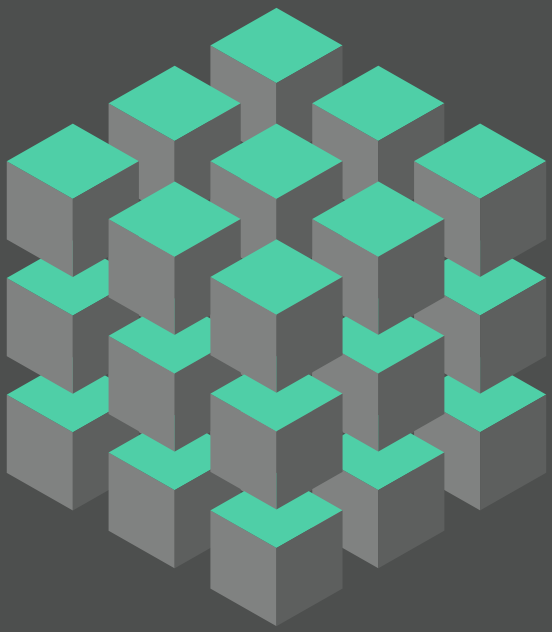
NOUVELLE ÉDITION AUGMENTÉE



BLOCKCHAIN

VERS DE NOUVELLES CHAÎNES DE VALEUR

MARTIN DELLA CHIESA

FRANÇOIS HIAULT

CLÉMENT TÉQUI

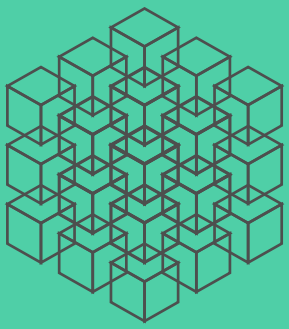
AVEC

NICOLAS BOUZOU ET THIBAUT GRESS

PROSPECTIVES Accuracy

Éditions EYROLLES

Rupture technologique, phénomène économique et sociétal, la Blockchain est devenue en quelques années un terme familier, une promesse de futur transformé, une notion centrale. Adulée ou détestée, elle reste cependant mal comprise, car complexe et singulière. Pour autant, maîtriser cette innovation est devenu indispensable pour cerner les nouvelles règles du jeu de l'économie mondiale. C'est l'objet de cet ouvrage.



Trop souvent réduite aux seules questions de confiance et de décentralisation, la Blockchain est ici restituée selon toute sa densité par une approche pluridisciplinaire : racontée dans son épaisseur historique, pédagogiquement décrite du point de vue technique, envisagée selon ses applications économique et financière, elle fait également l'objet d'une analyse philosophique destinée à en cerner la singularité.

Les auteurs expliquent dans son intégralité une révolution qu'ils considèrent de l'ampleur de celle d'Internet. Ils donnent ainsi à tous les clés de compréhension et les leviers d'action stratégique face à ce *new deal* technologique, économique et social.

Bloc par bloc.

www.editions-eyrolles.com

PROSPECTIVES
Accuracy

MARTIN DELLA CHIESA

Martin Della Chiesa est manager chez Accuracy et est en charge des activités Blockchain du cabinet. Plus généralement, il intervient sur des problématiques stratégiques, de *business planning* et de transactions, avec un focus important sur le secteur des services financiers, les nouveaux *business models* et la Fintech. Avant de rejoindre Accuracy en 2016, Martin Della Chiesa a passé quatre ans au sein du groupe BPCE, d'abord à la banque d'investissement puis à l'Inspection générale. Cofondateur du projet Blockchain au sein d'Accuracy, il s'intéresse plus particulièrement à la discipline émergente de *token-economy* et aux impacts économiques, stratégiques et financiers de la technologie. Diplômé de l'Institut d'études politiques de Strasbourg, il enseigne à l'université Paris-Dauphine et à Sciences Po Paris.

FRANÇOIS HIAULT

Diplômé de l'ISAE-SUPAERO, François Hiault a travaillé en audit financier avant de rejoindre le cabinet Accuracy en 2016, au sein duquel il intervient sur des problématiques de valorisation de produits financiers complexes, de diligences financières et stratégiques. Cofondateur de l'initiative Blockchain au sein d'Accuracy, il s'est particulièrement intéressé aux questionnements économique et financier autour du *token* et a réalisé plusieurs missions en lien avec ces problématiques. Il porte également un fort intérêt à la technologie, à travers le développement de *smart contracts*. François Hiault enseigne à l'université Paris-Dauphine.

CLÉMENT TÉQUI

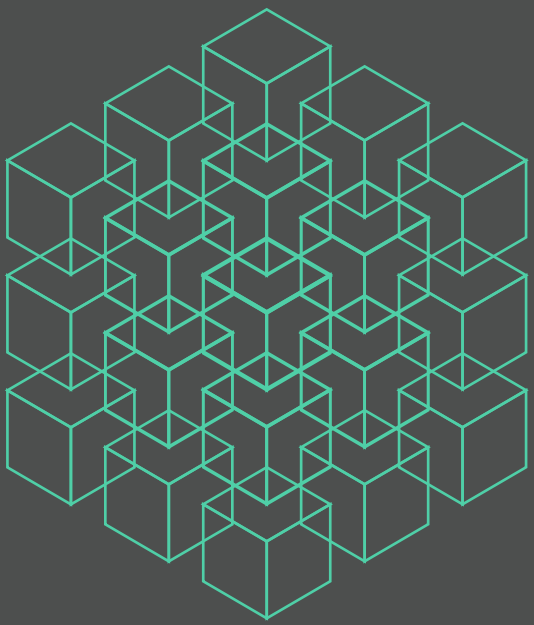
Diplômé du Master in Management de l'ESCP Europe et titulaire d'une maîtrise en mathématiques appliquées à l'économie et à la finance, Clément Téqui, à travers son expérience au sein du cabinet Accuracy, s'est spécialisé dans la modélisation financière complexe et quantitative. Technophile, il s'est intéressé tôt au potentiel de la Blockchain à travers l'angle de la monnaie, l'économie et la finance et intervient régulièrement dans le cadre de conférences. Il est membre fondateur de l'équipe Blockchain d'Accuracy. Clément Téqui enseigne par ailleurs à l'université Paris-Dauphine et à Sciences Po Paris.

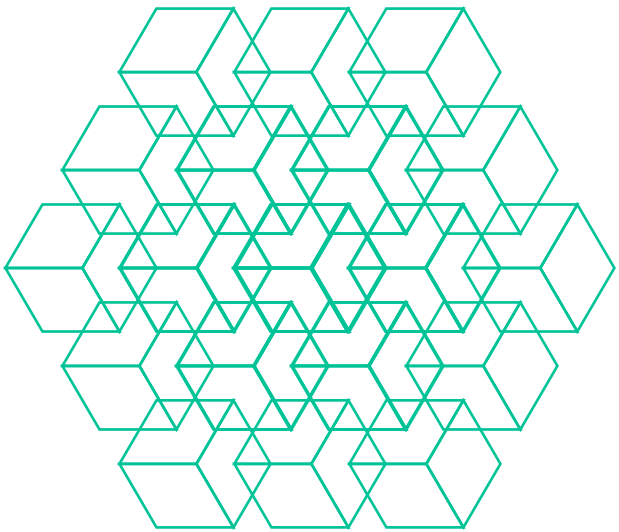
NICOLAS BOUZOU

Essayiste, spécialisé dans l'économie, Nicolas Bouzou a fondé Asterès, une société d'analyse économique et de conseil. Il a publié une dizaine d'ouvrages dont *La comédie (in)humaine* (avec Julia de Funès, éditions de l'Observatoire, 2018), *L'innovation sauvera le monde* (Plon, 2016) et *Le travail est l'avenir de l'homme* (Éditions de l'Observatoire, 2017).

THIBAUT GRESS

Ancien élève de l'École normale supérieure (Lyon), agrégé et docteur en philosophie, Thibaut Gress est l'auteur d'une dizaine d'ouvrages, consacrés à Descartes, à l'idéalisme allemand, à la philosophie de l'art et à l'histoire philosophique de Paris. Fondateur et directeur de la revue *Actu-Philosophia*, il enseigne au lycée et à l'université.





Éditions Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Nouvelle édition augmentée de l'ouvrage *Blockchain – Vers de nouvelles chaînes de valeur* paru en autoédition sur Amazon en 2018.

Maquette et infographies : © Les cyclistes

Mise en pages : Sandrine Escobar

ISBN : 978-2-212-57189-9

MARTIN DELLA CHIESA

FRANÇOIS HIAULT

CLÉMENT TÉQUI

AVEC

NICOLAS BOUZOU ET THIBAUT GRESS

BLOCKCHAIN

VERS DE NOUVELLES CHAÎNES DE VALEUR

Nouvelle édition augmentée

PROSPECTIVES Accuracy

Éditions EYROLLES

REMERCIEMENTS

Nous souhaiterions remercier chaleureusement Nicolas Darbo et Christophe Leclerc, associés chez Accuracy, pour leur soutien tout au long de l'écriture de ce livre, et pour l'ensemble des échanges que nous avons eus et qui ont permis à ce projet de voir le jour.

Merci également à Frédéric Duponchel, managing partner d'Accuracy, pour son soutien sans faille.

Merci à Rachid Oukhai, CEO de Peculium, notre mentor sur la Blockchain.

Merci à Thibaut Schaeffer, de l'association Ethereum francophone Asseth, pour sa relecture et ses conseils sur le plan technique.
Merci à Vincent C., journaliste, pour sa relecture et sa vision.

Merci à Alexandre Simon, Daniel Nassar, Pierre-Antoine Monin, et Pierre-Louis Terry pour leur aide.

Merci à Guillaume Pouyet pour les discussions des débuts.

Merci à l'équipe de communication, Fadia Benamar, Ine Ahonkhai, Davy Dubois et Jean de Belot d'Aria Partners.

Merci à Florence Collin pour son regard pointilleux, à Amaury de Saint Chamas pour sa rigueur et son professionalisme à toute épreuve, et à Clara Midart pour son travail sur les graphiques.

Merci aux Cyclistes, Aline Abou Saad et Jean-Jacques Sébille, pour la qualité de leur travail, et Éric Poupy sans lequel cet ouvrage n'aurait pas eu si fière allure.

SOMMAIRE

C. LA BLOCKCHAIN : UNE RÉPONSE TECHNIQUE À UN PROBLÈME SOCIOÉCONOMIQUE 67

D. BLOCKCHAIN : LA RENCONTRE DE L'ÉCONOMIE ET DE LA TECHNOLOGIE AU SERVICE DU DÉVELOPPEMENT ? 113

E. LA RUÉE VERS L'OR DIGITAL : FORCES STRATÉGIQUES ET JEUX D'ACTEURS 185

PRÉFACE

Le terme Blockchain n'est pas (encore) défini dans le dictionnaire. Mais quelles qu'en soient les définitions ou la portée qu'on lui prête, la Blockchain est perçue comme complexe, abstraite et très technique. La technologie de la transparence souffre d'un paradoxe : dépeinte comme obscure alors qu'elle est censée être claire. La Blockchain reste largement incomprise au-delà des débats d'experts. Elle reste en effet, pour beaucoup parmi le grand public, au mieux assimilée à la bulle spéculative des crypto-monnaies, au pire un outil immoral aux mains des fraudeurs et trafiquants.

Résumons : dans une chaîne de blocs, les transactions pourraient désormais être réalisées et enregistrées de pair-à-pair, sans tiers de confiance, dit-on. Soit, mais qu'est-ce donc que cette chaîne de blocs que l'on décrit comme inviolable ? Les transactions réalisées entre deux individus seraient exécutées par des algorithmes inconnus, programmés sur des ordinateurs à l'autre bout du monde par des personnes dont nous ne connaissons rien. Rien de très rassurant. Pas sûr non plus que l'information selon laquelle la technologie repose sur la capacité à combiner techniques cryptographiques et réseau décentralisé suffise à lever le voile de la complexité ou à dissiper les craintes. Et même si cela fonctionne, en quoi est-ce bien révolutionnaire ; comment une « simple » technique de validation de transactions pourrait-elle être à l'origine d'un grand chambardement mondial, économique, politique, social et financier, annoncé de l'ampleur d'Internet ?

Le futur d'aujourd'hui est le présent de demain, les bizarreries et folies d'une époque posent les bases des évidences de l'avenir. Cet ouvrage est né d'une curiosité et d'un doute, bornés par deux convictions finies : rien n'est évident et rien n'est impossible. La Blockchain nous invite à nous questionner plus qu'elle ne pose question. Pour la comprendre, elle requiert d'interroger l'évidence et de mener un travail de déconstruction de la réalité passée.

La Blockchain n'a donc rien d'évident, mais le monde et le système dans lesquels nous nous inscrivons ne le sont pas davantage. Notre capacité à construire collectivement des mythes et croyances au-delà des réalités objectives constitue, selon Yuval Noah Harari[1], un des fondements de l'histoire de la civilisation. Nous avons ainsi collectivement admis que des montants s'affichant sur l'application mobile de notre banque avaient une certaine valeur ; ou qu'un morceau de papier bleu sur lequel est inscrit le nombre 20 permettait bien en moyenne d'effectuer 7 km en taxi dans Paris, d'acheter 35 cafés au Portugal ou de payer 43 tickets de bus en Slovaquie. Cela permet de relativiser, en partie du moins tant le constat est fort, le fait qu'une écriture numérique d'une unité de

1. Yuval Noah Harari, *Homo Deus, Une brève histoire de l'humanité*, Albin Michel, 2015.

compte nouvelle – le bitcoin (BTC) – s'échange, à l'heure où nous écrivons, 3 235 euros[2]. L'unité de compte bitcoin et la création du protocole du même nom par un illustre inconnu, date de 2008. Mais comment quelque chose créé à partir de rien peut-il valoir quelque chose ?

Cet ouvrage vise à donner les clés de compréhension du Bitcoin (la première Blockchain) et de la « Blockchain », ensemble nébuleux caractérisant à la fois les technologies sous-jacentes et l'écosystème foisonnant de projets et d'initiatives. Il s'agit d'une interrogation de la Blockchain et, par ce biais, du monde, sous l'angle de la valeur. Quelle valeur accorder à la Blockchain ? Simple mode ou révolution ? Le bitcoin vaut-il quelque chose ? Et si oui, combien ? Pour répondre à ces questions, nous combinons les savoirs académiques classiques – histoire, philosophie, économie, finance et techniques – avec le savoir accumulé sur la Blockchain, par le biais de nos lectures, de nos réflexions, de nos échanges avec des dizaines d'acteurs et de nos missions de conseil dans ce domaine.

La Blockchain s'inscrit dans la continuité de l'évolution des techniques, de notre rapport à la valeur monétaire mais elle est aussi en rupture totale avec le passé puisqu'elle induit dans son essence une décentralisation à grande échelle (A). Comprendre la technologie et ses impacts nécessite de s'intéresser à l'épicentre, le Bitcoin, à ses racines philosophiques et à son système de valeurs (B). Le phénomène s'inscrit par ailleurs dans la continuité d'Internet et repose sur une innovation technologique structurelle en apportant une réponse technique à un problème socioéconomique : le besoin de tiers de confiance pour intermédier des relations éloignées (C). L'innovation dépasse largement le simple champ informatique et purement technique ; le Bitcoin et la Blockchain s'appuient sur des concepts économiques classiques pour les transcender, avec en ligne de mire une redistribution des cartes mondiale (D). Ce gisement de valeur et les débats philosophico-politiques engagés, cristallisant les débats d'antan (centralisation/décentralisation notamment) se traduisent par des jeux stratégiques entre anciens et nouveaux acteurs (E et F). Le marché financier naissant des crypto-monnaies (crypto-actifs) et des *Initial Coin Offering* (ICO) bouleverse les champs théoriques et opérationnels de la finance : quels outils de mesure de la création de valeur ? (G). En bref, l'avenir de cette technologie, qui n'est pas exonérée de limites, reste incertain mais promet d'être passionnant.

2. Au 31 décembre 2018 après avoir atteint des sommets à 17 000 euros, fin 2017.

A

LA BLOCKCHAIN, UNE RUPTURE HISTORIQUE DE LA NOTION DE CONFIANCE ?

I.
Une étape supplémentaire majeure dans l'évolution des échanges et des transactions

Définir la technologie Blockchain n'est pas un exercice aisé. Le plus souvent, les tentatives de définition se bornent à ses caractéristiques techniques et technologiques, en tenant pour acquis que les termes employés sont compris par tous. Prenons par exemple la définition qu'en donne Wikipédia :

« Une (ou un) Blockchain, ou chaîne de blocs, est la mise en œuvre d'une technologie de stockage et de transmission d'informations sans organe de contrôle. Techniquement, il s'agit d'une base de données distribuée dont les informations, envoyées par les utilisateurs, sont vérifiées et groupées à intervalles de temps réguliers en blocs, liés et sécurisés grâce à l'utilisation de la cryptographie, et formant ainsi une chaîne. [...]. Une Blockchain est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti[3]. »

La limite de la définition donnée par Wikipédia, ou par d'autres sites ou ouvrages spécialisés, réside dans le fait qu'elle se limite à des caractéristiques techniques dont les termes sont supposés maîtrisés. Or, les termes « technologie de stockage », « base de données distribuée », « cryptographie », « liste d'enregistrements », « nœuds de stockage », « registre distribué » et « système réparti », appartiennent tous à un champ lexical lié à la science informatique au sens large. Maîtriser ce champ lexical demande, *a minima*, un certain bagage technique en la matière. À cela vient s'ajouter une certaine maîtrise de concepts mathématiques liés à la science cryptographique. Cette double barrière à l'entrée, informatique et mathématique, explique pourquoi cette technologie apparaît très largement obscure au plus grand nombre : un langage d'initié exclut toujours ceux ne le maîtrisant pas. Or c'est aux initiés de faire un pas pédagogique vers le plus grand nombre et non au plus grand nombre de se mettre au niveau des initiés.

En effet, le plus grand nombre est capable de définir ce qu'est une voiture, un avion, une fusée spatiale ou une centrale nucléaire sans pour autant employer des termes techniques propres au champ lexical de la physique, de la mécanique et des mathématiques. Rares sont ceux

3. Lien : https://fr.wikipedia.org/wiki/Blockchain.

présentant, par exemple, la voiture comme étant un châssis constitué d'acier avec un moteur à combustion dégageant une certaine quantité d'énergie lui permettant d'avancer, tout en protégeant les passagers par une enveloppe externe. La voiture est d'abord comprise comme un moyen de locomotion pour une à cinq personnes. La compréhension technique des objets technologiques passe souvent après une compréhension conceptuelle et utilitaire de ceux-ci. C'est pourquoi, nous ferons, dans cette première partie de l'ouvrage, le choix de prendre du recul par rapport aux aspects techniques de la technologie Blockchain, aspects techniques qui seront néanmoins largement explicités et problématisés dans la partie C, « La Blockchain : une réponse technologique à un problème socioéconomique », pour nous concentrer sur une approche centrée sur l'objet conceptuel.

La technologie Blockchain propose une infrastructure permettant d'effectuer des transferts d'actifs (**a**) de manière sécurisée (**b**) sans dépendre d'un organe central de contrôle (**c**). La première technologie Blockchain de l'Histoire est apparue en 2008 grâce au protocole Bitcoin dont la description est faite dans le *White Paper* du désormais célèbre – sous son pseudonyme – Satoshi Nakamoto : *Bitcoin: A Peer-to-Peer Electronic Cash System*[4]. L'usage de la première technologie Blockchain, celle liée au protocole Bitcoin, est ainsi de permettre :

a. d'effectuer des transactions d'actifs *via* une monnaie digitale homonyme au protocole : le fameux bitcoin ;

b. de manière sécurisée : en dix ans d'existence, le protocole Bitcoin n'a jamais été défaillant ;

c. sans dépendre d'un organe central de contrôle : aucune banque ne valide les transactions. C'est le réseau décentralisé qui assure le processus de validation et de sécurisation des transactions (cf. la partie C pour de plus amples détails).

L'objet de cette partie est de questionner la Blockchain dans une perspective historique : rupture ou continuité ? L'Histoire a-t-elle connu des évolutions similaires ?

La technologie Blockchain apporte la promesse de révolutionner la façon dont s'effectuent les échanges et les transactions. Une révolution, si l'on s'en tient à la définition du Larousse, désigne un « changement brusque, d'ordre économique, moral, culturel, qui se produit dans une société ». Pourquoi, dès lors, parler de « révolutionner » pour une technologie dont le cas d'usage concerne ces choses si familières que sont les échanges et

4. Lien : https://bitcoin.org/bitcoin.pdf

les transactions ? Pour répondre à cela, il faut comprendre l'ordre économique qui organise les échanges et en quoi la technologie Blockchain est un changement brusque. L'économie du XXIe siècle se caractérise par une verticalité et une centralisation forte des organes dépositaires de la confiance : ces banques sont les tiers de confiance garants du système financier, les assureurs sont les tiers de confiance garants de la gestion collective du risque, l'État est le tiers de confiance garant de la sécurité, du droit et de la monnaie. La technologie Blockchain offre la possibilité d'un changement brusque de ce modèle organisationnel grâce à un déplacement des dépositaires de la confiance. Ce déplacement se fait d'un centre vers des extérieurs atomisés, créant ainsi un système caractérisé par son horizontalité plus que sa verticalité. Ce double mouvement d'atomisation et d'horizontalisation se place à revers du mode d'organisation économique propre à toute notre histoire économique.

Si l'on prend le cas des banques ou des assureurs, la valeur économique créée par ces dépositaires de la confiance repose sur leur capacité à garantir fluidité et sécurité dans les échanges marchands : un système économique dans lequel les échanges et les transactions souffriraient d'un manque constant de confiance serait totalement paralysé. Cette valeur économique a cependant un coût, supporté par l'ensemble des acteurs voulant participer aux échanges marchands, coût qui constitue une partie des revenus des acteurs privés.

Toute la puissance de la technologie Blockchain réside dans sa capacité à fournir fluidité et protection dans les échanges et les transactions en se passant de tiers de confiance à moindre coût. Ces derniers sont dissous par la technologie informatique sous-jacente et répartis dans un réseau d'ordinateurs connectés entre eux. Le seul coût de la confiance est alors celui de l'entretien et de la maintenance du protocole, créant ainsi une économie du bien commun de la confiance qui s'oppose au modèle privé décrit précédemment.

