pair-à-pair pour générer des preuves informatiques de l'ordre chronologique des transactions. Le système est sécurisé tant que des nœuds honnêtes contrôlent ensemble plus de puissance de calcul qu'un groupe de nœuds qui coopéreraient pour réaliser une attaque ".

6.4 Les erreurs de l'approche keynésienne

Extrait de : SALIN, Pascal, " Que peut-on demander à la politique monétaire ", Fondation Politique, mai 2014

Source : http://www.fondapol.org/wp-content/uploads/2014/05/056-SALIN-2014-07-09-web-Que-peut-on-demander-%C3%A0-la-politique-mon%C3%A9taire.pdf

" La théorie keynésienne considère que, dans certaines circonstances « normales », la politique monétaire peut avoir un effet positif sur l'activité économique. En effet, pour les raisons indiquées ci-dessus, une expansion monétaire implique une baisse du taux d'intérêt, ce qui stimulerait l'investissement. Dans une perspective keynésienne, cette augmentation de l'investissement est désirable, non pas parce qu'elle permettrait d'accroître la capacité productive, et donc ultérieurement la production, mais tout simplement parce qu'elle est censée accroître la demande globale, et donc la production. Nous aurons par la suite l'occasion de discuter cette proposition, mais restons pour le moment dans le cadre de la théorie keynésienne. Celle-ci se focalise, non pas sur cette situation « normale », mais sur une situation particulière qui est censée expliquer un équilibre de sous-emploi pour lequel, au demeurant, la politique monétaire perd sa capacité à stimuler l'investissement et la demande globale.

Sous le prétexte de développer une théorie macroéconomique générale, et plus particulièrement pour expliquer le chômage, Keynes a choisi un ensemble d'hypothèses très spécifiques qui, en les combinant, sont censées expliquer le chômage, et donc aider à la définition des politiques économiques à mettre en œuvre pour retrouver le plein-emploi. Le point de départ de la démonstration consiste à supposer que, pour une raison inexpliquée, il y a soudain une chute de l'investissement et donc un excès d'épargne. Une telle situation n'a pas de cause endogène, c'est-à-dire qu'elle ne résulte pas du fonctionnement normal du système économique ou même d'un choc extérieur, elle est tout simplement le résultat des « esprits animaux » des entrepreneurs qui deviennent tout d'un coup sceptiques à l'égard des développements économiques futurs, et préfèrent ne pas investir. Pour les économistes classiques, dans un tel cas, le taux d'intérêt devrait diminuer, ce qui ouvrirait de nouvelles opportunités d'investissement et réduirait l'épargne, de telle sorte qu'il y aurait

un retour à l'équilibre sur le marché des fonds prêtables. Mais, a n de poursuivre son propre but intellectuel, Keynes se doit d'inventer quelques mécanismes susceptibles d'empêcher que ce processus d'ajustement puisse se produire. Il y arrive en faisant deux hypothèses ad hoc, à savoir l'existence d'une trappe à liquidités, et l'inélasticité de l'investissement au taux d'intérêt.

Il n'est pas nécessaire, dans le cadre de la présente étude, d'insister sur ces deux hypothèses. Mais il est tout de même remarquable que ces deux hypothèses – qui sont le cœur de la théorie keynésienne puisqu'elles permettent de définir un équilibre de sous-emploi – soient totalement arbitraires et contraires aux fondements mêmes de toute analyse économique sérieuse. En effet, l'une et l'autre supposent implicitement que les agents économiques ne sont pas rationnels, soit parce que les investisseurs ne seraient pas sensibles aux signaux de taux d'intérêt, soit parce que les individus conserveraient des encaisses inutiles au lieu de les utiliser. On peut donc s'interroger sur ce paradoxe extraordinaire par lequel l'une des théories économiques les plus célèbres, la théorie keynésienne, est en fait l'une des théories les plus arbitraires et les moins réalistes. Elle doit probablement sa célébrité au fait qu'elle apporte aux gouvernements un alibi incomparable pour pratiquer des déficits budgétaires : grâce à Keynes, ils peuvent toujours prétendre agir ainsi pour permettre la « relance économique ». Mais il serait temps d'oublier la théorie keynésienne et de refuser d'appeler « politique de relance » une politique de déficit budgétaire. De manière plus générale, il est erroné de penser que l'activité économique puisse être stimulée par une augmentation de la demande globale obtenue soit par la politique budgétaire, soit par la politique monétaire (soit par les deux, comme tant de pays ont malheureusement essayé de le faire récemment pour sortir d'une crise qui n'avait strictement rien de keynésien) ".