La confiance, qui est le concept structurant de la technologie Blockchain, nécessite par conséquent d'être questionnée au regard de l'histoire économique prise dans un temps long. Or, il est difficile de dissocier le questionnement de la confiance dans les échanges, de la notion de monnaie. En effet, en tant qu'instrument d'échange, la monnaie constitue l'avatar le plus représentatif de la capacité des hommes à créer des mondes intersubjectifs pour mieux coopérer[5]. Dans ce qui suit, nous

5. Harari, *op. cit.,* p. 162 : « Les entités intersubjectives dépendent de la communication entre quantités d'humains plutôt que des croyances et sentiments des individus. Nombre des agents les plus importants de l'histoire sont intersubjectifs. L'argent, par exemple, n'a pas de valeur objective. Un dollar ne se mange pas, ne se boit pas et ne se porte pas. Pourtant tant que des milliards de gens croient en sa valeur, on peut s'en servir pour acheter de la nourriture, des boissons et des vêtements. »

montrerons que l'histoire est segmentée de ruptures dans les médias utilisés pour échanger : des tablettes cunéiformes sumériennes aux changes flottants boursiers, en passant par la pièce d'or grecque. Les évolutions de ces médias d'échanges apparaissent dans des contextes favorables dans les domaines technologiques mais également organisationnels. Elles créent ainsi, au cours de l'histoire longue, un phénomène de boucle de rétroaction positive, où les avancées technologiques et les changements organisationnels d'une époque permettent une évolution des médias et vice-versa.

II.
Les transactions, le cœur du développement des sociétés humaines

La transaction est à l'économie ce que l'atome est à la chimie : la plus petite unité insécable susceptible de se combiner. Dès lors, le système économique mondial, dans toute sa complexité, ne repose *in fine* que sur l'agrégation d'une multitude de transactions entre des acteurs privés, publics, individuels ou collectifs, offrant ou demandant des biens, des services ou des valeurs. Les transactions sont omniprésentes ; leur forme actuelle est le fruit de milliers d'années d'histoire.

Si l'on en croit les historiens, le commerce, dont l'origine semble s'ancrer aussi loin que les premières traces d'*Homo sapiens*, est considéré comme l'origine de la civilisation. L'agriculture en tant que telle n'a pas été inventée : le fait de planter une graine pour en retirer une plante ou un fruit fait partie de l'observable rapidement à la portée de l'homme. Ce que l'on entend par « révolution agricole », est le passage progressif – autour de 8 500 ans avant notre ère – par *Homo sapiens* de son statut de chasseur-cueilleur à celui de fermier. L'Homme passe d'une activité primitive de chasse et de cueillette pour sa seule subsistance à une activité plus collective et organisée, autour de la domestication des espèces animales et végétales. La révolution agricole a apporté beaucoup à l'espèce et a été à l'origine de nombreux changements : la maîtrise de l'eau, le développement des organisations humaines, l'utilisation de la force animale et bien d'autres évolutions qui auront permis d'augmenter la production, les rendements et les volumes de vivres par unités de territoires. L'apparition d'une corrélation négative entre la capacité de production d'un agriculteur et son besoin individuel (ou

celui de son entourage immédiat) induit deux conséquences majeures : l'opportunité d'échanger le surplus non utilisé par les « producteurs » avec d'autres groupes et l'opportunité de diversification et spécialisation des tâches humaines. Celles-ci ne nécessitant plus d'être entièrement dédiées à la chasse et la cueillette pour assurer la survie, elles peuvent s'orienter vers des activités de poterie ou de travail des métaux.

Des traces de centaines de coups de pioche préhistoriques ont par exemple été retrouvées au XIXe siècle dans la région de Mons en Belgique, témoignant d'une activité d'extraction, transformation (taillage) et commerce de silex[6]. Preuve que l'économie est née bien avant que nous ne la définissions dans le Larousse comme l'« ensemble des activités d'une collectivité humaine relative à la production, la distribution et la consommation de richesse ».

III.
La préhistoire : le registre comme facteur d'invention de l'écriture

Les travaux de recherche historiques placent l'« invention » de l'écriture vers 3400 av. J.-C. par les Sumériens dans la région de Suze, période également connue sous le nom de « culture d'Uruk ». Les travaux d'une équipe d'archéologues, sous l'égide de Hans Nissen à l'Université libre de Berlin, ont permis l'accès aux sources et l'analyse d'un corpus de plusieurs milliers de textes sumériens, livrant des enseignements clés dans la compréhension de cette invention par la description de signes et de procédures érudites.

L'invention de l'écriture est indissociable du contexte culturel de l'époque : l'agriculture a permis un essor de la croissance démographique important ce qui a amené les communautés humaines à s'organiser dans les domaines politique, social et idéologique afin de pouvoir gérer et organiser efficacement des corps sociaux toujours plus vastes, constituant ainsi les premières formes d'État. Cette nouvelle forme d'organisation politique a été également rendue possible par l'intensité d'innovation technologique très forte dans cette région du monde à cette époque : apparition de la roue révolutionnant les modes de transport,

6. Pierre Thomas, laboratoire de géologie de Lyon, ENS Lyon.

apparition des premières formes d'artisanat permettant la création de pots en céramique[7].

Or, l'apparition d'un État central contrôlant et administrant une population importante (de l'ordre de 10 000 personnes) nécessite ce que l'on nomme aujourd'hui un appareil d'État. Les besoins de l'appareil d'État étant proportionnels au corps social à administrer, très vite les capacités humaines sont dépassées pour pouvoir garder une vision d'ensemble des stocks et de l'impôt, mais également pour prévoir et distribuer. En bref, pour gouverner. L'écriture va donc apparaître par nécessité, en suivant un processus d'abstraction d'un système de numération utilisé par les Sumériens pour comptabiliser les transactions. Ce système était constitué de petites pièces d'argile servant d'unités de compte, appelées *calculi*. Différentes formes construites dans l'argile faisaient référence à des quantités de valeur afférentes : un cône valait 1, une bille 10, un grand cône 60, un grand cône perforé 600, une sphère 3 600 et une sphère perforée 36 000. Lors d'une transaction, les commerçants enfermaient le nombre de pièces correspondant au montant adéquat dans une bulle d'argile. Le marchand apposait son sceau sur la bulle, attestant par exemple qu'il s'agissait bien d'une transaction de blé et non de métal. Chaque image, signe distinctif sur la bulle, correspondait à l'identité du marchand, à sa signature, son image de marque. Preuve que la notion de confiance en économie était déjà bien présente dans l'Antiquité. Pour connaître la valeur contenue dans une bulle, il fallait la briser puis compter le montant total des *calculi*.

Ces bulles d'argile, tant qu'elles n'étaient pas brisées, pouvaient être échangées en tant qu'elles représentaient une reconnaissance de dette. Le montant adéquat de chaque transaction donnait ainsi la valeur intrinsèque de chaque bulle d'argile, si bien qu'on considère ces instruments comme les premiers médias d'échange acceptés par une communauté humaine élargie.

Ce système ingénieux évolua petit à petit puisque les hommes commencèrent à y dessiner des trous de différentes tailles, directement sur la surface de la bulle. Ces trous représentaient individuellement la valeur du *calculi* correspondant, enfermé dans la bulle. Il n'est plus nécessaire de casser la bulle puisque la valeur de la transaction est maintenant symbolisée à sa surface par un signe, dessiné avec une tige de bois. En quelques dizaines d'années, la bulle évolue naturellement vers une galette plate, ne contenant plus de *calculi,* formant ainsi une tablette. C'est désormais aux scribes d'apposer sur cette tablette une

7. Jean-Daniel Forest : www.clio.fr/BIBLIOTHEQUE/la_culture_duruk_ou_la_mesopotamie_du_ive_millenaire.asp.

série de tiges et signes de différentes tailles et formes, indiquant des informations de plus en plus élaborées (nature, quantité, qualité, origine, destination…) dans un contexte d'accélération et complexification des échanges. Si les premiers documents connus sont des inventaires de biens formalisant l'enregistrement de transactions, l'écriture connaît ensuite une diversification des usages, fondamentale dans l'évolution de l'organisation des sociétés humaines : récits guerriers et religieux, rédaction de lois, transmission de messages et création de fictions littéraires entre autres.

La culture d'Uruk a donné naissance à l'écriture dans un contexte de mode d'organisation nouveau – l'État comme entité supervisant une population humaine importante – et de forte inventivité technologique avec la maîtrise des techniques de l'artisanat lié à l'argile. L'écriture, *via* le registre de compte, a permis d'optimiser les échanges commerciaux au sein de la cité, favorisant ainsi non seulement la croissance et le déploiement de cette civilisation, mais également son rayonnement sur le plan culturel grâce à la transmission écrite des mythes : à cet égard on considère que le premier récit mythologique ayant laissé des traces dans l'histoire est celui narrant les exploits du roi d'Uruk vers 3000 av. J.-C. : Gilgamesh[8].

Le principe d'une tablette servant de support d'enregistrement des transactions constitue un élément clé pour la gestion administrative d'une puissance gouvernementale centralisée : les Égyptiens reprendront ce principe grâce au papyrus pour asseoir leur domination autour du troisième millénaire av. J.-C. Ces tablettes présentent néanmoins la limite de ne pas permettre un commerce libre et immédiat entre les différents acteurs d'un système économique, du fait de la lourdeur administrative liée à l'écriture de l'ensemble des transactions. Quelque 3 000 ans après l'apparition des tablettes d'argile, l'invention des pièces de monnaie en Grèce antique est une autre rupture dans l'histoire des médias d'échange.

8. Luc Ferry, *Parenthèse Culture* : https://www.youtube.com/watch?v=vTlQs95ZDj4

IV.
La Grèce antique : la pièce de monnaie comme affirmation du pouvoir de la cité

Les cités grecques ont introduit de nombreux concepts ayant structuré la pensée occidentale : démocratie reposant sur la liberté et l'égalité des individus formant la citoyenneté, expansion reposant sur un commerce intense entre les cités, enrichissement permettant le financement d'armées terrestres et maritimes importantes, invention d'une mythologie.

« Les Grecs, par ces innovations, instauraient le principe de gouvernement par la loi et celui de liberté individuelle qui lui est indissolublement lié, socle civique sur lequel seront construits les États de droit modernes[9]. »

C'est dans ce contexte d'innovation organisationnelle mais également technologique (maîtrise accrue des techniques de métallurgie) que vont se diffuser les pièces de monnaie métalliques. Ces dernières, en effet, apparaissent vers le VII^e siècle av. J.-C. en Asie Mineure occidentale, dans le royaume de Lydie. Dans ce royaume coulait le fleuve Pactole – d'où l'expression encore utilisée « toucher le pactole » – qui drainait des quantités importantes d'électrum, métal formé d'un alliage d'or et d'argent. Très vite, les pièces de monnaie en électrum connaissent un succès important de part et d'autre de la mer Égée : la plupart des grandes cités grecques (Athènes, Corinthe, Égine…) adoptent ainsi la pièce de monnaie comme moyen d'échange privilégié dès le VI^e siècle av. J.-C.

La diffusion et l'appropriation des pièces de monnaie métalliques dans le monde de la Grèce antique répondent à une nécessité pratique puisqu'elles favorisent le développement du commerce qui est au cœur de l'expression de la puissance des cités grecques. Pour symboliser cette puissance, chaque cité forge ses propres pièces de monnaie avec son symbole affiché dessus. Ainsi, la pièce de monnaie d'Athènes est reconnaissable de tous puisque symbolisée par une chouette et une branche d'olivier[10].

L'usage de ce nouveau média d'échange est associé à une double affirmation de l'expression du pouvoir public, intérieur et extérieur. Pouvoir intérieur, puisqu'il crée une verticalité entre le pouvoir central et les citoyens : le pouvoir de battre monnaie est réglementé et source de

9. Philippe Nemo, *Qu'est-ce que l'Occident ?* PUF, 2005, p. 15.
10. Notons que la pièce grecque d'un euro reprend cette symbolique.

profit (la valeur intrinsèque de la monnaie était inférieure à sa valeur nominale) et définit un pan de la souveraineté d'une cité. La pièce métallique est par ailleurs un moyen efficace pour le pouvoir public de gérer les affaires quotidiennes (paiement des dettes, levée de l'impôt…) Pouvoir extérieur, ensuite, puisqu'elle permet de définir une hiérarchie entre les cités. Athènes impose, en effet, sa monnaie comme valeur étalon auprès des autres cités de la ligue de Délos.

Cette affirmation du pouvoir par la monnaie illustre le « gouvernement par la loi » des cités grecques, pour reprendre l'expression de Philippe Nemo, puisque la création de la monnaie est régie par les lois de la cité. La monnaie illustre aussi le « principe de liberté individuelle » puisque ce nouveau média d'échange permet aux citoyens de commercer facilement et librement entre eux. *In fine*, la pièce de monnaie est d'une certaine manière l'expression de la dialectique entre « le gouvernement par la loi » et « le principe de liberté individuelle » caractérisant la philosophie politique des cités grecques de l'époque antique : le pouvoir public, par le biais de la loi, définit un cadre dans lequel peuvent s'exprimer les libertés individuelles. Appliquée au champ du commerce et de l'économie, cette dialectique fait de la monnaie le cadre fixant les échanges dans la cité tout en favorisant la liberté individuelle de commercer.

L'invention et la diffusion de la pièce de monnaie métallique comme média d'échange pour les transactions commerciales s'effectue donc dans un contexte culturel, économique et technologique particulier. Le succès de la pièce de monnaie métallique ne reste pas confiné à la Grèce antique puisque son usage est arrivé jusqu'à nous, plus de 2 500 ans après son apparition. Encore aujourd'hui, la pièce de monnaie est un des médias d'échange privilégiés pour les transactions de nature commerciale partout dans le monde[11].

La conception de la valeur associée à la pièce de monnaie a quant à elle évolué. La valeur des monnaies était, dans un premier temps, associée à sa valeur intrinsèque : « son pesant d'or ». Au cours du temps, cette valeur intrinsèque a laissé progressivement place à une valeur plus symbolique. Accorder une valeur symbolique à une monnaie demande un niveau d'abstraction plus élevé et nécessite un niveau de confiance plus important dans le système lui garantissant sa valeur. L'apparition des monnaies symboliques est née de l'invention des jeux d'écriture monétaire qui remonte à la fin du Moyen Âge en Europe occidentale et constitue une rupture par rapport aux pièces métalliques. Cette invention est le fait des banques naissantes.

---

11. Même si désormais les pièces de monnaie métalliques ne reposent plus sur des métaux précieux et sont par conséquent dénuées de valeur intrinsèque.

V.
Le Moyen Âge : la monnaie scripturale fait émerger les banques sous leur forme moderne

Les banques modernes[12] naissent au Moyen Âge entre le XII^e^ et le XIV^e^ siècle dans un contexte favorable au commerce international. L'Europe jouit alors d'une relative période de paix, d'un contexte politique stable, d'une vie économique stimulée par les échanges entre l'Occident et l'Orient et d'un climat plus clément.

Les échanges sont facilités par le va-et-vient de populations et de marchandises, dû aux croisades.

Mais certains en profitent plus que d'autres. Les cités-États de l'Italie du Nord (Milan, Florence, Venise), qui présentent l'avantage d'être situées géographiquement au carrefour des marchés occidentaux et orientaux, bénéficient particulièrement de cette période pour se développer et devenir des acteurs économiques, politiques et culturels incontournables. Et l'un des facteurs de ce développement est la constitution d'un réseau bancaire sans commune mesure à l'époque :

« Pour désigner les banquiers au Moyen Âge, on emploie le terme générique de "Lombards" car, très tôt et pendant tout le Bas Moyen Âge, les banquiers italiens sont la clé de voûte du métier. [...] Ces spécialistes s'installent sur les places où se pratiquent des changes internationaux, comme les villes de foire où se pressent les marchands de gros et les revendeurs, ou comme les villes de forte consommation de produits de luxe. Les foires de Champagne (et de Brie) sont leurs sites de prédilection aux XII^e^-XIII^e^ siècles », explique ainsi l'historien des banques Hubert Bonin, dans *La Banque et les Banquiers en France, du Moyen Âge à nos jours*.

Le nombre croissant d'interactions et d'échanges de biens de diverses parties du monde nécessite une sophistication du métier de banquier. Cette sophistication est rendue possible par deux innovations majeures : les lettres de crédit et la comptabilité en partie double.

---

12. Les traces des premières banques remontent à 3000 av. J.-C. en Mésopotamie, dans la région d'Uruk, parallèlement à la naissance de l'écriture. Entre cette époque et le Moyen Âge, les banques sont cantonnées à une activité de mise en dépôt et au crédit de biens physiques (les mécanismes de compensation et de comptabilité double leur sont inconnus).

Les lettres de crédit sont une réponse apportée à une problématique très concrète de l'époque des croisades : les chevaliers partant en croisade ne peuvent transporter avec eux des quantités importantes d'or et de marchandises, pour des raisons aussi bien pratiques que de sécurité. Cependant, les longs voyages qu'impliquent les croisades ont un coût élevé et les chevaliers doivent être en mesure de le financer de bout en bout. C'est pour faire face à cette problématique de *preuve* de richesse, sans en avoir matériellement possession, que naissent les lettres de crédit qui permettent aux chevaliers de déposer leurs biens dans un établissement foncier appelé commanderie, en échange de quoi on leur donne une lettre de crédit attestant de leur fortune. Nous devons ces lettres de crédit à l'ordre des Templiers qui finançait par ce biais les croisades. L'ordre des Templiers constitue à ce titre une des racines historiques des banques modernes. Comme l'évoque David Graeber, « on soutient souvent que les premiers pionniers de la banque moderne ont été les membres de l'ordre militaire des Chevaliers du Temple de Salomon, souvent nommés les Templiers. Cet ordre de moines-soldats a joué un rôle crucial dans le financement des croisades. Par l'intermédiaire des Templiers, un seigneur du Midi de la France pouvait hypothéquer l'un de ses biens immobiliers et recevoir une "lettre de change" payable en liquide auprès du Temple à Jérusalem ».

La comptabilité en partie double est le principe qui consiste à enregistrer sur un livre de compte des écritures portant sur le montant d'une opération financière simultanément au crédit d'un compte et au débit d'un autre. Cette opération présente de nombreux avantages puisqu'elle permet d'enregistrer des opérations différées dans le temps et de connaître à tout instant que la somme des crédits est bien égale à celle des débits. Les principes de ce mode d'enregistrement sont apparus la première fois dans les livres des Massari de Gênes, datés de 1340[13]. Cette méthode révolutionnaire permet de simplifier des situations d'échanges complexes et se propage dans les banques italiennes, leur assurant un avantage concurrentiel important. L'expansion de cette méthode est facilitée, un siècle plus tard, par l'innovation que représente l'imprimerie par Gutenberg entre 1434 et 1444. L'imprimerie favorise la diffusion du savoir à grande échelle et permet donc aux banques d'acquérir plus facilement les techniques comptables modernes de l'époque[14].

La constitution des banques des cités-États italiennes et leur développement constant jusqu'au XV^e^ siècle sont une étape clé dans l'histoire de l'évolution des supports d'échange, puisqu'elle introduit une abstraction accrue de la matérialisation des échanges grâce aux jeux d'écriture de la

13. Jean Fourastié, *La Comptabilité,* « Que sais-je ? », PUF, 1998, 21^e^ éd.
14. Ces techniques sont d'ailleurs affinées grâce aux deux traités célèbres de Luca Pacioli, publiés en 1494 à Venise : *La Summa de Arithmetica, Geometria, Proportioni et Proportionalità*, et *La Divina Proportione*.

comptabilité en partie double. L'introduction des lettres de crédit circulant sur des milliers de kilomètres permet, quant à elle, de matérialiser le fait qu'un simple bout de papier sur lequel est apposée une signature vaut autant que la richesse qu'il décrit.

Ces deux innovations sont les miroirs d'une époque où les échanges se multiplient, où deux mondes, l'Orient et l'Occident, tissent des liens de plus en plus forts, où l'initiative privée est favorisée par le capitalisme florentin et vénitien conquérant, où le besoin de financement pour des expéditions longues et périlleuses est de plus en plus important, où l'imprimerie favorise la diffusion du savoir. De la même manière que les monnaies métalliques avaient été un des moyens à Athènes d'imposer sa domination, la puissance des banques des cités-États italiennes sera le fer de lance de leur domination économique et politique sur le reste du monde entre le XIVe et XVIe siècle. Jacques Attali définit ainsi Gênes comme un cœur dominant de l'ordre marchand grâce à la maîtrise technologique de la comptabilité à partie double[15].

Les banques des cités-États du nord de l'Italie ouvrent également la voie au développement des banques modernes en établissant un glissement dans la confiance accordée aux échanges et au média d'échange. Tant que le système reposait sur des monnaies métalliques, la somme des richesses correspondait peu ou prou au poids des pièces métalliques que l'on possédait. Dans un tel système, la confiance repose essentiellement sur la qualité de la pièce métallique, qualité qui peut être aisément estimée. L'apparition des lettres de crédit et de la comptabilité implique un déplacement de la confiance : désormais la signature d'un établissement bancaire a autant de valeur qu'un montant de pièces métalliques. Ce déplacement de la confiance instaure la notion de tiers de confiance comme rouage essentiel dans les échanges commerciaux : en cas de perte de confiance ou de faillite des établissements bancaires, c'est toute une économie qui se voit dans l'incapacité de se financer.

15. Jacques Attali, *Une brève histoire de l'avenir*, Fayard, 2006.

VI.
L'époque moderne : la monnaie de crédit ou la création monétaire par les banques

Le système bancaire connaît un nouveau tournant décisif au XVIIe siècle avec l'apparition de la création monétaire bancaire, également appelée monnaie de crédit. Paradoxalement, cette invention monétaire n'est pas une initiative des banques mais des orfèvres anglais. Ces derniers ont transformé radicalement leur métier, mais également le système bancaire par la suite, dans un contexte politique et économique trouble pour le pays. En 1625, le roi Charles Ier accède au trône d'une Angleterre divisée sur le plan territorial et religieux. Afin de trouver un moyen de redonner les ambitions financières à son projet politique, il ordonne de saisir les stocks d'or et d'argent des aristocrates de la Tour de Londres en 1640[16]. À cette captation forcée de la richesse du pays s'ajoute une période de fortes instabilités où se succèdent deux guerres civiles, opposant les parlementaires et les royalistes, entre 1642 et 1649. Pour échapper à cette taxation forcée ainsi qu'à cette période d'incertitudes politiques, les personnes détenant les richesses du pays font affluer leurs biens dans les orfèvreries. Dotés de coffres-forts ainsi que d'une réputation de tiers dignes de confiance, les orfèvres accumulent or et argent, en échange de quoi ils fournissent un reçu nominatif qui indique le montant et les objets déposés, d'où le nom de « certificat de dépôt ». Ce reçu permet de convertir, dans n'importe quelle orfèvrerie du réseau, le montant inscrit en équivalent de métal précieux.

Les reçus nominatifs vont peu à peu devenir anonymes et ne plus spécifier les objets déposés pour seulement indiquer le montant. Ces reçus anonymes s'apparentent alors aux premiers billets de banque : ils peuvent être échangés facilement par des acteurs économiques puisqu'anonymes. La confiance placée dans les orfèvreries les rend aptes à échanger des métaux précieux. Les échanges sont grandement facilités par ce procédé. De manière simplifiée, on pourrait considérer que le bilan d'une orfèvrerie à cette époque est le suivant :

Actif	Passif
Dépôt métallique : 100	Certificats émis : 100

16. Roland Marx, « Banque, crédit et monnaie en Angleterre de 1640 à la fin du XVIIe siècle », *Revue de la Société d'études anglo-américaines des XVIIe et XVIIIe siècles*, 1980.

Dans ce système, le passif de l'orfèvrerie décrit le montant de monnaie en circulation. Le certificat émis possède une couverture de 100 % en dépôt à l'actif. Par conséquent, il n'y a pas de création monétaire *via* ce mécanisme mais simplement un transfert de média d'échange : les supports métalliques sont remplacés par des certificats au taux d'un pour un.

Cette pratique, après quelques décennies d'expérimentation, évolue : les orfèvres s'aperçoivent de manière empirique que les montants métalliques déposés à l'actif de leur bilan ne descendent jamais en dessous d'un certain seuil. Cela s'explique par le fait qu'un grand nombre d'opérations de retrait/dépôt engendre des compensations entre les flux entrants et sortants, créant ainsi un stock permanent. De plus, les acteurs économiques accordent une confiance importante à ce réseau d'orfèvrerie si bien qu'en pratique, la demande de conversion de certificats en métaux précieux se fait assez rarement. À partir de ces observations empiriques, les orfèvres commencent à émettre, vers 1655, des certificats non plus en échange de métaux précieux mais en échange de titres de dettes qui viennent s'inscrire à l'actif de leur bilan :

Actif	Passif
Dépôt métallique : 100 Titres de dette : 300	Certificats émis : 400

Dans ce nouveau système, les certificats émis demeurent identiques et ont le même usage qu'avant. Ils peuvent être dépensés et échangés de la même manière. La seule différence réside dans le taux de couverture de ces certificats qui n'est plus que de 25 %, contre 100 % précédemment. Cette différence est majeure puisqu'il y a désormais quatre fois plus de monnaie (sous forme de certificats équivalents à des billets) en circulation pour un même montant de dépôt métallique. Cependant, cette création monétaire n'est pas sans risque d'un point de vue microéconomique. Les titres de dette comportent un risque de défaut de la part de l'emprunteur. Un trop grand nombre de défauts pourrait déséquilibrer le bilan des orfèvreries puisque les titres de dettes n'auraient plus de valeur. Dans ce cas, pour équilibrer le bilan, les orfèvres seraient contraints de détruire des certificats en circulation. Une telle décision pèserait lourdement sur la confiance qu'on leur accorde. Cela met en exergue un second risque : les orfèvres ne sont plus capables de donner le change en dépôt métallique dans le cas où un trop grand nombre

de détenteurs de certificats demandent une conversion de leurs certificats[17].

Par ce jeu d'écriture, la monnaie devient, d'un point de vue macroéconomique, un crédit ou une sorte de créance sur elle-même. La masse monétaire pouvant être mise en circulation est alors décuplée puisque dans ce système, qui est celui sur lequel fonctionnent encore les banques commerciales d'aujourd'hui, c'est l'émission de crédit à des particuliers qui est la source principale de création monétaire. *A contrario*, dans un système reposant uniquement sur les monnaies métalliques, c'est la masse d'or et d'argent en circulation qui détermine la quantité de monnaie maximale.

Le glissement opéré dans le processus de création monétaire par les orfèvreries anglaises[18] du XVII^e siècle est une rupture importante dans l'histoire économique. En acquérant le pouvoir d'émettre des monnaies de crédit, les orfèvres, puis les banques, se placent au cœur de l'économie. Ils deviennent un tiers de confiance indispensable au bon fonctionnement du marché, puisque toute la valeur des certificats de crédit réside dans la confiance que les acteurs économiques accordent à son émetteur. Si ce dernier est surpris en train d'effectuer des opérations frauduleuses, comme émettre plus de certificats de crédit que nécessaire[19], les acteurs économiques perdent toute confiance dans les certificats et leur valeur tend vers zéro. Ce nouveau système monétaire demande aux agents économiques un niveau d'abstraction élevé pour accepter que le certificat qu'ils ont en main vaille autant que le montant métallique qui lui est sous-jacent. Cela dit, le certificat de crédit, puis les billets, sont des médias d'échanges plus pratiques dans la vie économique car ils sont plus faciles à transporter et à échanger et permettent donc de faciliter les interactions dans la vie économique.

La création de la monnaie de crédit est également le reflet d'une époque où le contexte est favorable à l'innovation : les échanges commerciaux s'établissent dans un espace économique de plus en plus mondialisé avec l'intégration progressive du continent américain. Cette mondialisation des échanges, inédite dans l'histoire économique, nécessite un média d'échange adapté et répondant aux problématiques de transportabilité, d'interopérabilité entre les nations, mais également capable de financer les convois transatlantiques comportant un risque intrinsèque élevé pour l'investisseur (naufrage, piraterie…).

Cette nouvelle forme de création monétaire, qui consiste à augmenter la masse monétaire en circulation en fonction des crédits émis, donne

17. Jean-Luc Bailly, *Économie monétaire et financière*, Bréal, 2006, 2^e éd.
18. Notons que des sources indiquent que le même processus a eu lieu à Stockholm à la même époque.
19. C'est-à-dire : faire « tourner la planche à billets », comme il est courant de le dire.

à celui qui la contrôle un pouvoir et une responsabilité importants. La monnaie étant la condition nécessaire pour commercer, celui qui peut l'émettre a le pouvoir de déstabiliser l'économie d'un État dans son ensemble. Cela explique la volonté des États de se réapproprier la création de monnaie *via* la mise en place progressive, entre la fin du XVII^e^ et le début du XX^e^ siècle, de banques centrales, établissements parapublics garants de la stabilité monétaire.

VII.
La banque centrale : de l'étalon-or au change flottant

Le mouvement de création monétaire lancé par les orfèvres anglais au XVII^e^ siècle est suivi de nombreuses initiatives bancaires privées qui s'approprient le processus d'émission de monnaie de crédit, entre le XVIII^e^ et le XIX^e^ siècle, créant ainsi une concurrence entre banques privées dans un mouvement dit de *free banking*[20], dont les exemples les plus marquants sont l'Écosse du XVIII^e^ siècle et les États-Unis du XIX^e^ siècle.

Dans un tel système, le pouvoir lié à la monnaie est atomisé entre les acteurs bancaires privés. Pour contrebalancer ce mouvement d'atomisation, qui fait perdre au pouvoir étatique centralisé une part de son pouvoir économique, des banques centrales se créent dans la plupart des pays occidentaux entre la fin du XVII^e^ et le début du XX^e^ siècle[21]. Selon l'économiste Denise Flouzat, une banque centrale se définit comme : « L'institution qui se situe au centre des systèmes de paiement pour garantir les règlements et contrôler l'expansion de la masse monétaire. C'est l'institution considérée comme apte à préserver la confiance dans la monnaie du pays[22]. »

---

20. Le *free banking* est défini par Larry Sechrest, dans *Free Banking: Theory, History and a Laissez-faire model* (Quorum Books, 1993). « Le terme *free banking* dénote généralement une approche à la monnaie décentralisée et axée sur le marché. Les principaux attributs du *free banking* sont l'absence de toute autorité centrale et l'émission de billets aussi bien que de comptes de dépôts par des banques privées individuelles. »

21. La première banque centrale est créée en 1688 en Suède (*Swerige RiskBank*), puis quelques années plus tard, en 1694, est créée la *Bank of England*. La Banque de France est créée par Napoléon en 1800 et la Réserve fédérale (ou *Federal Reserve* abrégé en *Fed*), en 1913 aux États-Unis.

22. Denise Flouzat, « Le concept de banque centrale », *Bulletin de la Banque de France*, n° 70, octobre 1999. Lien : https://www.banque-france.fr/sites/default/files/medias/documents/bulletin-de-la-banque-de-france_70_1999-10.pdf

Les banques centrales permettent aux États de reprendre le contrôle de la création monétaire puisque ces établissements institutionnels deviennent peu à peu les seuls habilités à émettre des billets qui ont cours légal dans un pays[23]. La mise en place progressive des banques centrales dans les pays occidentaux est allée de pair avec le système monétaire dit d'étalon-or.

L'étalon-or est « un système monétaire dans lequel (1) l'unité monétaire est définie en référence à un poids fixe d'or et (2) chaque monnaie nationale est librement convertible en or. Pour garantir cette convertibilité, la quantité de monnaie émise par la banque centrale est strictement limitée par ses réserves d'or. Les règlements entre pays sont effectués en or. Comme chaque monnaie nationale est fixée en poids d'or, le taux de change entre deux monnaies est fixe, et égal au rapport entre les poids d'or respectifs[24]. »

Ce système est donc une innovation de continuité vis-à-vis des premiers certificats de crédit émis par les orfèvres anglais au XVI^e^ siècle : la valeur du papier émis est garantie par un stock de monnaie métallique. La différence réside dans le fait que le certificat de crédit indiquait en lecture directe le montant d'or correspondant, alors que pour le billet d'une banque centrale le montant est indirect. Une parité or est ainsi fixée par rapport à la devise de référence : par exemple, 1 once d'or équivaut à 1 dollar. Tout montant, ou billet, aura ensuite son équivalent en or, calculé à partir de cette parité. L'étalon-or a été le système monétaire international de référence entre 1870 et les années 1930[25].

Si l'étalon-or *stricto sensu* disparaît en 1930, il n'en demeure pas moins que l'or, à la suite des accords de Bretton Woods de 1944 et du Gold Exchange Standard, sert toujours de référence pour le système monétaire : désormais seul le dollar est convertible en or (35 dollars l'once), le dollar devenant ainsi *as good as gold* comme l'étaient les certificats de crédit. Les autres monnaies internationales se contentent d'être indexées sur le dollar pendant que la valeur du dollar est garantie par les réserves d'or américaines. Le dollar, par le biais du Gold Exchange Standard, est une des composantes de la puissance américaine après la Seconde Guerre mondiale. Tout comme Athènes imposait la drachme à ses alliés de la ligue de Délos comme unité de compte, les États-Unis imposent le dollar comme monnaie de référence à leurs alliés économiques. Avec

---

23. « Cours légal » définit une monnaie qui « doi[t] être acceptée comme moyen de paiement ». Source : Dalloz.
24. Publication de la Banque de France, *Qu'est-ce que l'étalon-or ?,* 2010.
Lien : https://publications.banque-france.fr/sites/default/files/medias/documents/focus-05_2010-11-22_fr.pdf
25. Le krach de 1929 a entraîné une crise économique dont l'ampleur était telle qu'elle a bouleversé tous les équilibres macroéconomiques dont celui de la gestion monétaire.

les accords de Bretton Woods, les États-Unis s'étaient engagés à limiter le montant total de dollars en circulation afin de garantir un niveau de conversion or-dollar. Cet engagement n'est pas tenu, et la masse de dollars ne cesse de croître, à tel point que Nixon met fin au système de Bretton Woods le 15 août 1971[26].

Désormais, le taux de change entre les monnaies est flottant et l'appréciation ou la dépréciation d'une monnaie est calculée selon l'agrégation de la quantité d'offres et de demandes qui est proposée. Un tel système demande aux agents économiques un niveau d'abstraction important pour accepter qu'une monnaie, à travers un billet ou le montant qu'indique le compte en banque de mon application mobile, possède bien la valeur que chacun lui prête alors qu'elle est dépourvue de toute valeur intrinsèque. Ce système repose par conséquent sur un degré de confiance important envers les grandes institutions garantes de la conduite de la politique monétaire : la Réserve fédérale américaine, la Banque centrale européenne, la Banque populaire de Chine. Le PIB cumulé des États-Unis, de la zone Euro et de la Chine s'élève, en 2016, à *ca* 40 000 milliards de dollars soit plus de 50 % du PIB mondial (*ca* 76 000 milliards de dollars[27]). Ainsi, la stabilité monétaire de plus de 50 % du PIB mondial repose sur trois établissements, ce qui montre le niveau important de centralisation du système actuel. Notons que dans ce système, les banques privées jouent le rôle d'intermédiaires financiers qui ont pour rôle de recevoir les dépôts et d'accorder les prêts. Par ce mécanisme, elles émettent de la monnaie de crédit selon un mécanisme similaire à celui des orfèvres, la différence notable étant que désormais aucune valeur métallique n'est déposée au Passif des banques pour garantir les crédits, mais seulement les dépôts des agents économiques. Ainsi, les dépôts des uns sont les crédits des autres, sans plus aucune référence à une valeur métallique.

Le système monétaire actuel répond, à première vue, efficacement à l'économie libérale et mondialisée du XXIe siècle : les échanges commerciaux entre les pays sont de plus en plus importants, la fluidité des échanges nécessite des monnaies liquides dans lesquelles tout agent économique peut placer un degré de confiance élevé, les transactions doivent être assurées dans un temps court et sécurisé. Le système monétaire est également le reflet de la technologie de notre époque et se nourrit de chaque innovation pour améliorer son efficacité : dans la plupart des pays occidentaux, la monnaie est avant tout immatérielle. Les médias d'échange sont désormais moins les billets que les cartes de crédit, les smartphones, les comptes en ligne… La digitalisation des

26. Lien : https://www.youtube.com/watch?v=mAMnyWl2GCY : discours de Richard Nixon sur la fin de la convertibilité-or.
27. Source : Banque mondiale. Lien : https://donnees.banquemondiale.org/indicateur/NY.GDP.MKTP.CD?year_high_desc=true

moyens de paiement va de pair avec la digitalisation de l'économie dans son ensemble. L'enjeu de ce système est de garantir, à moindres frais, des transactions fluides et sécurisées.

L'analyse historique des évolutions des médias d'échange et des systèmes monétaires montre que ces derniers épousent bien souvent les traits d'une époque aussi bien d'un point de vue technologique que politique. Cette histoire est faite de ruptures, mais la tendance de fond semble dessiner une dialectique entre des médias d'échange de plus en plus immatériels, donc fondés uniquement sur leur valeur symbolique, et un système monétaire de plus en plus centralisé. Cette évolution s'explique par le fait que plus un média d'échange a une valeur symbolique, plus il nécessite une confiance élevée dans l'institution qui l'émet.

Considérée sur le long terme, la technologie Blockchain est dans la continuité de l'évolution des systèmes monétaires dans le sens où elle prolonge le phénomène de rupture technologique des médias d'échange. En revanche, c'est une technologie de rupture totale puisqu'elle renverse le lien entre immatérialité accrue du support et centralisation.

VIII.
La Blockchain, une technologie de rupture fondamentale

La technologie Blockchain, en proposant une infrastructure permettant de créer les nouveaux médias d'échange que sont les crypto-monnaies, s'inscrit dans la continuité historique d'une évolution de ces médias se faisant au gré des possibilités techniques d'une époque. Essayons donc de replacer l'invention de la technologie Blockchain dans un cadre plus large d'intensité technologique, propre à notre époque, qui ne pouvait que déboucher sur un changement de média d'échange.

L'économie mondiale est, en effet, entrée à la fin du XX^{e} siècle dans une vague de destruction créatrice schumpétérienne d'une ampleur et d'une vitesse inédites. Cette vague ne concerne pas seulement le numérique mais aussi les technologies dites NBIC (nanotechnologies, biotechnologies, informatique et technologies cognitives – notamment l'intelligence artificielle) auxquelles on peut ajouter la robotique. Aujourd'hui, les applications les plus concrètes et spectaculaires de cette vague

d'innovation concernent en priorité les secteurs de la santé (séquençage du génome, immunothérapies, robotique chirurgicale, implants miniaturisés…) et des transports (véhicules autonomes, fusées partiellement réutilisables…). Mais l'innovation est globale. Elle concerne l'ensemble de l'économie et, par suite, des « superstructures » de la société. C'est même la définition d'une « révolution industrielle », laquelle se caractérise par l'émergence de *general purpose technologies*, que l'on peut traduire par « technologies à large spectre[28] ». Cette vague d'innovation est schumpétérienne pour trois raisons :

- elle a pour origine l'utilisation dans le domaine économique d'inventions scientifiques transformées en innovations. Elle fait le lien entre la recherche fondamentale et l'économie de marché ;

- elle concerne la convergence d'un ensemble de technologies (les technologies NBIC, la robotique, l'imprimante 3D…). On reconnaît le phénomène dit de « grappe technologique » (*cluster* dans la terminologie schumpétérienne) ;

- elle constitue un phénomène de destruction créatrice à l'état chimiquement pur (en France, Luc Ferry emploie l'expression encore plus pertinente d'« innovation destructrice[29] »). De nouvelles technologies, de nouvelles activités, de nouveaux métiers se substituent à un ancien ordre économique, ce qui instille de l'anxiété dans les sociétés, en tout cas dans un premier temps. Les crypto-monnaies n'échappent pas à ce phénomène. Faute d'être comprises, et en dehors des gens qui les utilisent, elles inquiètent, notamment en raison de leur potentiel de destruction créatrice.

Cette vague de destruction créatrice est la première dans l'histoire de l'économie qui soit mondialisée. Elle se caractérise de fait par une double concurrence : concurrence entre les États qui veulent stimuler l'innovation ; concurrence entre les entreprises qui doivent se différencier par l'innovation. Ainsi, la hauteur de la vague de destruction créatrice et sa vitesse de propagation sont inédites à l'échelle de l'histoire de l'humanité. Elle est en outre accélérée par les caractéristiques technologiques en jeu, notamment le *deep learning* (méthode utilisée par les algorithmes pour apprendre par eux-mêmes, grâce à des analyses d'une grande quantité de données) et la loi de Metcalfe (qui stipule que la valeur d'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs).

---

28. Pour une analyse complète de cette mutation et sa mise en perspective historique, se reporter aux ouvrages de Nicolas Bouzou : *On entend l'arbre pousser mais pas la forêt tomber, croire en l'économie de demain*, J.-C. Lattès, 2013, et *L'innovation sauvera le monde, manifeste pour une planète pacifique, prospère et durable*, Plon, 2016.
29. Luc Ferry, *L'Innovation destructrice*, Plon, 2014.

Cette destruction créatrice est globale. Il n'est donc pas étonnant qu'elle affecte le système monétaire et financier dans la mesure où les médias d'échange apparaissent, sur un temps long, comme le miroir grossissant des technologies d'une époque. Au fond, le fait de payer en monnaie (physique ou dématérialisée) est, pour les individus, l'un des actes les plus répétés quotidiennement. Notre relation avec le système financier est constante. Tous les jours, nous utilisons de la monnaie, nous achetons des biens et des services et nous sollicitons des services financiers (virements, placements, demandes de crédits, transferts de liquidités…). Très tôt dans la temporalité de la vague NBIC, le système financier a fait l'objet d'innovations. Paypal a été créé en 1998 (et racheté par eBay en 2002). Depuis les années 2000, les nouvelles solutions de paiement se sont développées de façon là aussi exponentielle, notamment en Chine avec, par exemple, WeChatPay, l'application de paiement du groupe Tencent qui permet de régler en ligne ou en boutique grâce à un QR code. Apple propose un paiement avec empreinte digitale et le service de transaction financière d'Alibaba, Alipay, a lancé chez certains de ses partenaires Smiletopay, un service de paiement par reconnaissance faciale.

Que les produits financiers ou les systèmes de paiement fassent l'objet d'innovations n'est donc pas surprenant. Mais ce qui est nouveau avec la vague NBIC, c'est que la monnaie elle-même semble subir la destruction créatrice, en particulier grâce à la technologie Blockchain. Ce simple fait, que la monnaie soit touchée, montre au passage la force de la vague d'innovation contemporaine.

Il faut ainsi garder à l'esprit qu'il y a, à l'origine des crypto-monnaies, un facteur technologique. C'est bien le doublement régulier de la puissance des microprocesseurs (loi de Moore) qui a permis la Blockchain, technologie support du bitcoin. L'histoire du bitcoin en témoigne. Ainsi, dès les années 1990, le mathématicien américain David Chaum avait voulu concevoir une monnaie dématérialisée. Mais ce qui était concevable intellectuellement ne l'était pas encore en pratique : il a échoué du fait des trop faibles capacités de calcul des ordinateurs et du manque d'intégration entre Internet et le commerce[30]. Les avancées conceptuelles et les technologies qui ont permis le bitcoin se sont développées dans les années 1990, notamment grâce à un jeune ingénieur nommé Wei Dai qui a forgé le concept de b-monnaie. Dans ses articles, Dai avait identifié deux nécessités pour qu'une crypto-monnaie fonctionne : (1) qu'une base de données puisse enregistrer la valeur des unités monétaires détenues par les agents ; (2) que les données sur la circulation monétaire soient disponibles dans l'ensemble du réseau. C'est finalement en

30. Sur l'histoire et l'idéologie du bitcoin, nous recommandons également le livre de Philippe Rodriguez, *La Révolution Blockchain*, Dunod, 2017.

2008 que le mystérieux Satoshi Nakamoto présente le bitcoin et rend public le logiciel Bitcoin-QT qui crée et met en circulation les premières unités de cette crypto-monnaie.

La technologie Blockchain est le fruit de l'histoire intime entre monnaie et technologie. Cette histoire est faite de rupture et de continuité, où une invention en chasse une autre, devenant tour à tour totem puis tabou. La technologie Blockchain, en proposant une infrastructure complètement décentralisée, permettant la création de nouveaux médias d'échange et se passant de tiers de confiance, renverse le processus historique dont les esquisses ont été décrites précédemment. Ce renversement dialectique explique les réactions exacerbées la concernant, que ce soit de la part de ceux qui la méprisent ou de ceux qui l'adulent.

- Le bitcoin est par exemple mal compris, car l'appréhender nécessite d'entrer dans l'intimité des technologies qui le sous-tendent, ce qui exige un investissement intellectuel important. La plupart des macro-économistes connaissent parfaitement le fonctionnement des systèmes monétaires contemporains mais les phénomènes d'émergence de nouvelle monnaie et d'histoire monétaire de long terme sont mal connus.

- Il est par ailleurs adulé car il a été conçu par des personnes très idéologisées. Son protocole a été développé par des ingénieurs et des informaticiens « cypherpunks » (Julien Assange en est l'un des plus célèbres représentants) dont le but est de concevoir les moyens technologiques de protéger la vie privée, de la rendre invisible aux entreprises et aux pouvoirs publics. Le bitcoin n'est donc pas une innovation définalisée au sens du « monde de la technique » de Heidegger. Il existe un projet derrière les crypto-monnaies, qui consiste à échapper à la surveillance des autorités. C'est la raison pour laquelle, philosophiquement, le bitcoin renvoie originellement à l'anarchisme et au libertarianisme.