6.5 La théorie autrichienne des cycles économiques

Extrait d'un entretien entre Cécile Philippe, directrice de l'Institut Economique Molinari, et Grégoire Canlorbe (03/12/03).

Source : https://www.institutcoppet.org/2014/12/03/entretien-avec-cecile-philippe-par-gregoire-canlorbe

" A l'inverse de Keynes, les économistes de l'école d'économie autrichienne voient dans les manipulations monétaires la cause des cycles économiques. Loin d'être inhérent à nos systèmes dits capitalistes, ils sont la conséquence d'un trop grand laxisme dans la création de monnaie.

Selon eux, un excès de monnaie – créé en multipliant les crédits offerts – va financer des projets d'investissement qui ne pourront pas tous être terminés, faute de ressources réelles. Au fur et à mesure que les acteurs vont s'en rendre compte, ils vont dans un premier temps chercher par tous les moyens des ressources pour finir leurs projets. Faute de les trouver, ils devront mettre la clé sous la porte. Ils se verront donc dans l'incapacité de rembourser les emprunts qui leur ont permis de se lancer dans ces aventures, menaçant ainsi la solvabilité des banques qui leur ont fait ces prêts.

La faillite d'un entrepreneur n'est pas un drame majeur pour la collectivité dans son ensemble. Elle peut être gérée assez facilement, en accompagnant l'entrepreneur concerné, ses salariés et ses créanciers.

En revanche, le problème est dû au fait qu'il arrive qu'un très grand nombre d'entrepreneurs fassent faillite au même moment. Il n'est plus question de la faillite d'un seul entrepreneur, mais d'un grand nombre d'entre eux qui font ensemble des malinvestissements. L'ampleur des erreurs ainsi commises rend impossible un atterrissage en douceur.

Le problème vient de ce que la création monétaire, qui s'exprime à travers une politique généreuse de crédit, suscite de véritable " cycles d'erreurs " Elle trompe de nombreux acteurs, en leur permettant de se lancer dans des projets qui se révéleront impossibles à terminer et qui seront donc générateurs de pertes.

Car ces nouveaux crédits émis de façon excessive trouveront acquéreur à des taux d'intérêt artificiellement bas. Or les taux d'intérêt sont une référence pour évaluer la profitabilité d'un projet. Lorsqu'on les manipule, on brouille la vision de l'entrepreneur et sa capacité à anticiper correctement ses profits et ses pertes potentiels. Le calcul économique, dont nous avons vu qu'il était nécessaire à un développement rationnel et durable, s'en trouve faussé.

Sur un marché libre, les taux d'intérêt résultent de la préférence temporelle des individus pour le présent. Vous comme moi préférons bénéficier immédiatement des services d'un bien plutôt que de devoir en profiter plus tard. Il est ainsi préférable d'avoir 100 euros aujourd'hui plutôt que demain. Pour se séparer de l'usage de ces 100 euros aujourd'hui, il faut espérer en avoir non pas 100 demain mais, par exemple, 105. Dans un tel cas, le taux d'intérêt est de 5 %. Ce taux reflète la préférence pour le présent. Plus ce taux est élevé, plus la préférence pour le présent est forte, et plus il est faible, plus la préférence pour le présent est réduite.

Les taux d'intérêt sont donc normalement des prix supposés refléter la quantité d'épargne que les individus sont prêts à mettre à la disposition d'investisseurs, leur permettant ainsi de mener à bien leurs projets. Quand on manipule à la baisse ces taux, on laisse penser qu'il existe un stock d'épargne plus important et surtout que la volonté de consommer est moindre que ce qu'elle n'est en réalité. Ce point est fondamental pour comprendre que tous les projets lancés sur la base de taux d'intérêt faussés ne pourront pas tous être menés à bien.