- Le bitcoin est craint et détesté pour la même raison qu'il est adulé. Simplement pas par les mêmes personnes. Le bitcoin échappe ainsi (pour l'heure) à la gestion et même au contrôle d'une autorité centrale, publique ou pas. Les autorités de régulation centrale l'ont d'abord dédaigné et mal compris. Elles s'en inquiètent désormais et veulent reprendre une forme de contrôle.

La technologie Blockchain est finalement un objet dont la valeur économique est difficile à saisir. Pour ses adeptes, les crypto-monnaies sont considérées comme des totems porteurs d'idéologies politiques et philosophiques fortes. Tout objet totémique a une valeur sans véritable corrélation avec sa valeur intrinsèque et tend en général vers l'infini.

Pour ses détracteurs, la technologie Blockchain est un objet obscur, souvent diabolisé car associé au terrorisme, au *DarkWeb*, à la drogue… Ils considèrent dès lors que sa valeur devrait tendre vers zéro. Si l'on essaye de prendre du recul vis-à-vis de sa valeur idéologique en s'intéressant à sa valeur technologique seule, là encore la confusion est grande : répondre à cette question revient à se demander quelle est la valeur technologique associée à l'invention de l'écriture par les Sumériens ? Impossible de quantifier rigoureusement de tels apports. Pour autant, les crypto-monnaies ont des cotations quotidiennes fixant des valeurs à chacune.

Pour mesurer plus aisément le non-quantifiable, il est nécessaire de questionner philosophiquement cet objet nouveau pour mieux comprendre les concepts qu'il promet de révolutionner : contrats, confiance, monnaie, liberté, surveillance… Quelle valeur peut-on donner à un objet qui bouleverserait notre compréhension de concepts aussi familiers ?

SYNTHÈSE SCHÉMATISÉE D'UNE PERSPECTIVE HISTORIQUE

TABLETTE D'ARGILE → **MONNAIE MÉTALLIQUE** → **MONNAIE FIDUCIAIRE**

IVe millénaire av. J.-C. | *VIIe siècle av. J.-C.* | *XIIe/XIIIe siècles*

Amélioration du commerce mais peu de fongibilité.	On ne peut pas être plus riche qu'il n'existe de pièces d'or.	Émergence de la banque moderne grâce aux lettres de crédit et à la comptabilité en partie double.

Abstraction et centralisation : transfert de la valeur intrinsèque en une valeur immatérielle, devant être garantie par des tiers de confiance eux-mêmes de plus en plus centralisés. → Décentralisation

MONNAIE DE CRÉDIT → **BANQUES CENTRALES / ÉTATISATION** → **FIN CONVERTIBILITÉ OR** → **BLOCKCHAIN**

XVIIe siècle | *XVIIe/XXe siècles* | *1971* | *2009*

La monnaie est adossée à une dette et sa création se fait par jeux d'écritures.	Processus d'étatisation de la monnaie *via* l'émergence des banques centrales.	Stock de monnaie traditionnelle plus adossé à un stock de valeurs tangibles.	Monnaie scripturale. **Échange de valeurs entre deux comptes non bancaires, indépendants du système financier et monétaire actuels.** Enregistrement dans un registre infaillible distribué.

B

QUESTIONNER LE SENS PHILOSOPHIQUE DE LA BLOCKCHAIN : VERS UN *SMART CONTRACT* SOCIAL ?

Penser philosophiquement la Blockchain et les crypto-monnaies impose de comprendre que l'on a affaire à quelque chose de singulier, d'irréductible aux anciens schémas de pensée, c'est-à-dire à quelque chose d'inédit dont les philosophies du passé ne peuvent aucunement rendre compte. Cette singularité se joue dès le nom, déroutant, de « Blockchain ». Fondée comme nous le verrons sur une philosophie anarchiste de la liberté individuelle, la technologie Blockchain se décrit pourtant elle-même comme une chaîne, ce qui peut surprendre dans la mesure où cette dernière évoque dans l'imaginaire l'idée d'emprisonnement, de contrainte, d'assujettissement. Inversement, se libérer de ses chaînes évoque la plupart du temps l'idée de liberté, ainsi qu'en témoigne par exemple la représentation du *Génie* de la Bastille dont l'affranchissement est symbolisé par les chaînes brisées que brandit fièrement sa main gauche. Il faut donc en déduire que la chaîne dont il est question dans la Blockchain doit être pensée dans le cadre de liens volontairement contractés et non dans celui de liens aliénants.

Cette seconde vision de la chaîne, par opposition à celle qui emprisonne, peut se percevoir à son tour de deux façons. La première s'inscrit dans l'idée générale de la communication par laquelle la mise en commun des informations – ce que l'on appelle la communication au sens propre – revient à créer une chaîne où circule un certain nombre de données. On peut à ce titre la figurer par le dieu Hermès, dieu de la communication et des messages chez les Grecs[31].

La seconde est plutôt celle du contrat – qui vient du latin *contrahere* au sens de « resserrer ». Par ce terme, nous entrons de plain-pied dans l'idée de liens que l'on resserre et par lesquels se forme une chaîne. En d'autres termes, « contracter » peut être pensé comme le fait de s'enchaîner volontairement à autrui, générant une obligation librement consentie et non une contrainte imposée arbitrairement de l'extérieur. Mais un tel enchaînement contractuel – dont nous verrons qu'il est décisif dans la Blockchain – suppose de s'interroger sur le type de relation que le contractant entretient à l'égard des autres, et donc de sonder la nature de la confiance qui semble devoir fonder la possibilité même de contracter.

---

31. C'est la raison pour laquelle Michel Serres a intitulé *Hermès* sa vaste analyse de la communication publiée en cinq volumes (éditions de Minuit, 1968-1980).

I.
Réflexions sur la confiance et l'idéal *trustless*

Le premier élément de la technologie Blockchain est celui de la confiance. Mais en quoi celle-ci se trouve-t-elle au centre du système de transactions ? Et ce mot est-il bien choisi pour caractériser le processus à travers lequel s'effectuent les transactions en question ?

I.1 Confiance et fiduciarité

La confiance, du latin *confidentia*, venant lui-même de *confidere* que l'on peut littéralement traduire par « se fier à » ou encore « transmettre un secret à », s'apparente étymologiquement à la confidence. Elle peut être définie par l'idée que l'on peut se fier à quelqu'un ou à quelque chose. Notons d'emblée que, par nature, l'identité du destinataire de la confiance est multiple : il peut aussi bien être un individu humain qu'un système général, une fonction particulière qu'une compétence donnée. Je peux avoir confiance en un ami, en un médecin, en Dieu, en un pouvoir politique, en la valeur d'une monnaie… En somme, la confiance ne se définit aucunement par l'identité de ce en quoi je la place, mais bien plutôt par la croyance que ce en quoi je place ma confiance me paraît fiable.

Cette confiance peut prendre des formes diverses, la première d'entre elles étant peut-être celle du pari sur la moralité d'autrui : conclure une transaction par une poignée de main scellant la confiance de part et d'autre signifie faire confiance à la capacité de chacun des contractants à respecter un engagement. Cela suppose en réalité de parier sur le temps. En faisant confiance à autrui, je crois que le temps qui passe n'altérera pas le respect de sa parole, c'est-à-dire que le temps ne corrompra pas la parole donnée. Cette nature morale des relations humaines a longtemps structuré le crédit et la dette, l'honneur consistant à respecter, malgré le temps qui passe, la parole donnée. De telles pratiques se sont observées dans le monde prémoderne, aussi bien antique que médiéval et ont été analysées à de nombreuses reprises. « Dans ce monde, écrit par exemple l'anthropologue David Graeber, la confiance était tout. La monnaie était pour l'essentiel de la confiance, au sens strictement littéral, puisque la plupart des accords de crédit étaient des transactions

conclues par une poignée de main[32]. » Le crédit a ainsi été indexé pendant des siècles sur l'honneur et la respectabilité, fondement qualitatif de la possibilité des échanges humains.

Mais la confiance, notamment en matière monétaire, ne se limite aucunement à la dimension morale de l'honneur et du respect de la parole donnée ; la dimension fiduciaire de la monnaie réside essentiellement dans la confiance accordée à la puissance politique, à la croyance dans la souveraineté politique[33]. Qu'une monnaie puisse posséder une valeur désindexée de la quantité de métal qu'elle contient et que les citoyens croient à cette valeur revient à dire que ces derniers croient à la parole de l'autorité souveraine :

« La déconnexion de la valeur nominale des pièces par rapport au poids et à la qualité du métal qui en est le support physique rend possible l'acte souverain consistant à modifier ce rapport, tant que la monnaie demeure *dokima*, c'est-à-dire unanimement acceptée par les utilisateurs. On voit que dès l'origine, l'art de la politique monétaire est celui de la confiance[34], » explique ainsi l'économiste Michel Aglietta.

La confiance peut également caractériser le rapport de l'homme à Dieu. En particulier pour les catholiques, elle désigne la foi que l'homme est censé entretenir à l'égard de la bonté de Dieu. L'une des facettes du péché est alors la perte de cette confiance en cette dernière. C'est cette perte de confiance en la bonté et la parole divines que symbolise d'ailleurs la tentation exercée par le serpent envers Ève puis Adam dans la Genèse : « L'homme, tenté par le diable, a laissé mourir dans son cœur la confiance envers son Créateur et, en abusant de sa liberté, a désobéi au commandement de Dieu. C'est en cela qu'a consisté le premier péché de l'homme. Tout péché, par la suite, sera une désobéissance à Dieu et un manque de confiance en sa bonté[35]. »

De manière plus générale encore, il serait possible de considérer que la confiance ne se limite pas à un domaine précis – confiance dans la monnaie, dans le pouvoir… – mais qu'elle est le fondement inaperçu des catégories à travers lesquelles nous nous rapportons au monde. Nous accordons foi à un certain nombre de concepts, dont nous estimons évident qu'ils correspondent à certaines réalités afin de penser le monde selon ces concepts. Ainsi, quelles que soient nos morales personnelles, nous croyons par exemple qu'il y a du bien et du mal dans le monde. C'est-à-dire

---

32. David Graeber, *op. cit.*, p. 399.
33. À cela, peuvent être ajoutées selon les époques les confiances d'ordre social dans la tradition de la monétarisation de l'échange, matériel dans la qualité du métal servant de monnaie et technologique dans la fiabilité du système informatique sous-tendant les algorithmes.
34. Michel Aglietta, *La Monnaie. Entre dettes et souverainetés*, Paris, Odile Jacob, 2016, p. 103-104.
35. *Catéchisme de l'Église catholique,* Paris, Pocket, 1999, § 397, p. 305.

que nous croyons qu'il légitime et rend pertinent de décrire le monde selon les catégories de bien et de mal. Or, on pourrait tout à fait défendre l'idée selon laquelle ce sont là des présupposés fiduciaires dont Nietzsche se propose justement de sonder la validité en vue de les ébranler : « Je suis descendu dans les profondeurs, j'ai foré le fond, nous dit ce dernier, j'ai commencé d'examiner à fond et de miner une ancienne confiance sur laquelle nous autres philosophes avions coutume, depuis quelques millénaires, de construire comme sur le fondement le plus assuré […] : j'ai commencé de saper notre confiance en la morale[36]. » Il ne s'agissait pas pour lui de détruire telle ou telle morale mais de remettre en cause l'idée même de se rapporter au monde selon les catégories du bien et du mal.

I.2 Il n'est de confiance que là où demeure l'incertitude

Il faut maintenant se demander quel point commun structure ces différentes formes de confiance, que celle-ci porte sur la parole donnée dans un cadre moral, sur la fiabilité d'une parole publique, sur l'évidence d'une vision du monde, ou encore sur la fiduciarité d'une monnaie. Repartons de Nietzsche : pourquoi évoque-t-il cette confiance en la morale au moment d'exposer son projet de destruction de celle-ci ? Il semble clair que cela tient à la révélation du caractère précaire, incertain et faillible de cette confiance. Autrement dit, parler de confiance, c'est aussitôt envisager la possibilité de sa rupture. C'est également prendre en compte l'éventualité d'une faillite de ce en quoi avait été placée la confiance. Dire que la morale est objet de confiance, c'est révéler la possibilité que cette approche morale du monde, selon le bien et le mal, ne soit pas pertinente et la remplacer par de meilleurs critères en vue d'évaluer plus subtilement la réalité du monde.

Plus généralement, nous pouvons considérer qu'il n'y a de confiance que là où il y a incertitude et relative précarité de la relation : autrui peut être défaillant, ne pas tenir sa parole, le temps peut corrompre son engagement, l'autorité souveraine peut se révéler plus faible que prévu, l'homme peut rompre sa confiance envers Dieu et devenir pécheur… En d'autres termes, il n'y a de sens à parler de confiance que là où l'incertitude liée à la faillibilité de l'individu ou du système demeure possible et envisageable. Cela revient à dire que l'exigence de garantie et d'assurance est incompatible avec la confiance, celle-ci ne pouvant s'exercer qu'à la condition que l'on ait renoncé à exiger celles-là.

---

36. Friedrich Nietzsche, *Aurore. Pensées sur les préjugés moraux*, Préface, § 2, traduction Éric Blondel, Paris, GF, 2012, p. 30.

I.3 La Blockchain comme système de certification *trustless*

Dans de telles conditions, est-il encore pertinent de considérer que la confiance structure le procès de la Blockchain ? Analysons son processus à l'œuvre, notamment en partant de l'application des bitcoins. À chaque fois qu'un nœud, c'est-à-dire un ordinateur connecté au réseau et doté d'une puissance de calcul, envoie des bitcoins à un autre nœud, la transaction est sécurisée en même temps que certifiée, à l'aide de l'envoi d'une clé cryptographique dont le déchiffrement permet de confirmer en retour ladite transaction. La clé cryptographique est un paramètre permettant de chiffrer et déchiffrer une information, qui est ainsi protégée lors de sa transmission. Or, un tel procès de chiffrement/déchiffrement est répété un nombre indéfini de fois par les différents nœuds du réseau, la transaction recevant ainsi un nombre croissant de confirmations au cours du temps ; cela signifie donc que la technologie Blockchain ne fait pas tant appel à la confiance qu'elle ne permet de certifier la validité de l'échange en la confirmant à chaque fois. Elle est, en théorie du moins, *trustless*.

I.4 Substitution de procédures quantitatives à l'autorité qualitative

Y a-t-il alors encore place pour l'incertitude et la faillibilité de la transaction ? Assurément non : la confirmation substitue à la confiance prise *stricto sensu* le cadre de l'assurance et de la certitude. S'insérer dans la chaîne n'implique pas de tenter le pari inhérent à toute forme de confiance, mais sollicite plutôt le savoir qu'aucune technologie connue ne saurait à l'heure actuelle être plus certifiante que celle-ci. De sorte que le rapport dominant est bien moins celui de la confiance que celui de la garantie par réitération indéfinie de la confirmation de la validité de la transaction. Insistons sur ce point décisif. C'est bien la répétition de la confirmation qui garantit la validité, et non l'aval d'un tiers dont l'autorité suffirait à obtenir celle-ci en une intervention. Ici, la quantité de confirmations se substitue à la qualité du confirmateur, la puissance itérative de chaque mine conférant à la longue une certitude, qu'une entité unique et souveraine ne saurait détenir par sa seule autorité. Le minage (nous y reviendrons par la suite) est le processus permettant d'assurer la validation et la sécurité du réseau.

La technologie Blockchain opère donc deux déplacements d'importance. Le premier consiste à introduire un système de transactions si fiables

et si garanties que la notion même de confiance devient obsolète, le système pouvant être qualifié en théorie de *trustless*. Le second vise à substituer le quantitatif au qualitatif : dans une relation fiduciaire classique, la confiance repose sur la qualité des agents, que cette qualité soit envisagée dans l'ordre moral, politique, financier, technologique ou encore religieux. Je fais par exemple confiance à la qualité morale de l'agent quand je lui fais crédit, je fais confiance à la qualité intellectuelle et financière des banquiers centraux quand j'utilise de la monnaie centrale corporelle, je fais confiance à la puissance divine quand j'accorde crédit à la parole de Dieu… Mais avec la Blockchain, c'est le quantitatif qui s'impose, la réitération indéfinie de l'opération de déchiffrement par les nœuds permettant de certifier la transaction et, du même geste, d'accomplir la substitution de la certitude à la confiance. Ainsi le caractère *trustless* de la Blockchain trouve-t-il son fondement dans la substitution de l'itération confirmative à la confiance envers les qualités déterminées d'un individu ou d'une entité donnée.

II.
Philosophie sous-jacente de la Blockchain : l'inspiration crypto-anarchiste

II.1 Liquidation de l'*auctoritas* en son sens classique

Si c'est la réitération d'une opération de déchiffrement d'une clé cryptographique qui permet de confirmer la validité d'une transaction, alors la qualité du nœud qui opère le déchiffrement n'importe pas. Il en découle que le monde de la Blockchain ressemble à un monde horizontal où seules existent des différences intensives de puissance de calcul – de chiffrement/déchiffrement – et où sont abolies les différences de nature entre les entités, aucune n'étant plus légitime qu'une autre pour garantir la validité d'une transaction.

En d'autres termes, le monde de la Blockchain est un monde d'où se trouve bannie l'autorité au sens classique, laquelle suppose nécessairement des différences qualitatives entre ceux qui détiennent l'autorité et ceux qui s'y trouvent soumis. L'*auctoritas* latine est en effet dérivée de la notion d'*auctor* qui désigne habituellement la possibilité pour une entité ou un individu de disposer du pouvoir d'imposer l'obéissance par sa qualité propre. Structurellement parlant, la Blockchain remplace l'incarnation de l'autorité, et évacue l'idée d'une différenciation qualitative entre les êtres, au moins quant à la souveraineté et à la décision. Chacun est aussi souverain que les autres, l'accumulation seule pouvant engendrer des différences dans la chaîne.

II.2 La philosophie crypto-anarchiste comme telle

Concrètement, cela revient à dire que la Blockchain repose sur une philosophie très identifiable pour laquelle les entités classiquement détentrices de l'autorité n'ont plus aucune légitimité dans le cyberespace, aucune entité ne pouvant se prévaloir d'une qualité telle que lui reviendrait un pouvoir décisionnaire particulier. Cette philosophie est appelée crypto-anarchisme, et utilise les techniques de cryptographie pour échapper dans le cadre du cyberespace au contrôle et à la maîtrise des États. Dotée d'un Manifeste, parodiant par sa première phrase le *Manifeste du Parti communiste* de Marx et Engels, rédigé par l'ingénieur informaticien Timothy C. May, cette philosophie craint, pardessus tout, la puissance de contrôle des États et recherche les conditions d'une préservation de l'intimité à travers des moyens de soustraction au contrôle qu'exerce la puissance publique sur les citoyens. Voulant par des protocoles cryptographiques « modifier en intégralité la nature de la réglementation gouvernementale, la capacité de taxer et de contrôler les interactions économiques, mais aussi la capacité de conserver des informations secrètes[37] », cette pensée élabore les conditions d'un « devenir-invisible » des individus dans le cyberespace afin de contourner l'utilisation étatique de la surveillance informatique.

Classiquement anarchistes par leur refus radical d'une autorité supérieure à celle de l'individu – qu'elle soit politique, religieuse, traditionnelle ou encore sociale –, ces penseurs ne sont pas sans rappeler l'anarcho-individualisme d'un Ernest Armand (1872-1962) pour qui « l'anarchisme est [...] la philosophie de l'anti-autoritarisme[38] » et

37. Lien : groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html
38. Ernest Armand, *Initiation individualiste anarchiste*, La Lenteur - Le Ravin bleu, 2015, *in* Alain Laurent, *L'Autre Individualisme, une anthologie*, Paris, Les Belles Lettres, 2016, p. 357.

élaborent une réponse non politique au problème politique de l'hyper-puissance ou, plus exactement, de l'hypercontrôle étatique que rend aujourd'hui possible la technologie informatique. Ainsi créent-ils un monde sans frontières, délivré à la fois des différences qualitatives du réel, donc des territoires, des lois positives et du droit mais aussi de la surveillance de la puissance publique. Monde où ne se rencontrent pas tant des individus identifiables que des pseudonymes effectuant entre eux des transactions de tout ordre que ne peut maîtriser ni même réguler aucun des États actuels.

Parce qu'il est centralisé et qu'il semble obéir à un certain contrôle bancaire, l'argent fait lui aussi l'objet d'une tentative de soustraction aux circuits traditionnels, contrôlés aussi bien par les banques centrales pour tout ce qui concerne les monnaies centrales corporelles, que par les banques commerciales pour les monnaies scripturales (lesquelles forment d'ailleurs l'essentiel de la masse monétaire). Une telle centralisation repose, du point de vue crypto-anarchiste, sur une différence qualitative indue, celle consistant à prêter une compétence et une légitimité particulières à des banquiers centraux ou à des banquiers commerciaux, leur conférant une certaine autorité sur les flux et les émissions monétaires. Dès lors, lorsque le dénommé Satoshi Nakamoto propose en 2008 un modèle monétaire, c'est pour créer les conditions d'une circulation et d'un flux qui échapperaient au contrôle bancaire, quelle que soit la forme de la banque en question, le système devant donc générer sa propre monnaie à travers le calcul des nœuds capables de miner[39].

II.3 L'anonymat et le chiffrement comme formes anarchistes de la liberté

Dans ces communautés virtuelles, le refus structurel des qualités rejaillit sur la nature même des agents effectuant des transactions : anonymes ou dissimulés derrière des pseudonymes, ils n'apparaissent pas tels qu'ils sont, et ne se présentent pas comme des sujets dotés d'une identité précise mais bien plutôt comme des nœuds anonymes, définis quand ils minent par une certaine puissance de calcul, ou comme des identités fictives associées à de faux noms.

On comprend que le préfixe « crypto », dans crypto-anarchisme, ne désigne en rien quelque chose d'analogue à ce que pourrait être par

39. Miner, comme nous l'expliquerons par la suite, est le processus qui permet de sécuriser les données inscrites dans la Blockchain ainsi que de rémunérer les personnes assurant la sécurité de la Blockchain.

exemple le crypto-communisme : les crypto-anarchistes ne sont pas des anarchistes avançant masqués, mais bien des anarchistes considérant que la liberté et la sauvegarde de la vie privée sont désormais conditionnées à la possibilité de vivre caché. En d'autres termes, le droit à l'anonymat constitue lui-même la condition de l'accomplissement de la liberté, la cryptographie étant alors le moyen de réalisation de cette dernière.