En effet, la pression à la baisse des taux d'intérêt va inciter des entrepreneurs à se lancer dans des projets de durée de plus en plus longue, puisque les taux en vigueur indiquent – au moins sur le papier – qu'il est maintenant rentable de les lancer. Or, des projets de plus longue durée, c'est-à-dire plus capitalistiques, nécessitent une immobilisation plus longue de nombreuses ressources, dont il va falloir s'assurer la disponibilité pendant tout le processus de production.

Or, c'est justement là que les choses s'enveniment. En effet, puisque la préférence pour le présent des individus n'a pas changé, aucune ressource réelle n'a été libérée des processus de production visant la consommation immédiate où la demande reste inchangée.

Par conséquent, pour obtenir les ressources en travail, matières premières, etc., indispensables à la réalisation de ces projets plus capitalistiques, il va devenir nécessaire d'enchérir sur le prix des biens en question, ce qui alimente des bulles sur les marchés concernés. Ce faisant, la marge de profitabilité des projets va diminuer par rapport aux projets qui satisfont plus rapidement les besoins des consommateurs.

Ce renchérissement du prix des matières premières va aussi susciter des besoins de liquidités supplémentaires auprès des banques. Si celles-ci sentent leur solvabilité menacée, elles peuvent décider de ne plus octroyer de nouveaux crédits provoquant ainsi la faillite des entrepreneurs en question. C'est d'autant plus probable que le renchérissement des prix peut être à l'origine de tensions à la hausse du niveau général des prix, incitant les banques centrales à remonter leurs taux directeurs rendant le refinancement des banques commerciales plus difficile.

C'est alors que la bulle éclate avec fracas et entraîne l'arrêt de nombre de projets, la faillite en cascade d'entreprises et l'augmentation du taux de chômage. Ces phénomènes sont la preuve que de nombreux malinvestissements ont été produits. Ils montrent aussi que des ajustements au sein de la structure de production sont nécessaires.

La spécificité de l'école d'économie autrichienne est ainsi de montrer les effets de la création monétaire sur la structure de production, à savoir qu'elle est augmentée de façon artificielle et insoutenable et doit être diminuée pour se réadapter aux préférences des consommateurs.

Enfin, la crise des subprimes me semble être le parfait exemple du cycle économique et j'y consacre d'ailleurs un chapitre dans mon dernier livre. Plus encore, on ne peut vraiment pas accuser cette crise d'être le symbole d'un capitalisme débridé quand on analyse les faits d'un peu plus près. Car que constate-t-on à ce sujet ? Qu'elle est le pur produit de l'interventionnisme, et ce,

– dans le domaine monétaire, avec une politique monétaire accommodante de la part de la Fed, la monnaie rappelons-le restant un bien public,

– dans le domaine bancaire, le Community reinvestment act visant à favoriser les crédits auprès des minorités défavorisées,

– et enfin dans le domaine foncier, l'explosion des prix s'étant concentrée là où dès les années 70, les politiques dites de " déve-

loppement intelligent ” ont limité l’usage du foncier. Le tout s’est accompagné d’un marché immobilier “ distordu ” où des entités que je qualifierais de faussement privées comme Fannie Mae et Freddie Mac ont permis et facilité l’accumulation de crédits de qualité de plus en plus faible.

Dans un tel contexte, ceux qui ont accusé les fameuses déréglementations bancaires – qui ont effectivement permis aux quelques 9 000 banques américaines de se développer sur l’ensemble du territoire plutôt que de rester confiner à des activités dans leur État de création – ne voient que la toute petite partie émergée de l’iceberg.

Bien loin de la vision, trop souvent répandue, d’un marché américain qui aurait pâti d’une déréglementation à outrance, l’histoire montre au contraire que les subprimes sont une coproduction des pouvoirs publics et d’acteurs privés chargés d’exécuter leurs souhaits ”.

Réalisation & conception : Gwenaël Bony
Février 2018