La fonction de *hash*[40] ne vise pas à redécouvrir un contenu précis mais à garantir que le contenu transmis est bien le même, c'est-à-dire que l'identité du contenu n'a pas été altérée ni modifiée au cours de la transaction par un utilisateur malveillant. On comprend le caractère décisif de cette fonction : en codant toute information, c'est-à-dire en transformant tout contenu en un chiffre hexadécimal, composé aussi bien de lettres que de nombres, elle permet à la fois de coder n'importe quel contenu et, en même temps, de le chiffrer car cette fonction n'est pas réversible : il est strictement impossible de retrouver le contenu à partir du code. Ainsi peuvent être transmises toutes les informations possibles et imaginables sous une forme chiffrée qui présente le double mérite d'être associée à l'identité d'un contenu et de ne pas autoriser la découverte de celui-ci à partir du code.

III.
Paradoxes et ambiguïtés de la technologie Blockchain

III.1 Refus de surveillance mais exigence de transparence

Ces premières conclusions nous conduisent à certains paradoxes de cette technologie. Ses concepteurs pensent l'État un peu à la manière dont Jeremy Bentham (1748-1832) pensait la prison idéale, c'est-à-dire comme un panoptique où une tour centrale permettrait aux gardiens de surveiller et contrôler tous les prisonniers sans que ceux-ci puissent

40. Son rôle sera précisé dans la partie C : « La Blockchain : une réponse technique à un problème socioéconomique ».

déterminer s'ils sont ou non observés, et se comportant donc comme s'ils l'étaient en permanence. Dans de célèbres analyses développées dans *Surveiller et punir*, Michel Foucault avait fait de ce panoptique une sorte de modèle du pouvoir moderne (qu'il dénonçait), pouvoir n'étant plus tant assumé par une personne qu'accompli par une fonction anonyme et automatique, diffuse et universelle[41]. De la même manière, le crypto-anarchiste voit le contrôle étatique comme cet organe central de surveillance généralisée à partir duquel seraient épiées toutes les informations informatiquement transmises. Et à ce « panoptisme[42] » étatique en matière informatique ne pourrait répondre efficacement qu'une structure décentralisée, soustraite au contrôle par dissimulation des identités et des informations que rendrait possible la cryptographie.

Toutefois, il serait naïf de ne retenir de la philosophie crypto-anarchiste que l'idée de dissimulation et de cryptage des données. Que la technologie Blockchain permette de se soustraire non seulement au contrôle étatique, mais en plus aux juridictions positives d'un territoire donné, à la censure du Net, à la conservation des données, et peut-être surtout à la taxation, n'implique aucunement l'opacité générale du système. La Blockchain repose en effet sur une base de données distribuée, c'est-à-dire qu'elle se présente comme un réseau composé de plusieurs machines, les fameux nœuds déjà évoqués. Dans ce réseau, chaque transaction est obligatoirement rattachée à un bloc[43], tandis que chacun d'entre eux est rattaché à la Blockchain dont l'intégralité est publique, c'est-à-dire transparente.

Techniquement parlant, cette transparence se manifeste à titre d'exemple par le fait que, pour mettre en place un logiciel de minage sur une machine et ainsi devenir un nœud, il est nécessaire de disposer d'une copie exhaustive de la Blockchain sur celle-ci, ce qui signifie que les transactions sont presque littéralement gravées dans le marbre et donc ouvertes et accessibles à tous, c'est-à-dire transparentes. Mieux encore, parce qu'elle est une sorte de registre, la Blockchain permet d'établir une traçabilité parfaite et complète de toutes formes de biens et de services imaginables, conservant l'intégralité de l'historique des transactions effectuées.

Ainsi, ces fichiers d'un mégaoctet assimilables à des registres que l'on appelle blocs, et dont la fonction est de consigner des séries indéfinies de transactions, monétaires ou autres, n'ont-ils rien d'opaque : le

---

41. « Dispositif important, car il automatise et désindividualise le pouvoir », *in* Michel Foucault, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, coll. « Tel », 1993, p. 235.
42. *Ibid*., p. 228.
43. Un bloc est le nom donné à l'élément permettant de stocker les données inscrites dans la Blockchain. Ces blocs de données sont liés les uns aux autres, ou chaînés, formant ainsi la chaîne de blocs : la Blockchain.

montant des transactions, leur horaire ainsi que l'identifiant des agents sont, dans la chaîne, parfaitement transparents et traçables. La finalité du chiffrement ne consiste donc pas tant, au moins pour les bitcoins, à dissimuler l'existence des transactions qu'à garantir leur authenticité, c'est-à-dire leur non-falsification à partir d'une modification malveillante. Et cette non-falsification s'assimile à son tour à la garantie de l'identité, donc de la permanence, des données.

Ainsi se révèle le paradoxe fondamental qui structure le processus de la Blockchain : fondée sur une philosophie de la dissimulation, selon laquelle seuls la cryptographie et les algorithmes permettent d'échapper à la surveillance, elle rejoint en même temps l'idéologie contemporaine de la transparence et de la traçabilité pour laquelle l'opacité de certaines données entre agents conscients et consentants[44] réintroduit une forme de domination et d'autorité qu'il conviendrait de combattre. C'est donc à une dialectique de l'invisibilité et de la traçabilité que nous convie la Blockchain, à une oscillation complexe entre volonté crypto-anarchiste d'échapper à toute surveillance, et visibilité exhaustive de certaines données, qu'il ne serait pas excessif de rattacher à ce que Byung-Chul Han a récemment appelé « la société de transparence[45] ». Ce philosophe allemand identifie la société transparente à une forme de totalitarisme opposée aux sociétés de la confiance où l'opacité et l'incertitude constituent les garants de la liberté authentique, en tant qu'elles autorisent l'imprévu et le contingent. Une société transparente est celle où l'information est si parfaitement traçable que les comportements deviennent excessivement anticipables, et où la liberté se réduit comme peau de chagrin à mesure que progresse la transparence de l'information.

Toute l'ambiguïté du projet de la Blockchain est ici mise en lumière : fondée sur une philosophie crypto-anarchiste, elle propose une solution effective pour échapper à un type de contrôle et de centralisation, et protège de ce fait contre une forme de surveillance liberticide ; mais dans le même temps, en éradiquant la confiance, en privilégiant le *trustless* par la disparition de l'incertitude et en faisant de la transparence et de la traçabilité de l'information la norme du réseau, elle reproduit en son sein l'un des aspects les plus saillants de l'idéologie contemporaine, « aucun mot d'ordre ne dominant autant le discours public aujourd'hui que celui de la transparence[46] », selon Byung-Chul Han.

L'idée même d'information s'inscrit dans ce cadre idéologique : circulant sous la forme du code, elle est intrinsèquement mobile et transparente et structure ces registres, lesquels finissent par former un système fiable

44. Byung-Chul Han, *La Société de transparence*, Paris, PUF, 2017.
45. *Ibid*.
46. *Ibid*.

et traçable d'information à l'intérieur duquel il est non seulement impossible d'effacer une transaction antérieure mais où, en plus, toute erreur se propageant sur la chaîne est *ipso facto* aussitôt repérable. Ce système informationnel est si transparent qu'il présente une situation idéale pour un audit puisqu'il permet, pour une entreprise par exemple, de retrouver l'environnement des données à un moment donné du passé. Dans ces conditions, c'est l'idée même de secret, impliquée par le crypto-anarchisme, qui devient mystérieuse : se soustraire aux contrôles étatique et bancaire suffit-il à parler de secret ? Être invisible ou non identifiable pour certaines autorités institutionnelles signifie-t-il évoluer dans un cadre secret ?

III.2 L'espace secret ou le retour des différences qualitatives

C'est peut-être ici que doivent être précisées certaines analyses en lien avec le secret. Celui-ci, tiré du latin *secretum*, porte en lui une charge géographique ou topographique : le *secretum* est d'abord le lieu caché, la retraite, la solitude, et signifie ainsi un lieu qui a été séparé des autres. Le secret caractérise donc une étendue, une spatialité soustraite à la connaissance classique ou au regard habituel. À cet égard, le cipherspace[47] comme espace spécifique des crypto-anarchistes, répond à cette définition d'un espace affranchi et séparé de l'espace de la vie régulière.

De là naissent deux paradoxes inattendus. Le premier tient à la nature de ce cipherspace qui, du point de vue même de la logique crypto-anarchiste, se révèle qualitativement supérieur et donc qualitativement préférable au cyberespace[48] classique. Comme l'expliquait subtilement le philosophe Pierre Boutang, le secret est intrinsèquement lié à l'introduction d'une différence de nature entre éléments hétérogènes :

« Est secret ce qui a été mis à l'écart, séparé ; cependant toute séparation ne constitue pas un secret […] ; nous tendons à concevoir la séparation comme disjonction de deux égaux, dans l'homogène ; celle du secret met à part deux inégaux, et instaure plusieurs couples d'inégalités : séparant l'être secret des êtres manifestes, le séparant encore de l'apparence qui le "recouvre", de la non-apparence (selon un type d'apparition

47. Le cipherspace est l'espace du Net formé par les communautés de personnes connues seulement sous un pseudonyme. Par conséquent, aucune géographie et donc aucune loi ne peuvent être appliquées à ces espaces, si ce n'est celles mises en place par la communauté elle-même.
48. Le cyberespace se définit comme l'« ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs ». (Petit Robert)

qu'il faudra définir) qui lui est essentielle mais qui n'est pas son être, le mettant enfin à part des autres secrets[49]. »

Si la séparation se creuse entre deux éléments comparables, de même nature et de qualités identiques, le secret introduit une distinction qualitative, réactivant des différences de nature entre deux ensembles, entre l'espace secret et l'espace profane. Les qualités, qui avaient été exclues par la dimension horizontale de la chaîne au profit d'une validation par réitération purement quantitative, ne sont pas définitivement neutralisées puisqu'elles se trouvent réintroduites au fondement axiologique du système en tant qu'elles permettent de distinguer un espace secret d'un espace contrôlé, le premier se révélant qualitativement supérieur au second.

III.3 Sacraliser la liberté en niant la liberté de choix

Or, dans le cadre de la distinction entre cyberespace classique et cipherspace, une telle séparation ne va pas de soi : en effet, le crypto-anarchisme présuppose une axiologie – une théorie hiérarchisée des valeurs – dans laquelle il serait évident et indiscutable que l'anonymat et la soustraction à un contrôle collectif ou transcendant – État, banques… – soient préférables au contrôle social. Autrement dit, le crypto-anarchisme juge évident que l'autorité dont l'individu dispose sur lui-même doit l'amener à dissimuler son identité auprès des organismes publics et collectifs. De sorte que, non seulement, le cipherspace se veut qualitativement supérieur à un cyberespace où les codes source fermés pourraient transmettre à l'insu de l'utilisateur des données personnelles mais, de surcroît, il s'agit d'un anarchisme surprenant au sens où les individus ne disposent au fond que d'une et une seule solution pour être libres, au sens anarchiste du terme : ils ne sont libres qu'à la condition de se dissimuler en intégrant le cipherspace, de sorte que l'on peut se demander s'il s'agit véritablement d'un choix et, partant, de l'exercice d'une liberté.

Le paradoxe initial, consistant à remarquer que la Blockchain, qui visait à se soustraire aux contrôles étatique et bancaire, se conjuguait à une exacerbation de l'idéologie de la transparence s'accompagne de nombreuses conséquences inattendues : d'une part, la technologie Blockchain se voulant *trustless* substitue la réitération de la confirmation à la confiance envers telle ou telle qualité des agents, la quantité se substituant donc à la qualité. Et en même temps, se révèle le fait que tout raisonnement qualitatif n'a pas disparu de la structure intellectuelle

49. Pierre Boutang, *Ontologie du secret*, Paris, PUF, coll. « Quadrige », 1998, p. 48.

soutenant la technologie Blockchain : l'idée même de secret introduit des espaces hétérogènes, qualitativement différents, axiologiquement différenciés, en ceci qu'il est jugé évident qu'un espace de dissimulation est intrinsèquement préférable à un espace de contrôle, la notion de secret indiquant ce fossé qualitatif entre ces deux formes d'espace ».

Cette axiologie, constitutive du soubassement idéologique de la Blockchain, génère à son tour une difficulté logique : le caractère jugé indiscutable de la dissimulation comme condition d'exercice de la liberté anéantit en même temps le libre choix. En effet, si la supériorité du cipherspace ne se discute pas, alors il devient nécessaire de le rejoindre, la liberté de l'individu étant à cet égard niée au motif que les circonstances technologiques devraient contraindre sa décision et donc nier la pluralité des options disponibles. Or, cela a-t-il un sens de créer un cadre jugé propice à l'exercice de la liberté individuelle à partir d'une origine qui, intrinsèquement, la nie ?

IV. Restriction du domaine de l'espace humain

IV.1 La liberté de l'anonymat contre la liberté de la volonté

La précédente difficulté doit nous amener à comprendre un point majeur du lien entre liberté et cipherspace : dans cet espace secret, la liberté n'est pas positivement définie par l'exercice souverain de la volonté personnelle mais est d'abord appréhendée de manière négative comme le fait de ne pas être contrôlé, de ne pas être observé par une autorité transcendante. Il découle de cela que la liberté s'identifie à l'anonymat, donc à la dilution de l'identité réelle de l'individu et à la dissimulation de ses qualités véritables. Dès lors, l'idée même d'imputation s'effondre : je suis libre du fait même que l'on ne peut pas m'imputer réellement telle ou telle parole, telle ou telle conversation, tel ou tel achat, dont la teneur est de toute façon indécodable si elle est chiffrée.

Cela n'exclut toutefois pas la réactivation de rapports sociaux dans la chaîne. Si l'anonymat est structurellement lié à une perte d'intérêt envers les différences individuelles, donc envers les différences qualitatives, il n'en demeure pas moins qu'un ensemble d'entités anonymes adoptent un certain comportement et que ce comportement génère à son tour des réflexes sociaux. Si, dans la vie « réelle », le SIDE *(Social Identity Model of Deidentification Effects)* a pu objectiver que l'anonymat s'accompagnait toujours d'un désintérêt envers les qualités différenciées des individus, il a également pu relever qu'il générait des marqueurs sociaux par lesquels les entités anonymes se regroupaient. Appliquée au cyberespace en général, et au cipherspace en particulier, cette sociologie du marqueur social se retrouve dans la notion d'e-réputation ou encore de « cyber-réputation » qui réactive un certain nombre d'indices destinés à agréger ou désagréger les relations.

IV.2 L'obsédante présence du passé : l'infalsifiabilité de l'historique

Cette liberté négative qui concerne exclusivement la possibilité pour l'individu réel de se soustraire au contrôle, par l'anonymat autant que par le chiffrement des données, n'implique aucunement que la volonté personnelle soit souveraine dans le cipherspace. Paradoxalement, une contrainte s'y exerce en permanence, à savoir celle du temps : la création de cet espace secret et libre s'accompagne nécessairement d'une assomption du temps comme pilier substantiel de la limitation de la volonté de tous. En effet, parce que la traçabilité et l'audibilité du système caractérisent la technologie Blockchain, alors le passé est comme conservé et cristallisé, avec la garantie qu'il ne sera ni modifié ni oublié, les calculs des *proofs-of-work* rendant, dans les faits, impossible toute falsification de l'historique. En d'autres termes, le passé y est intégralement disponible, et cela constitue à n'en pas douter une contrainte majeure à l'égard des volontés individuelles, en tant que celles-ci ne peuvent ni le modifier, ni le taire, ni même l'oublier.

Certes, du fait même que le cipherspace soit celui de l'anonymat et non de l'expression de l'individu réel ni de ses qualités, il en découle que ce passé n'est pas réellement le passé de l'individu ni ne caractérise sa nature propre ; ce passé se présente plutôt comme l'historique des transactions garanti par l'ensemble du travail du réseau. Mais une telle distinction est de nul effet au regard de la situation réelle : d'une certaine manière, celle-ci est intégralement conçue pour éviter la fraude, donc pour éviter que des volontés individuelles contournent le passé.

La question de la « double dépense » inhérente à la monnaie bitcoin est à cet égard exemplaire : afin d'éviter qu'un agent ne prétende disposer de plus d'argent qu'il n'en a, le processus est conçu de telle sorte qu'en l'absence de banque validant la transaction selon un ordre précis, le réseau prenne le relais et « décide », à la majorité, de la validité – ou non – de la transaction. Ainsi, la finalité s'avère-t-elle être la même que dans un échange monétaire classique, la différence se jouant au niveau de la seule source de légitimation de la transaction : la majorité du réseau se substitue à l'organe bancaire centralisé, la quantité se substituant à la qualité de l'autorité.

Une fois encore, les conséquences doivent être analysées de près. Si, dans les deux systèmes, la finalité est d'éviter que soient effectuées des transactions non provisionnées, la fiabilité de la technologie Blockchain, quoique plus lente, est largement supérieure. Mais l'autorité ne disparaît pas, elle se contente, si l'on peut dire, de changer de nature. Déliée de son rapport aux qualités d'un agent donné, elle se distribue de manière quantitative, le nombre acquérant de sa seule masse l'autorité et la légitimité suffisantes pour autoriser ou non la transaction en jeu. On pourrait y voir, certes, une projection « démocratique » par laquelle la souveraineté du corps social serait corrélée à la décision majoritaire. Mais ce serait là une analogie trompeuse, car ce ne sont pas des décisions qui sont ici en jeu, ce sont des calculs. De ce fait, la Blockchain illustre à merveille le transfert de la légitimité de la décision humaine vers des calculs anonymes dont la coïncidence statistiquement signifiante des résultats suffit à fonder l'autorisation d'une transaction ; celle-ci ne relève plus de la décision humaine, de l'analyse ni de la délibération, mais d'un niveau statistique jugé signifiant d'une série de calculs aux résultats concordants, le monde du cipherspace « se faisant nombre » pour reprendre le titre d'un récent ouvrage du philosophe Olivier Rey[50].

IV.3 Analyse du *Smart Contract*

Le concept de *Smart Contract*[51] illustre à la perfection cette substitution du calcul à la décision humaine. Conçus par Nick Szabo en 1993, ces « contrats intelligents » utilisent la technologie Blockchain de telle sorte que chaque nœud du réseau *peer-to-peer* agisse comme un titre de registre en vue d'exécuter le changement de propriété de manière

50. Olivier Rey, *Quand le monde s'est fait nombre*, Paris, Stock, 2016.
51. À titre d'exemple, Axa propose un contrat d'assurance contre les retards d'avion reposant sur des *Smart Contracts* via Fizzy. Ces contrats permettent à l'assuré d'être remboursé automatiquement. Les données relatives aux heures d'arrivée de l'avion sont alimentées par une source extérieure (le site fligthStat), sans intervention humaine.

automatique, sans faire appel à la délibération humaine, et selon les règles prévues par le contrat.

L'automaticité ici en jeu signifie que le protocole contractuel est conçu de telle manière que certaines données extérieures suffisent à déclencher les codes logiciels de la Blockchain, ces données déclenchant par ailleurs les codes logiciels de manière nécessaire ; ainsi la délibération humaine qui, par nature, ne peut porter sur ce qui est nécessaire, mais uniquement sur « les choses qui sont à notre portée et qui sont exécutables[52] », se trouve-t-elle singulièrement réduite du fait même que s'étend le domaine de la nécessité et que se restreint celui du contingent.

Ici se retrouvent les analyses inaugurales consacrées à la confiance ; le domaine de la Blockchain vise à éliminer le plus possible l'incertitude et l'aléatoire, donc le contingent, de telle sorte que se substituent à la confiance, toujours corrélée à la faillibilité d'un système, les notions d'assurance et de garantie. Celles-ci étant produites par l'itération de calculs dont les résultats sont jugés statistiquement satisfaisants, il en découle que c'est le domaine propre de l'humain qui s'efface progressivement au profit de procédures automatisées fondées non sur la délibération mais bien sur la certification. Cette dernière sera d'autant plus forte qu'elle aura réussi à éliminer l'incertitude que fait toujours régner l'intervention de la délibération humaine.

Certes, les récentes déconvenues de The DAO fonctionnant sur Ethereum ont relancé les spéculations sur la durabilité et la fiabilité de la technologie Blockchain, The DAO ayant été piraté quelques semaines après son lancement, soulevant la question de la réactivation de décisions et de délibérations spécifiquement humaines (et unanimistes) pour remédier à la situation. Mais l'imperfection circonstancielle d'une technologie ne doit pas être l'arbre qui masque la forêt : une défaillance locale ne permet pas d'inférer que cet événement ait signé « la fin de l'idéal *trustless* »[53], comme l'a énoncé la chercheuse au CNRS Primavera de Filippi. Un cas particulier de défaillance et de faillibilité ne saurait autoriser l'élargissement immédiat à une réflexion universelle sur l'avenir et la nature de la technologie en jeu bien qu'il ne doive pas être non plus évacué au seul motif de son extrême particularité.

Ainsi, lorsqu'Aristote remarque que « les hommes, chaque fois qu'ils délibèrent, portent leur attention sur ce qu'ils peuvent exécuter par eux-mêmes[54] », il est pour lui évident que le domaine spécifiquement humain de la délibération existe et qu'il est immédiatement corrélé à celui où les

52. Aristote, *Éthique à Nicomaque*, III, 1112a30-31, traduction Richard Bodeüs, Paris, GF, 2004, p. 145.
53. Cf. l'article étrange de Primavera de Filippi : « La fin de l'idéal *trustless* » ; Lien : https://Blockchainfrance.net/2016/07/20/la-fin-de-lideal-trustless/
54. *Op. cit.*, 1112a34-35, p. 145.

connaissances « peu rigoureuses » (ce sont ses termes) imposent de ne pas accomplir de manière automatique le choix des moyens permettant de parvenir aux fins retenues. Parce que les « connaissances peu rigoureuses » sont remplacées par des informations parfaitement fiables en même temps que suffisantes, la Blockchain est cet espace dans lequel la délibération devient inutile : mais de cette élimination découle une éradication plus vaste, celle du champ humain, le domaine propre de l'exécution humaine se voyant lui-même contesté. Cela n'a pas à être loué ni critiqué, c'est un fait impliqué par la logique interne de la Blockchain, substituant de manière générale l'assurance à la confiance et l'automaticité de l'exécution – dans le cas des *Smart Contracts* – à la complexité imparfaite de la délibération. Il n'est néanmoins pas certain que, du point de vue de la cohérence interne du système, cette restriction du domaine du contingent soit compatible avec la revendication de liberté inhérente à toute philosophie anarchiste.

V.
Mise en perspective intellectuelle de la technologie Blockchain

V.1 La technologie Blockchain actualise-t-elle la théorie anarcho-capitaliste ?

Si l'on rattache brièvement l'ensemble des conclusions précédentes à l'histoire de la philosophie, il est tentant d'établir un lien entre le crypto-anarchisme et les théories anarcho-capitalistes, dont Murray Rothbard est peut-être le plus célèbre des représentants. Aussi bien l'anarcho-capitalisme que le crypto-anarchisme, en tant que pensées anarchistes, visent en effet à présenter l'État comme une structure nuisible et inutile, et à concevoir l'autorité comme ce qui doit être contesté dès lors qu'elle ne désigne pas l'autorité de l'individu sur lui-même. L'anarchiste, disait Armand, « ne saurait être considéré seulement comme un négateur personnel d'autorité, il est aussi un négateur personnel d'exploitation[55] ». Contre ces ennemis communs que sont l'État, l'autorité et l'exploitation,

55. Ernest Armand, *op. cit.*, cité par Alain Laurent, *op. cit.*, p. 360.

se crée *de facto* une alliance objective dont il ne faudrait néanmoins pas surdéterminer la parenté : en effet, par leur refus des territoires mais aussi des législations, les crypto-anarchistes s'écartent de l'anarcho-capitalisme sur un point décisif, à savoir celui du droit conçu selon une certaine positivité, et ce en dépit du refus de l'État. Rothbard présente ainsi son propre programme :

« La théorie positive de la liberté se résume alors à analyser quelles sont les relations objectives qu'il est possible de considérer comme les droits de propriété et, par voie de conséquence, quels sont les actes qui peuvent être jugés comme des violations du droit. Bref, comme toute bonne théorie du droit naturel, elle propose une théorie normative du droit (en l'occurrence, une théorie du droit libertarien[56]). »

En tant que libéraux, les anarcho-capitalistes maintiennent – et Rothbard en est la parfaite illustration – un versant positif à la liberté à travers le droit et la législation ; déduits du droit naturel, ceux-ci visent à garantir la propriété privée et certains droits fondamentaux, bien au-delà de ce que la liberté négative, observée avec la nécessité de se soustraire au contrôle étatique ou bancaire, permettait d'esquisser. Il suffit d'ailleurs de voir les critiques virulentes qu'adresse à la fin de l'ouvrage Rothbard au concept de « liberté négative » développé par Isaïah Berlin[57] pour se convaincre que la place du droit distingue de manière irrémédiable l'anarcho-capitalisme du crypto-anarchisme.

V.2 La technologie Blockchain actualise-t-elle les espoirs de Milton Friedman ?

Peut-être serait-il dès lors plus pertinent de se tourner vers Milton Friedman dont les propos récurrents concernant les banques centrales rejoignent les préoccupations spécifiques du crypto-anarchisme et, plus concrètement, des crypto-monnaies. À de nombreuses reprises, il mit en garde contre l'action des banques centrales, lançant même ce mot d'ordre resté célèbre : « Pour parler à la manière de Clemenceau, la monnaie est une question trop sérieuse pour être confiée à des banquiers centraux[58]. » Friedman avance deux arguments fondamentaux : l'un est axiologique, l'autre purement économique. Par le premier, il est

56. Murray Rothbard, *L'Éthique de la liberté*, traduction François Guillaumat, Paris, Les Belles Lettres, préface, 1991, p. XIV-XV.
57. Voir p. 286-290.
58. Milton Friedman, *Capitalisme et Liberté*, traduction. A. M. Charmo, Paris, À contre-courant, 2010, p. 105.

évident que Friedman préfigure un certain refus axiologique du contrôle de la monnaie par une autorité non élue :

« Tout système est mauvais qui confère à une poignée d'hommes un pouvoir et une liberté d'action tels que leurs erreurs – excusables ou non – peuvent avoir des effets d'une si grande portée. C'est un mauvais système pour ceux qui croient en la liberté, simplement parce qu'il donne un pareil pouvoir à quelques-uns sans aucun contrôle efficace du corps politique – c'est là l'argument majeur contre une banque centrale "indépendante"[59]. »

Friedman se situe ici du point de vue de la liberté et s'inquiète de l'autorité confiée à une poignée d'hommes tout en précisant que son inquiétude est d'abord de nature politique : l'ensemble des citoyens subit les effets de décisions qui échappent au contrôle démocratique des citoyens ou de leurs représentants. On voit donc que l'argument de Friedman, quoique fondé sur la question axiologique de la liberté, ne place pas le curseur au même endroit que les crypto-anarchistes : ceux-ci déplorent l'excessif contrôle des échanges monétaires par des autorités bancaires alors que Friedman déplore essentiellement l'absence de contrôle des citoyens sur l'autorité bancaire ; ainsi, sa position l'amène fort logiquement à plaider pour l'établissement de règles à travers lesquelles les citoyens pourront contrôler la politique monétaire, par la médiation de leurs représentants.

On voit que, par cette différence peu perceptible de prime abord, Friedman se maintient dans une sphère libérale et démocratique pour laquelle la légitimité s'enracine dans la décision collective du corps politique hors de laquelle règne le risque de l'arbitraire. De leur côté, les crypto-anarchistes, bien plus anarchistes que démocrates, perçoivent sans aucun doute ce corps politique comme une entité collective qui pourrait nuire aux intérêts de l'individu. De leur point de vue, le problème des banques centrales n'est pas tant qu'elles ne sont pas contrôlées par le corps politique mais le fait qu'elles contrôlent elles-mêmes – au sens de « surveillent » – la circulation monétaire qui devrait être protégée du sceau du secret.

L'écart entre les crypto-anarchistes et Friedman se creuse avec le second argument qu'il propose :

« Excusables ou non, on ne peut éviter les erreurs dans un système qui, en dispersant la responsabilité, n'en donne pas moins le pouvoir à un

59. *Ibid*., p. 104.

petit nombre d'hommes, et qui fait ainsi dépendre d'accidents de la personnalité d'importantes initiatives[60]. »

Ici se retrouve un argument très classique chez les libéraux, qui combine deux aspects : le premier, implicite dans ce texte, mais très explicite chez Hayek ou d'autres auteurs, vise à remarquer qu'il est strictement impossible de prévoir le résultat d'interactions complexes, et donc profondément absurde de confier à une autorité le soin d'anticiper de tels résultats. En d'autres termes, les interactions humaines, notamment économiques, sont si complexes que, pour en anticiper à moyen ou long terme les effets, il faudrait disposer d'une masse d'informations tellement importantes et subtiles que nulle entité humaine ne saurait les collecter ni même les traiter. Dès lors, c'est l'impossibilité informationnelle inhérente à la complexité des interactions qui rend absurde la croyance dans l'anticipation des décisions vertueuses dans le cadre d'une politique monétaire. Le second argument incrimine la faillibilité des décisions humaines : puisque l'incertitude et le brouillard sont le cadre normal des résultats d'interactions complexes, le risque de prendre une mauvaise décision est extrêmement élevé, puisque les données elles-mêmes ne sont pas fiables. De ce fait, des initiatives d'un petit nombre d'hommes peuvent entraîner des conséquences désastreuses.

C'est pourquoi, lorsque Friedman déclare dans un entretien avec Rus Roberts qu'il a toujours été « en faveur de l'abolition de la Réserve fédérale et de sa substitution par un programme qui augmenterait de façon stable et graduelle la quantité d'argent[61] », il ne préfigure pas tant le crypto-anarchisme qu'il ne reprend à son compte des éléments classiquement libéraux, tant axiologiques en tant qu'ils défendent la liberté contre le risque d'arbitraire, qu'économiques en tant qu'ils visent à assurer la plus grande efficience possible du marché en limitant au maximum les décisions irrationnelles. Techniquement parlant, Friedman juge que si l'impératif est de maintenir les prix, et si ces derniers sont corrélés par l'équation de Fisher à la quantité de monnaie, alors l'optimum monétaire consiste à fixer un taux permettant d'éviter que l'émission de monnaie soit supérieure à la production en vue d'assurer la stabilité des prix.

60. *Ibid*., p. 104-105.
61. Lien : www.econlib.org/library/Columns/y2006/Friedmantranscript.html

V.3 « *Code is Law* » : retour sur les analyses de Lawrence Lessig

Il serait conceptuellement confus, voire erratique, d'identifier le crypto-anarchisme qui sous-tend intellectuellement la technologie Blockchain à une forme d'anarcho-capitalisme ou de libéralisme monétariste, et ce en dépit d'une alliance objective tournée contre l'État. Que l'ennemi soit commun n'implique pas que les principes philosophiques le soient, ni que le sens de la liberté retenu dans le crypto-anarchisme et l'anarcho-capitalisme ou chez Friedman soit le même.

La place du droit, si décisive aussi bien dans l'anarcho-capitalisme que chez les libéraux en général, se trouve marginalisée chez les crypto-anarchistes. Une place qui est d'ailleurs tout à fait assumée dans leur manifeste qui raille les craintes étatiques selon lesquelles le cipherspace risquerait de charrier en toute impunité des marchandises soustraites à tout contrôle juridique – drogues, armes, secrets d'État… – en concluant que de telles préoccupations « étaient valables » tout en considérant que ce genre d'échanges ne pose pas de problème particulier. En effet, dans le monde déjuridisé de la Blockchain, quelle entité dispose d'une autorité suffisante pour décréter licite ou illicite le contenu de la transaction ? Seule importe sa validité formelle, c'est-à-dire l'itération du procès de confirmation par chiffrement-déchiffrement, qui est profondément indifférente au contenu concret de la transaction.

Il n'en demeure pas moins que tout échange complexe nécessite, à défaut d'un droit positif ou d'une législation, une régulation. La Blockchain s'insère à n'en pas douter dans cette nouvelle forme de régulation analysée par Lawrence Lessig, professeur de droit à Harvard. Dans un célèbre article publié en 2000 et intitulé « *Code is Law. On Liberty in Cyberspace*[62] » (« Le code fait office de loi. De la liberté dans le cyberespace »), Lessig avait montré que le fait de se soustraire au contrôle étatique ou public ne suffisait aucunement à garantir les formes positives de la liberté. Selon lui, la supposée liberté négative – ne pas être contrôlé par une autorité supérieure – échoue dans les faits à créer les conditions minimales de l'exercice positif d'une liberté. D'une phrase, il conteste la philosophie crypto-anarchiste et, avec elle, l'ensemble des théories anarchistes :

« Mais nous sommes tellement obsédés par l'idée que la liberté équivaut à une libération du joug gouvernemental que nous ne voyons même plus qu'il y a aussi régulation au sein de ce nouvel espace.

62. Lawrence Lessig, « Code is Law. On Liberty in Cyberspace », *Harvard Magazine*, 2000 – Lien : https://harvardmagazine.com/2000/01/code-is-law-html

Par conséquent, nous ne voyons plus non plus la menace que cette régulation représente pour la liberté. »

En analysant la nature même du « code » conçu comme seul outil régulateur du cyberespace[63], Lessig montrait que, par nature, celui-ci était difficilement régulable, d'abord en raison de sa neutralité à l'égard des données, ensuite par l'anonymat de la plupart des utilisateurs. À cet égard, la Blockchain peut être pensée comme le paroxysme de la logique analysée par Lessig, comme le paroxysme d'un système où le code est la seule régulation possible, où donc la régulation au sens classique perd toute signification. Dans une organisation qui n'a pas d'administrateur central, la responsabilité se dilue, l'anonymat permettant par exemple aux créateurs de logiciels de ne pas être identifiés et de ne pas répondre de leurs actes.

V.4 Inventer de nouvelles manières de questionner la singularité de la technologie Blockchain

Avec la technologie Blockchain, deux éléments se surajoutent au cyberespace classique : le premier tient au fait que les relations contractuelles peuvent elles-mêmes être créées par le code, y compris lorsqu'elles sont de nature contraignante – pensons aux *Smart Contracts*. On voit à cet égard que la Blockchain conduit à dissocier la règle du droit, en transférant au seul code la charge de construire la régularité de l'échange. Le second tient au fait que les transactions effectuées dans le cipherspace ne sont pas sans effet dans le monde social réel. Dès lors se pose le problème de déterminer pour quelle raison les lois positives du monde réel devraient demeurer juridiquement muettes au regard de ce qui se passe dans ces échanges. Une transaction d'armes échappant à tout contrôle et servant à accomplir un acte terroriste dans le monde réel pose de sérieuses difficultés, y compris pour la sécurité de ceux qui revendiquent l'anonymat et la cryptographie. Indépendamment de tout point de vue juridique, et du seul point de vue de l'intérêt des individus, il n'est pas certain qu'il soit rationnel de juger désirable la dissimulation principielle du contenu des transactions et de l'identité des contractants. Partant, de manière générale, nous pouvons faire nôtre l'interrogation de Lessig quant à la signification de la soustraction au regard de l'État :

« Lorsque le gouvernement se met en retrait, cela ne signifie pas que rien ne prend sa place. Cela ne signifie pas non plus que le privé n'a pas

63. « Le code – les *software* et *hardware* qui font du cyberespace ce qu'il est – constitue ce régulateur. »

lui aussi des intérêts ; comme si ces intérêts privés n'avaient pas certains buts à atteindre. Appuyer sur le bouton "anti-gouvernement" ne veut pas dire que l'on va atterrir directement au jardin d'Éden. Une fois les intérêts gouvernementaux mis de côté, ils sont remplacés par d'autres. Mais connaît-on ces derniers ? Et sommes-nous certains qu'ils soient, de quelque façon, meilleurs ? Notre première réaction doit être de douter. »

Mais la question est presque insoluble car les problèmes que fait naître la Blockchain devraient appeler des solutions que la philosophie qui la sous-tend interdit d'adopter. Souhaiter que cette technologie « accompagne le droit », offre une certaine « transparence » au gouvernement, voire s'inscrive dans l'idéologie contemporaine et inclusive de « l'accès pour tous » comme le réclame régulièrement Primavera de Filippi[64], est pour le moins déroutant : en effet, la technologie Blockchain n'est pas neutre et ne se réduit pas à l'usage que l'on en fait. Elle est axiologiquement marquée, axiologiquement inscrite dans le refus du contrôle d'une autorité supérieure, étatique, juridique, publique, bancaire, et c'est cela qui lui confère son sens. Le problème n'est pas tant de déterminer si cette philosophie sous-jacente est bonne ou mauvaise mais de comprendre que la Blockchain perdrait son sens en dehors d'un tel soubassement idéologique.

Dès lors, il nous semble non pertinent de faire comme s'il s'agissait là d'un pur problème d'usage qui pourrait être orienté selon les « décisions » d'un certain nombre d'individus – lesquels ? Au nom de quelle autorité ? Il nous semble en revanche urgent d'inventer de nouvelles manières de questionner ces technologies, urgent de s'arracher aux questions idéologiques anciennes inadaptées aux problèmes actuels : se demander quel usage peut être mené de ces technologies, se demander si tout le monde peut en bénéficier, se demander si cela favorise une société plus juste, ce sont là des manières de questionner trop générales, trop peu spécifiques, applicables à n'importe quel problème et ne cernant pas la singularité de cette technologie. Ce sont des paresses intellectuelles doublées d'un confort idéologique, indéfiniment déclinables pour n'importe quelle question.

Cette technologie nous impose bien davantage de redéfinir la place du monde humain dans le monde contemporain et d'intégrer sa nécessaire transformation pour ne pas dire son inévitable restriction : la technologie Blockchain introduit de l'inéluctable, du nécessaire, de l'automatique là où l'on croyait avoir affaire à la sphère contingente de l'incertitude ouvrant à la délibération humaine autant qu'aux relations

64. Primavera de Filippi, Danièle Bourcier, « Réseaux et gouvernance. Le cas des architectures distribuées sur Internet », *Pensée plurielle*, 2014/2 (n° 36), p. 37-53. DOI : 10.3917/pp.036.0037. Lien : https://www.cairn.info/revue-pensee-plurielle-2014-2-page-37.htm

de confiance. Elle introduit du secret là où l'on croyait le pouvoir de surveillance étatique tout puissant, elle introduit, par le code, de la règle en dehors du droit, et là se jouent autant de marqueurs de la destitution de l'homme quant à la maîtrise de son destin. Cela n'est ni bon ni mauvais, cela est. Et c'est cette nouvelle donne qui doit être pensée à nouveaux frais, en de nouveaux termes, selon de nouveaux concepts.

En introduction, nous avons questionné la raison pour laquelle la technologie Blockchain, fondée sur une philosophie anarchiste de libération, avait pris le risque de s'auto-qualifier de « chaîne », laquelle évoque bien souvent ce qui aliène et emprisonne. Montrant qu'il est des chaînes qui désignent des obligations contractuelles fondées sur la libre décision, nous avions inscrit cette chaîne dans la double entente de la communication et de la contractualité, en négligeant quelque peu le premier terme de la locution, à savoir le bloc. Terme tiré du néerlandais, *block* signifie à l'origine le « tronc », l'axe vertical, le pilier supportant la structure.

Les ambiguïtés de la Blockchain que nous avions relevées se cristallisent peut-être dès la mention du mot retenu : en effet, si la chaîne est horizontale, communicationnelle, sans aspérité, transparente, le bloc, lui, est vertical, fixe, substantiel, permanent. La tension entre la fluidité de la chaîne et l'autorité tranquille de la verticalité du tronc nous paraît constitutive des paradoxes de la Blockchain. Elle ne se libère en effet de la tutelle du contrôle étatique et bancaire et, plus généralement de l'autorité verticale, qu'à la condition de rétablir une forme de pilier inamovible qu'est le bloc. Porteur du passé sous la forme de l'historique, il est l'autorité sereine à laquelle se soumet toute validation ultérieure. Garant de l'identité des transactions, il est soustrait au flux permanent de la chaîne : il fixe pour toujours un certain état des transactions et échappe à l'agitation constante du flux des informations.

Il faut donc se garder de ne penser la Blockchain qu'avec les outils conceptuels postmodernes qui ne retiennent du monde que la différence, le mouvant, le flux, la fluidité, la liquidité, la communication. Cette communication et cette contractualité indéfinies dont la chaîne est porteuse ne sont possibles qu'en vertu de l'identité et de la stabilité que procure le bloc. Le mouvement et la fluidité n'existent que par la garantie qu'offre l'historique du bloc, lequel est d'ailleurs associé à l'identité des résultats que présente le calcul des mineurs. Autrement dit, si l'idéologie contemporaine n'aborde plus le monde qu'en termes de « différence », de « flux » et de « mouvement », la Blockchain nous permet pourtant de comprendre que cette liquidité des transactions repose tout entière sur les concepts d'identité, de stabilité et de mêmeté. Mieux encore, rien ne serait pire que l'altération des données – littéralement le « devenir autre » de ces dernières –, le hashage se présentant explicitement comme le moyen de conserver l'intégrité d'une identité.

Néanmoins, et peut-être est-ce là la révolution fondamentale de la Blockchain, cette identité ou cette stabilité ne sont pas celles de l'individu, de l'homme : ce sont celles de calculs, d'opérations procédurales et de coïncidences statistiques de résultats. L'identité et la stabilité sur lesquelles reposent transactions et contrats semblent donc externalisées au regard du genre humain, et fondées en autre chose que l'individualité spécifiquement humaine : les activités humaines d'échanges exproprient l'homme du fondement de ces mêmes échanges, et y substituent codes et algorithmes, lesquels construisent un nouveau monde où règne l'anonymat.

Les codes et les algorithmes seraient ce qui donne à la Blockchain toute sa singularité en devenant le garant de la confiance, dont le concept même semble se dissoudre par l'ordre calculatoire établi. Cette affirmation n'est pas sans soulever de nombreuses interrogations quant à la technologie elle-même. Après tout, les codes et les algorithmes existent depuis les débuts d'Internet et sont les fondements de son fonctionnement. Dès lors, en quoi la technologie Blockchain, qui semble de prime abord reposer sur les mêmes bases qu'Internet, pourrait-elle être révolutionnaire ? Rapidité d'exécution, automaticité, numérisation du monde étaient déjà les promesses de l'informatisation ; la technologie Blockchain en est-elle une brique supplémentaire ? Si c'est le cas, peut-on parler réellement de révolution technologique ? Si ce n'est pas le cas, en quoi son infrastructure diffère-t-elle de celles que nous connaissons aujourd'hui ? Est-ce un système concurrent ou complémentaire ?

C

LA BLOCKCHAIN : UNE RÉPONSE TECHNIQUE À UN PROBLÈME SOCIOÉCONOMIQUE

Pour bien comprendre la technique rendant possible la Blockchain, il est nécessaire de questionner le fonctionnement de l'Internet actuel. Or, ce travail demande de retracer l'histoire d'Internet tout en s'interrogeant sur la raison pour laquelle cette infrastructure a été créée. Quels étaient les usages initialement imaginés ? Comment ceux-ci ont-ils évolué ? Pourquoi cette infrastructure, cette technologie, ne permettent-elles pas de faire émerger une monnaie décentralisée ? La différence avec la technologie Blockchain est-elle une différence de nature ou de degré ? Pour répondre à toutes ces questions, il est inévitable de se plonger dans le fonctionnement technique de ces deux technologies.

I.
Internet : quelle structure pour quels objectifs, quelles limites ?

Internet : entre centralisation et décentralisation. La technologie promettait une décentralisation majeure, mais n'a finalement pas débouché sur un système plus horizontal qu'il ne l'était auparavant. La Blockchain est-elle, comme certains le prétendent, ce qu'Internet aurait dû être, à savoir l'Internet des valeurs ? Une chose est sûre, la Blockchain permet le transfert sécurisé de valeurs de pair à pair, ce qui n'est pas réalisable avec Internet du fait de la contrainte des doubles dépenses, sur laquelle nous reviendrons plus loin.

Pour comprendre pourquoi, il faut revenir à l'apparition d'Internet, à la seconde moitié du XX^e^ siècle, dont la construction repose sur plusieurs briques technologiques. La première est le réseau ARPANET créé en 1969 par l'agence américaine DARPA *(Defense Advanced Research Projects Agency)*. Ce réseau avait pour but de relier quatre universités américaines. Il reposait sur le système de transfert IMP *(Interface Message Processor),* permettant le stockage et l'échange de données, ainsi que sur un protocole de communication NCP *(Network Control Program)* pour la gestion de la couche dite de transport des informations. Les systèmes IMP étaient reliés les uns aux autres *via* des modems connectés à des réseaux téléphoniques spécifiques.[65]

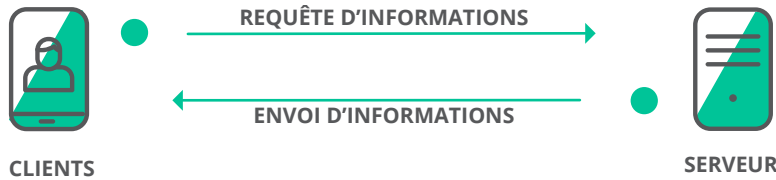
65. Lien : https://www.britannica.com/topic/ARPANET

La deuxième brique technologique est l'invention du protocole de communication TCP/IP par Vinton Cerf et Robert Kahn en 1973. TCP *(Transmission Control Protocol)* permet de contrôler que la transmission des données s'effectue sans erreur tandis que IP *(Internet Protocol)* permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message. Le modèle TCP/IP a été décomposé en quatre modules effectuant les uns après les autres une tâche précise. Ces quatre modules sont la couche application, la couche transport, la couche Internet et la couche accès réseau. Cette décomposition en couches a permis d'harmoniser la suite de protocoles de n'importe quels machines, logiciels ou matériels voulant se connecter entre eux.[66]

La troisième brique technologique est le développement des DNS *(Domain Name System)* par Jon Postel et Paul Mockapetris en 1983[67]. Les DNS permettent la correspondance entre un nom de domaine et une adresse Internet dite IP (pour *Internet Protocol*). Tout objet connecté au réseau Internet possède une adresse IP, un peu à la façon d'un annuaire téléphonique répertoriant chaque objet connecté au réseau.

La quatrième brique technologique est celle qui a rendu possible l'apparition du World Wide Web en 1991 (ci-après le Web) tel que nous le connaissons aujourd'hui : Tim Berners-Lees et Robert Cailliau[68] ont, en effet, mis au point le protocole HTTP *(Hypertext Transfer Protocol)*, le langage HTML ainsi qu'un navigateur et un éditeur de pages Web. Le protocole HTTP est un moyen de communication qui permet l'échange de données sur le Web entre les clients et les serveurs. L'architecture « clients – serveurs » est fondamentale pour comprendre le Web. Les clients sont les utilisateurs du Web. Ils envoient des requêtes à des serveurs qui leur envoient des réponses.

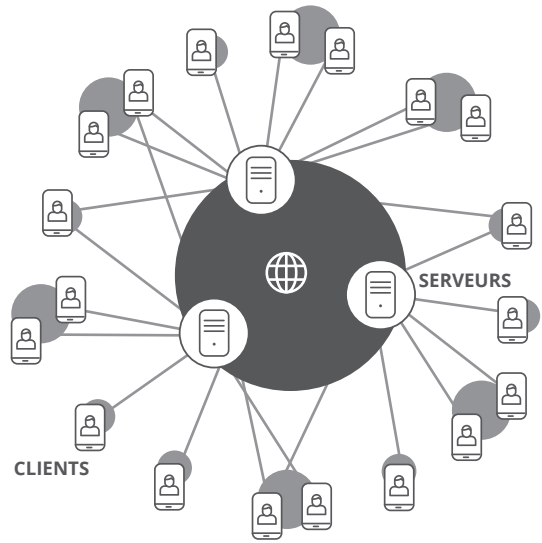
L'ARCHITECTURE « CLIENT-SERVEUR » DU WEB



66. Lien : https://www.britannica.com/biography/Vinton-Cerf
67. Lien : https://www.britannica.com/topic/DNS
68. Lien : histoire-internet.vincaria.net/public/archives/www-announce.txt

Dans l'architecture pensée pour le Web, les serveurs sont des hébergeurs qui centralisent la donnée pour en envoyer une copie aux clients qui souhaitent y avoir accès. Parallèlement à la création du Web, se sont développés des fournisseurs d'accès à Internet qui ont dessiné l'architecture d'Internet et du Web d'aujourd'hui. Les appareils – les clients – se connectent au réseau *via* les fournisseurs d'accès à Internet qui le gèrent grâce à des satellites, des antennes, des fibres… Ce réseau permet aux appareils d'envoyer des requêtes à des serveurs (sur le modèle du protocole HTTP) qui leur renvoient les données. Le réseau Internet pourrait être décrit comme semi-centralisé : centralisé, car les données sont stockées sur des serveurs ; semi, car il existe de nombreux serveurs et relais de l'information.

SCHÉMA DE L'ARCHITECTURE SEMI-CENTRALISÉE DU WEB



Les serveurs du Web fournissant les données sont semi-centralisés. Repartis sur la planète, ils stockent et envoient l'information aux clients.

La cinquième et dernière brique technologique est la création, en 1999, de Napster par Shawn Fanning. Napster est le premier réseau pair-à-pair[69] du Web. Un réseau pair-à-pair se définit comme un réseau d'ordinateurs connectés les uns aux autres, où chaque ordinateur joue à la fois le rôle de client et de serveur, c'est-à-dire que chaque ordinateur stocke une partie des données du réseau et requête les autres ordinateurs du

69. En anglais, *peer-to-peer,* connu aussi sous sa forme abrégée « P2P ».

réseau pour recevoir d'autres données. Les réseaux pair-à-pair sont par essence décentralisés, puisque la donnée est stockée dans chaque ordinateur composant le réseau qui devient alors serveur. L'avantage des réseaux pair-à-pair est leur robustesse, puisque le risque est réparti entre les ordinateurs qui le composent, contrairement à un réseau centralisé par serveur dans lequel le risque est concentré dans les serveurs qui regroupent l'information.

Pour résumer, l'architecture sur laquelle a été bâti Internet repose sur une relation « clients-serveurs », où l'information circule grâce au protocole TCP/IP et par le DNS. Le Web est la dernière brique technologique d'Internet qui a permis de le rendre accessible à tous. Le Web a aussi servi de structure pour le développement de nouveaux usages : réseaux sociaux, applications mobiles… L'usage qui nous intéresse dans ce propos est la digitalisation de la monnaie : nous nous sommes tous habitués à effectuer un nombre toujours plus important d'achats sur Internet, en témoigne le développement des sites de e-commerce. Malgré toutes les évolutions qu'a pu apporter le Web, on peut se demander pourquoi il n'a pas réussi à faire émerger une monnaie digitale et décentralisée, c'est-à-dire se passant de l'autorité d'un tiers de confiance, qu'il soit bancaire ou non (par exemple : Paypal). Ce paradoxe est d'autant plus prégnant que de nombreux outils que nous utilisons quotidiennement avec Internet, comme les e-mails, sont relativement décentralisés.

Pour répondre à cette question, il faut d'abord établir quelles sont les contraintes qu'implique une monnaie digitale et décentralisée.

- La première contrainte est celle de la confiance dans le système. Une monnaie digitale ne peut être acceptée qu'à condition que le système qui assure sa protection soit réputé infaillible. Ce rôle est associé aujourd'hui, comme nous l'avons montré, aux États ainsi qu'aux banques centrales et privées, garants des systèmes monétaires. Dans un système décentralisé, la confiance repose sur le réseau lui-même, d'où la nécessité que celui-ci soit infaillible.

- La deuxième contrainte est celle dite des dépenses doubles, c'est-à-dire s'assurer que l'argent dépensé ne l'a pas déjà été, ou, dit autrement, que le même argent ne puisse pas être utilisé pour deux dépenses distinctes. Dans un système de monnaie fiduciaire, cette problématique n'existe pas puisque l'échange de papier-monnaie implique instantanément un transfert de propriété. Dans un système de monnaie digitale, ce sont les banques qui assurent ce travail de vérification. Dans un réseau décentralisé, le réseau doit assurer ce rôle.

- La troisième condition est celle de la confidentialité des données et des utilisateurs. Les banques, *via* le secret bancaire, assurent usuellement cette confidentialité. Dans un réseau décentralisé, c'est au système de garantir cette confidentialité.

L'architecture du Web et des réseaux pair-à-pair, tels que nous les avons décrits précédemment, ne peut pas garantir le dépassement de ces contraintes, et en particulier celle des doubles dépenses. En effet, sur les réseaux pair-à-pair développés jusqu'à présent, l'objectif est un partage de l'information, envoyée sous forme de copie aux autres membres du réseau. Concrètement, sur un réseau pair-à-pair comme a pu l'être Napster, lorsqu'un utilisateur requête l'envoi d'un fichier musical à un des nœuds du réseau, celui-ci lui envoie une copie. À la fin de la transaction, l'utilisateur ayant requêté la musique et celui qui la lui a envoyée posséderont tous deux une copie. À travers cet exemple, nous nous apercevons que la contrainte liée à celle des dépenses doubles ne peut pas être dépassée par un réseau pair-à-pair tel qu'il a été pensé la première fois par la société Napster : lors d'un transfert d'argent, celui qui le possédait au début de la transaction ne devrait plus l'avoir à la fin du transfert.

C'est cette impasse qui a mené Satoshi Nakamoto à créer la technologie Blockchain, permettant la création du Bitcoin en 2008[70].

II.
La technologie Blockchain et le protocole Bitcoin : une réponse aux limites d'Internet

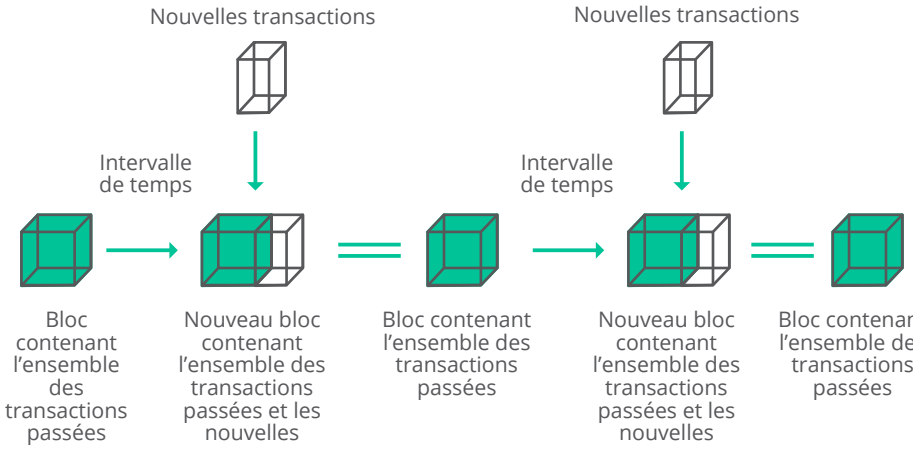
Dans cette partie, nous traiterons exclusivement de la technologie Blockchain restreinte au protocole Bitcoin, première Blockchain et épicentre du séisme observé aujourd'hui. Le protocole Bitcoin est une technique efficace et élégante pour répondre aux contraintes que pose la création d'un système monétaire digital et décentralisé.

---

70. Pour plus de précisions sur les liens entre la Blockchain et l'architecture Internet, nous recommandons la lecture de *The Business Blockchain*, de William Mougayar (éd. Wiley, 2016).

En simplifiant, la technologie Blockchain pourrait être définie de la sorte : grand livre de comptes distribués enregistrant à intervalles de temps réguliers l'ensemble des transactions du système. Ce registre distribué *(Distributed Ledger)*, s'appuie sur une chaîne de blocs d'informations venant s'imbriquer les uns dans les autres. Chaque nouvelle transaction est enregistrée dans un nouveau bloc d'information qui vient s'agréger aux blocs précédents afin de mettre à jour le registre de transactions. Schématiquement, le mécanisme fonctionne de la sorte :

MÉCANISME D'IMBRICATION DES BLOCS



Cette définition succincte de la technologie Blockchain doit être mise en perspective avec celle donnée dans le *whitepaper* du Bitcoin. Dès l'introduction, Satoshi Nakamoto la définit dans ces termes :

« Le réseau horodate les transactions en les hashant en une chaîne continue de preuves-de-travail, formant un enregistrement de données qui ne peut pas être changé sans avoir à refaire la preuve-de-travail[71]. »

Cette définition élargit celle que nous avons donnée précédemment puisque la plupart des concepts clés y sont introduits :

- Les registres distribués (*record* dans le texte) comme nous l'expliquions précédemment ;
- La fonction dite de *hash* qui permet une optimisation du processus de chaînage ;

71. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009.

- La preuve de travail (*proof-of-work*) qui permet de valider chaque bloc et de rémunérer les contributeurs du réseau (Théorie des jeux)[72].

À ces trois concepts, il faudrait ajouter celui de cryptographie asymétrique qui permet l'authentification et la signature des transactions dont émetteur et destinataire peuvent ne pas avoir de registre d'identité central. Dans ce qui suit, nous verrons comment la combinaison de ces quatre concepts permet de répondre aux trois contraintes que nous avions identifiées, pour voir émerger une monnaie digitale et décentralisée.

II.1 Le registre distribué comme réponse à la contrainte de confiance

La première contrainte identifiée pour la création d'une monnaie digitale et décentralisée est la création d'un système sur lequel repose la monnaie jugée infaillible. Comme nous nous situons dans un univers digital, par infaillible il faut comprendre « inattaquable » et infalsifiable par des pirates informatiques. Comment, en effet, placer une confiance dans un système monétaire qui pourrait être sous la menace d'attaque informatique ?

Pour répondre à cette problématique, la technologie Blockchain propose une articulation ingénieuse de deux concepts : la fonction *hash* et le registre distribué pair-à-pair.

II.1.a La fonction *hash*

La fonction *hash*, que nous noterons H dans la suite, permet de compresser l'ensemble des informations contenues dans les anciens blocs afin d'optimiser le processus de chaînage, composante assurant la sécurité du réseau. Une fonction *hash* est, en effet, une fonction de cryptographie qui transforme des données d'*input* en un unique *output* (appelé le *hash* dans la suite). Quelle que soit la longueur des données d'*input*, l'*output* d'une fonction *hash* aura toujours la même longueur, à savoir une suite de 32 – ou 64[73] – caractères numériques et/ou alphabétiques. Ainsi, que l'on mette en *input* d'une fonction *hash* le dictionnaire de langue française ou simplement un prénom, l'*output* sera toujours constitué d'une chaîne de 32 – ou 64 – caractères numériques et/ou alphabétiques. Une

72. L'explication technique du protocole Bitcoin est fondée sur l'ouvrage d'Andreas Antonopoulos, *Mastering Bitcoin,* O'Reilly, 2017, 2e éd.
73. Le nombre de caractères de l'*output* dépend de la fonction de *hash* choisie.

des grandes forces des fonctions *hash* est qu'elle n'est pas réversible : c'est une fonction à sens unique. Soit *x* un *input* de la fonction H, nous avons alors rapidement H(x)= y, où *y* est une chaîne de 32 caractères. Au contraire, étant donné l'*ouput y*, il est très difficile, voire impossible, au vu des puissances de calcul disponibles aujourd'hui, de pouvoir retrouver l'*input* l'ayant généré. La seule solution consiste à essayer l'ensemble des *inputs* possibles afin de trouver le bon.

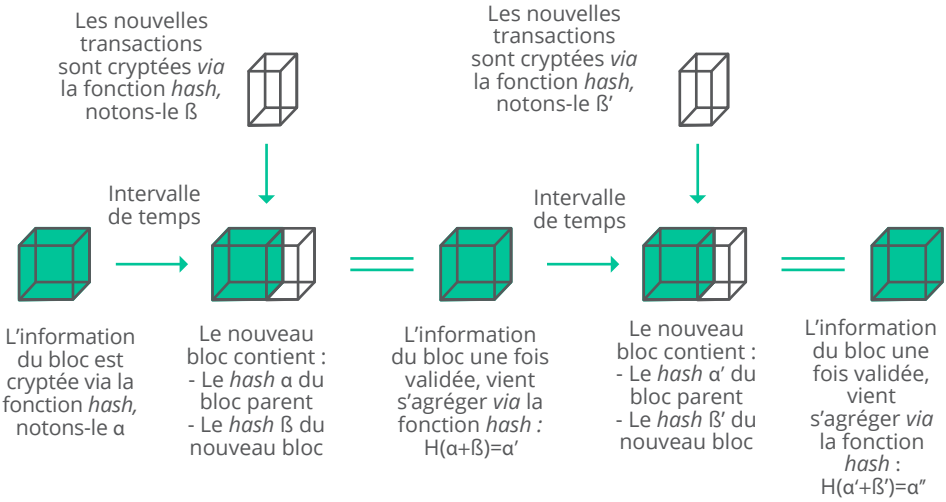
EXEMPLE DE FONCTION *HASH* SIMULÉE SUR LE LOGICIEL PYTHON (L'*OUTPUT* EST DE 64 CARACTÈRES) :

```
import hashlib

print (hashlib.sha256 ("What is the hash of Accuracy".encode
  ("utf-8")).hexdigest ())
Results :
 4e33928aaec190b0aa175e13ff44af53906c75c2357c8eeb92244c687c21999b
```

Chaque bloc constituant la Blockchain est ainsi identifié par un *hash* généré par l'algorithme cryptographique de la fonction *hash* (pour le protocole Bitcoin, l'algorithme SHA256 est utilisé en particulier). Chaque bloc contient une référence au bloc précédent, considéré comme le bloc-parent. La Blockchain est donc constituée d'une chaîne de *hash* reliant chacun des blocs à ses parents jusqu'au premier bloc *(genesis block)*.

MÉCANISME D'IMBRICATION DES BLOCS AVEC *HASHAGE*



Ce mécanisme d'imbrication de fonctions *hash* permet de protéger les informations contenues dans la Blockchain. Imaginons, par exemple,

qu'un utilisateur malveillant souhaite modifier une information sur un bloc afin de changer le montant de bitcoins qu'il possède. Ce changement d'information va engendrer un *hash* différent dans le bloc modifié et, par voie de conséquence, modifier tous les *hash* de la chaîne de blocs.

Comme une copie de la Blockchain est détenue par chaque nœud du réseau (voir les parties sur le réseau pair-à-pair et la preuve de travail), cette modification sera en effet identifiée et rejetée par les autres nœuds du réseau. Le registre partagé par l'ensemble des utilisateurs doit contenir toujours la même information. Ainsi toute version différente de la chaîne de blocs est rejetée par le réseau. Cette opération d'imbrication de l'information par bloc, ou chaînage, est l'élément qui permet de sécuriser l'information contenue dans la Blockchain.

Dans l'exemple précédent, changer α en δ (avec, évidemment, $\alpha \neq \delta$) entraîne une modification de toute l'information contenue dans la chaîne de blocs ainsi que l'*output* final puisque nous obtenons, dans le dernier bloc, $\alpha'' \neq \delta''$.

Le fonctionnement de la Blockchain est souvent assimilé aux couches géologiques de la Terre où s'accumulent des strates de roches. Chaque couche correspond à un ensemble sédimentaire plus ou moins homogène. Les couches les plus anciennes sont celles les plus enfouies dans la terre tandis que les couches les plus récentes sont celles les plus proches de la surface. Une fois qu'une strate géologique se constitue et se fixe dans le temps, elle devient immuable. L'observation géologique de ces couches permet ensuite de reconstituer l'histoire de la Terre. La Blockchain fonctionne de la même manière : un empilement de strates de transactions les rendant immuables. La puissance cryptographique de la fonction *hash* permet à ce mécanisme, lourd en espace de stockage de l'information, d'être optimisé. Plus le nombre de blocs créés dans la Blockchain est important, plus celle-ci devient robuste.

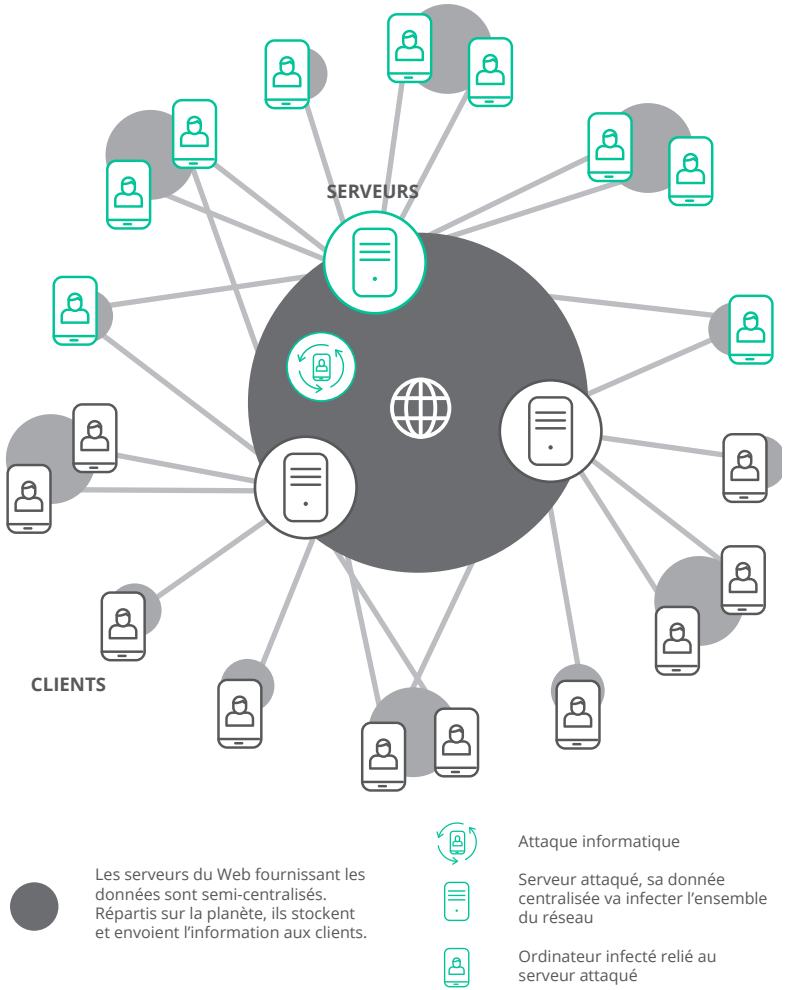
La fonction *hash* permet de sécuriser les données transactionnelles contenues dans la chaîne de blocs. Cette sécurisation est complémentaire avec l'architecture du réseau Blockchain, à savoir un réseau pair-à-pair.

II.1.b Le réseau pair-à-pair

Dans le cas particulier de la Blockchain, le réseau pair-à-pair est constitué d'ordinateurs (appelés les nœuds du réseau) possédant chacun une copie de la chaîne de blocs. L'avantage de ce maillage du réseau est de garantir une plus grande sécurité de celui-ci. Comme nous l'expliquions précédemment, dans un réseau pair-à-pair, le risque est réparti à travers les nœuds : pour y falsifier une information, il faut être capable de falsifier simultanément plus de 50 % des nœuds du réseau. Cette contrainte,

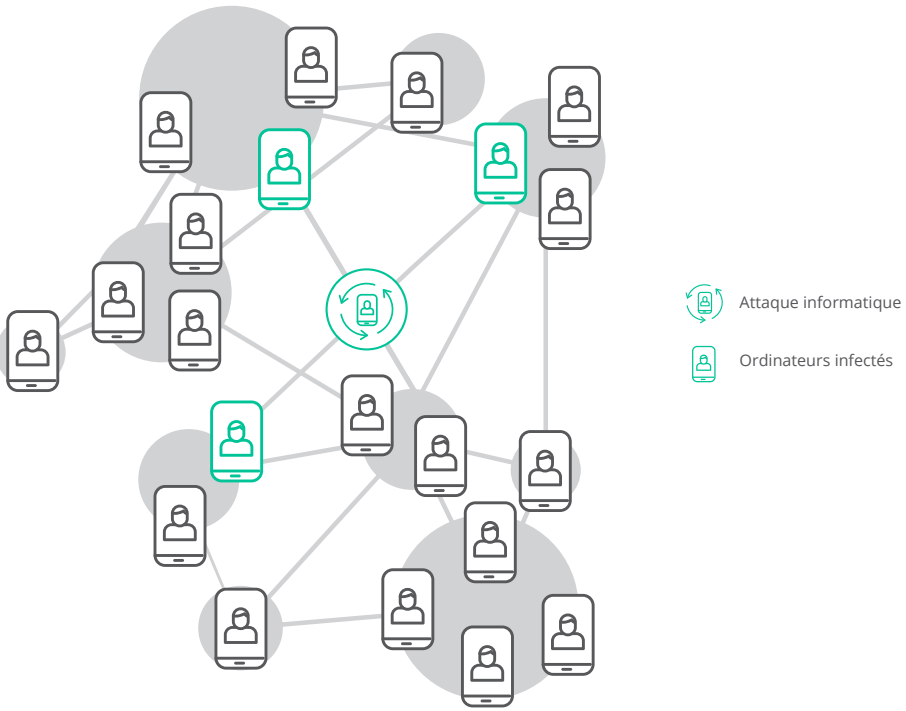
de puissance de calcul pour y parvenir, rend imperméable le réseau à ce type d'attaque. *A contrario*, dans un réseau semi-centralisé comme le Web, des attaques ciblées sur les principaux serveurs du réseau peuvent avoir des impacts plus importants[74].

ATTAQUE CONTRE UN RÉSEAU SEMI-DÉCENTRALISÉ COMME LE WEB

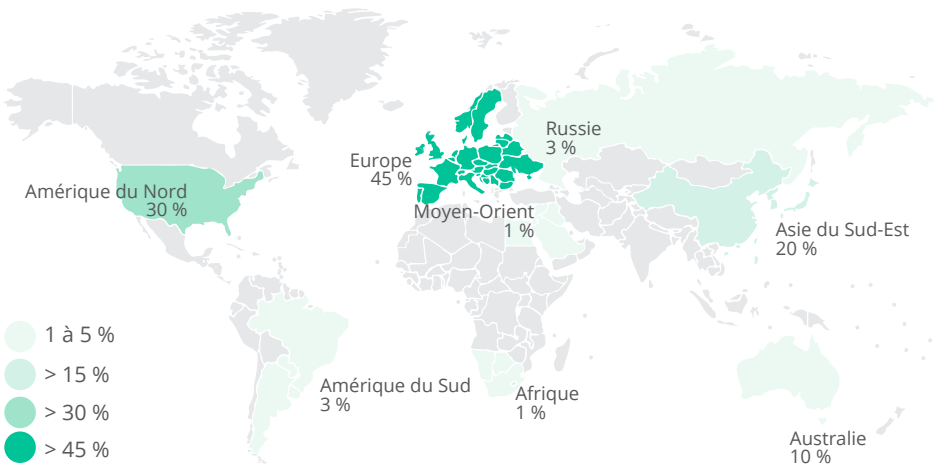


74. Pour plus de précisions sur les similitudes et différences d'une Blockchain et d'un réseau pair-à-pair, nous recommandons le blog de Valentin Kalinov. Lien : https://www.quora.com/How-is-blockchain-technology-similar-to-torrent-technology-How-is-it-different Concernant les avantages et inconvénients d'une Blockchain par rapport à une base de données décentralisée, nous recommandons le blog de Gideon Greenspan. Lien : https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

ATTAQUE CONTRE UN RÉSEAU PAIR-À-PAIR COMME LA BLOCKCHAIN



LES NŒUDS DU BITCOIN DANS LE MONDE – DÉCEMBRE 2018[75]



75. Lien : https://bitnodes.earn.com/

Conclusion : l'imbrication entre une utilisation de la fonction *hash* pour chaîner les transactions par bloc et l'utilisation du réseau pair-à-pair assure une infaillibilité au réseau.

II.2 La preuve de travail comme réponse à la contrainte des dépenses doubles

La deuxième contrainte identifiée, pour la création d'une monnaie digitale et décentralisée, est la problématique des dépenses doubles. Dans la science cryptographique, elle est souvent présentée comme le problème des généraux byzantins. Elle a été décrite en 1985 par une étude menée par Leslie Lamport, Robert Shostak et Marshall Pease[76]. Elle porte sur la transmission d'informations dans des réseaux informatiques dont les nœuds peuvent présenter une ou plusieurs failles. La problématique est illustrée sous la forme d'une métaphore où des généraux doivent se mettre d'accord pour définir un plan d'attaque pour conquérir la ville de Byzance. Disposés en cercle autour de la ville, ils doivent communiquer de manière efficace pour coordonner leurs attaques. Le problème vient du fait que des potentiels traîtres, parmi les généraux, peuvent altérer l'information transmise et, par conséquent, faire échouer l'attaque. Dès lors, il faut inventer un moyen de communication pour permettre aux généraux loyaux de communiquer efficacement entre eux sans être pollués par les messages envoyés par les traîtres.

La Blockchain, notamment pour résoudre la contrainte des dépenses doubles, doit beaucoup à cette analyse qui conjugue les problématiques de transmission de l'information dans un réseau distribué et l'algorithme qui permet aux membres du réseau de vérifier la validité de l'information transmise. Cette validation apporte une couche de sécurité au système en le protégeant contre des manipulations frauduleuses de la monnaie. Un rôle traditionnellement joué par les banques.

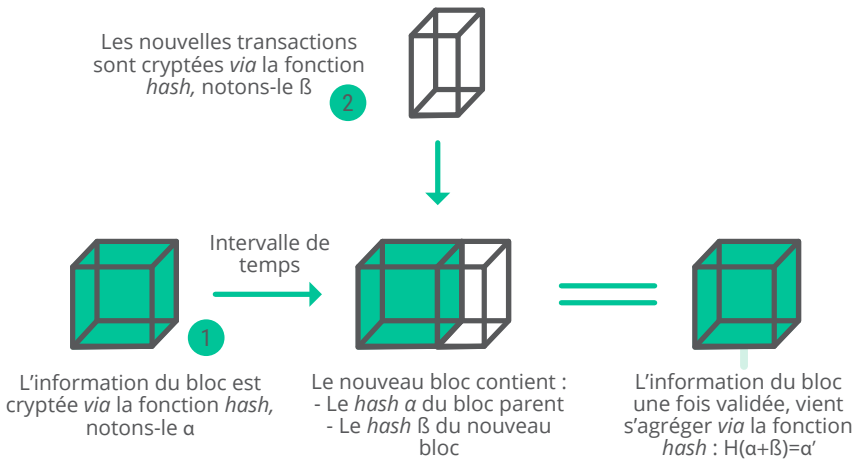
Dans l'écosystème de la Blockchain, cette validation de l'information transmise dans le réseau est appelée preuve de travail (*proof of work*). Elle consiste à faire résoudre un algorithme de consensus par les nœuds du réseau. Ceux qui jouent ce rôle sont appelés les « mineurs » dans le vocabulaire propre à l'écosystème de la Blockchain. Le rôle des mineurs est fondamental dans le fonctionnement du protocole Bitcoin puisque ce sont eux qui valident les nouvelles transactions et les enregistrent dans le grand livre qu'est la Blockchain. À noter que cet algorithme ne sert

76. Lien : https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-Byzantine-Generals-Problem.pdf

pas à vérifier la véracité des transactions en elle-même, mais à accorder l'ensemble des nœuds du réseau sur les nouvelles transactions validées à ajouter à la Blockchain. De cette façon, chaque nœud a le même historique de transactions, empêchant ainsi les doubles dépenses.

Dans le protocole Bitcoin, un bloc est « miné », c'est-à-dire validé, toutes les 10 minutes environ. Une fois validé, ce bloc vient s'ajouter à la chaîne de blocs formant le registre immuable précédemment décrit. Le schéma « Mécanisme d'imbrication des blocs avec *hashage* », en p. 75 montrait de manière simplifiée l'utilisation des *hash* dans la validation des blocs. En réalité, ces derniers contiennent plus d'informations.

COMPOSITION D'UN BLOC



	TYPOLOGIE	DESCRIPTION
	Version	Indique la dernière version du logiciel
1	*Hash* du bloc précédent	Fait référence au *hash* du bloc précédent. Dans notre schéma, α
2	L'arbre de Merkel	*Hash* résultant de l'arbre de Merkel pour inclure de nouvelles transactions. Dans notre schéma, β
	Horodatage (*Timestamp*)	Date de création du nouveau bloc
	Cible (*Target*)	L'algorithme de preuve de travail cible pour ce bloc
	Variable de consensus (*Nonce*)	Compteur utilisé pour l'algorithme de preuve de travail

La preuve de travail s'articule autour de deux concepts : celui de cible *(target)* et celui de variable de consensus *(nonce)*. Nous l'avons vu précédemment, la fonction *hash* prend un *input* des chaînes de caractères de toute taille et renvoie en *output* une chaîne de 32 – ou 64 – caractères pseudo-aléatoires. L'idée de la preuve de travail est de donner un *hash* cible en utilisant une variable de consensus *(nonce)* qui est simulée aléatoirement jusqu'à ce que le *hash* cible soit atteint. Une fois que la variable de consensus adéquat au *hash* cible a été trouvée, on considère que la preuve de travail a bien été effectuée. Considérons le code suivant :

```
import hashlib

text = "What is the hash of Accuracy"

for i in range (1, 10):

# Définition de la variable de consensus (Nonce)
nonce = range (i)

# Ajout de la variable de consensus à l'input
input = text + str (nonce)

# Calcul du hash de l'input
hash = hashlib.sha256 (input.encode («utf-8»)).hexdigest ()

# Affichage du résultat
print ("{}?\nThe hash of Accuracy is {}".format (input, hash))
```

Les *outputs* de ce code sont :

```
What is the hash of Accuracy1 ?
The hash of Accuracy is
 b2a1ab0f88a1d0ab97d3b8245c1e085e2bd57dddd7c4c12a8b1314919866dc82
What is the hash of Accuracy2 ?
The hash of Accuracy is
 5ddd665cca53e5c3071568461eae186c50542887c9a975023c053b366b418c7f
What is the hash of Accuracy3 ?
The hash of Accuracy is
 a831eab91e40ca7ad4af9355994d4adff67bbea1843eb2104f78c0ddc92bc307
What is the hash of Accuracy4 ?
The hash of Accuracy is
 fea1ce66e504e28fb464c921cad5b83302e6161a501d3b2ffd91dbf6dd9cad1e
What is the hash of Accuracy5 ?
The hash of Accuracy is
 fd36fb055505d99b07601b8432b49b0b1db09856e96160cdc8f39444923b4fccc
What is the hash of Accuracy6 ?
The hash of Accuracy is
 f368ebe56efaae3964aaac571b4bf849f94beb6891f9dc1b13a1ef90b673a20b
What is the hash of Accuracy7 ?
The hash of Accuracy is
 ce1404d41219ca09c91471b8650aed688d0c21bd8cb73a276f15229ed5463649f
What is the hash of Accuracy8 ?
The hash of Accuracy is
 dd356cc489cec40ec644db0a295f32d822aa4874b337be5a3bb923e764e378f2
What is the hash of Accuracy9 ?
The hash of Accuracy is
 3ef0d8c41488d9c81b2b1525f826ac3d35801 3ddbefef00c9fc7cd9307fb96b9
```

Plaçons-nous maintenant dans le cas où la cible qui a été fixée pour résoudre la preuve de travail est d'avoir un *hash* final dont le premier caractère commence par la lettre *a*. Dans l'exemple que nous avons simulé, le *hash* cible s'obtient au bout de 3 itérations.

Une bonne métaphore pour comprendre cette relation entre la cible, la variable de consensus et les nœuds est d'imaginer le jeu suivant : chaque participant (les nœuds) possède un jeu de 52 cartes classiques (les variables de consensus). Tour à tour, chacun tire 4 cartes aléatoirement et le premier joueur à tirer des cartes de la même couleur (la cible) gagne la partie (réussit la preuve de travail). La probabilité d'y parvenir est d'environ 1,1 %, ce qui signifie qu'il faudra en moyenne une centaine de tirages pour gagner la partie[77]. La difficulté de la preuve de travail demandée dépend de la probabilité de réussir à atteindre le résultat demandé. Plus la probabilité de succès est faible, plus le temps moyen de résolution sera long.

Il faut avoir cette analogie en tête pour bien comprendre le mécanisme de preuve de travail : c'est une compétition entre chaque nœud ou mineur du réseau qui produit des *hash* pour trouver l'*output* qui correspond à la cible fixée. Il est important de noter également que cette compétition engendre une course à l'armement en efficacité et puissance de calcul. Plus un nœud possède une puissance de calcul importante, plus sa probabilité de résoudre l'algorithme de consensus est forte. En revanche, afin de rendre le minage économiquement viable, le mineur doit optimiser la consommation électrique nécessaire au minage[78]. La compétition porte donc plus sur l'efficacité énergétique et la recherche d'économies d'échelle qu'une simple course à la puissance de calcul. Ce phénomène se traduit par une forme de centralisation (illustrée notamment par la consolidation en cours dans ce secteur), remettant en cause l'atomicité des facteurs de production. Les coûts d'électricité, l'accès à une technologie de minage de qualité, les économies d'échelle étant des données non uniformément réparties dans le monde, on assiste à un phénomène d'arbitrage géographique. Des entités dédiées au minage se créent donc principalement dans les pays les moins coûteux en électricité (notamment la Chine, le Canada ou l'Islande).

Ce constat soulève deux questions :

- La question de la localisation des nœuds (et donc des pools de minage) est une problématique géopolitique majeure, autour notamment de l'accès et du coût de l'énergie. Au-delà de l'expérience libertaire du

77. Probabilité d'obtenir 4 cartes de la même couleur (Pique, Cœur, Carreau, Trèfle) = 1× 12/51 × 11/50 × 10/49 ≈ 1,1%

78. Pour une description plus détaillée de l'équation économique du minage, voir la partie D, « Blockchain : la rencontre de l'économie et de la technologie au service du développement ? »

bitcoin et d'autres crypto-monnaies, les intérêts des États s'inscrivent en filigrane et structurent un jeu géopolitique trouble. Si la Chine semble adopter une position ambiguë envers les crypto-monnaies, elle concentre néanmoins une activité très importante d'initiatives Blockchain, que ce soit en plates-formes d'échange ou en minage. Le pays profite d'un prix du kWh compétitif (deux fois moins cher qu'en France, quatre fois moins cher qu'en Allemagne, en 2018[79]), et d'un avantage technologique dans l'électronique. Des fermes de minage gigantesques s'installent près des barrages hydroélectriques pour accéder au surplus d'électricité. Les quatre principaux pools mentionnés sur le graphique ci-dessous sont chinois (BTC.com, Antpool, ViaBTC, BTC Top) et représentent ensemble plus de 49,3 % de la puissance de calcul mondiale. Selon le média *Asialyst*, les entreprises privées du pays contrôleraient près de 70 % de la production du bitcoin[80].

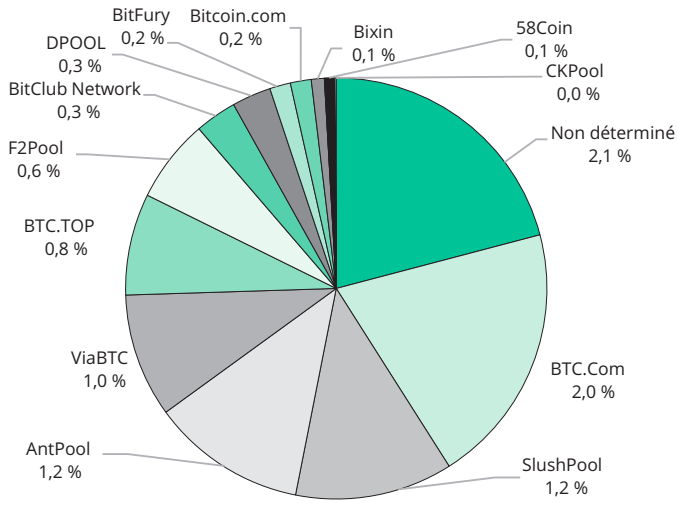
On peut toutefois noter que le deuxième semestre a été très difficile pour les principaux mineurs établis, en raison de la baisse très forte du cours du Bitcoin. À l'instar des forages pétroliers coûteux engagés lors de la période de hausse du cours du pétrole, des mineurs ont installé des capacités importantes lorsque le Bitcoin affichait un cours élevé. La chute du cours a rendu non rentables certaines exploitations, et entraîne dans la foulée un potentiel de rebattage des cartes intéressant.

- La concentration des nœuds et de la puissance de calcul sur une minorité d'acteurs est un facteur d'inquiétude générale. En effet, le principal pool concentre 21,5 % de la puissance de calcul (BTC.com) et les trois principaux pools, 53,7 %. Ce qui signifie qu'en coopérant, ces trois acteurs pourraient à eux seuls détruire le bitcoin ou organiser un vol massif de bitcoins en falsifiant la chaîne. En réalité – et c'est tout l'intérêt du protocole –, ils n'ont aucun intérêt à le faire puisqu'un tel événement détruirait la confiance dans le bitcoin et sa valeur tomberait instantanément ou presque à zéro. Pour prendre une image, une telle action reviendrait à braquer une banque et brûler automatiquement les billets à l'instant même où ils seraient dérobés. Rationnellement, une telle opération ne peut donc pas venir de ces trois acteurs.

---

79. Lien : https://www.statista.com/statistics/263492/electricity-prices-in-selected-countries/
80. Bertrand Hartman, *La Chine, puissance dominante du bitcoin, crypto-monnaie libertaire,* 12/09/2017. Lien : https://asialyst.com/fr/2017/09/12/chin-puissance-dominante-bitcoin-crypto-monnaie-libertaire/

RÉPARTITION DE LA PUISSANCE DE CALCUL À L'ÉCHELLE MONDIALE PAR NŒUD[81]



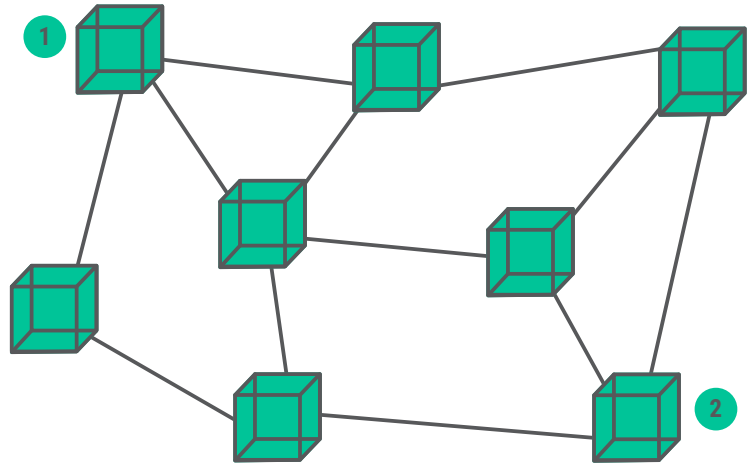
La question que l'on peut se poser naturellement, alors, est : qui fixe cette cible (le *nounce*) à atteindre ? Sans entrer dans des considérations trop techniques, il faut savoir que la cible à trouver est un paramètre dynamique dont le niveau de difficulté est fixé, de manière probabiliste, pour que le temps de calcul moyen pour y parvenir soit d'environ 10 minutes. Le niveau de difficulté s'adapte donc à la puissance de calcul disponible du réseau, c'est-à-dire la puissance de calcul totale fournie par l'ensemble des nœuds.

Dès qu'un nœud du réseau trouve la solution du puzzle cryptographique, celle-ci est sélectionnée par l'algorithme de consensus. Le bloc est ensuite ajouté à la Blockchain et horodaté, ce qui permet d'avoir un continuum chronologique et de retracer l'histoire des transactions dans le temps. Mais que se passe-t-il si deux nœuds, par un hasard peu probable mais possible, résolvent en même temps l'algorithme de *hash* ? De manière générale, comment réussir à garder une information consistante dans un réseau décentralisé où peuvent se propager des informations contradictoires ?

Dans le cas où deux nœuds arrivent à résoudre, de manière quasi simultanée, l'algorithme de preuve de travail, il se passe ce qui est appelé un *Fork.* Partons de la situation où tous les nœuds du réseau possèdent la même information :

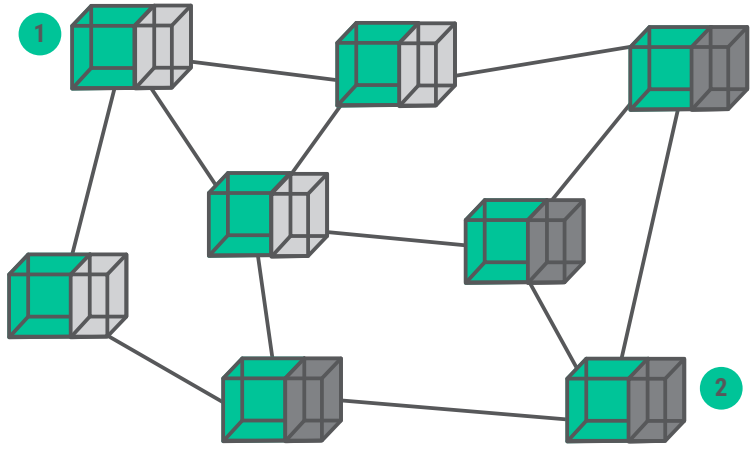
81. Lien : https://Blockchain.info/fr/pools

ÉTAPE Nº 1 : L'ENSEMBLE DU RÉSEAU POSSÈDE LA MÊME INFORMATION[82]



Après cet état initial, les nœuds 1 et 2 de ce réseau réussissent de manière quasi simultanée à résoudre l'algorithme permettant de valider un nouveau bloc pour l'ajouter à la chaîne de blocs. Ces nœuds propagent alors la nouvelle chaîne de blocs à leurs voisins.

ÉTAPE Nº 2 : LES NŒUDS RÉSOLVENT L'ÉQUATION ET PROPAGENT LE NOUVEAU BLOC



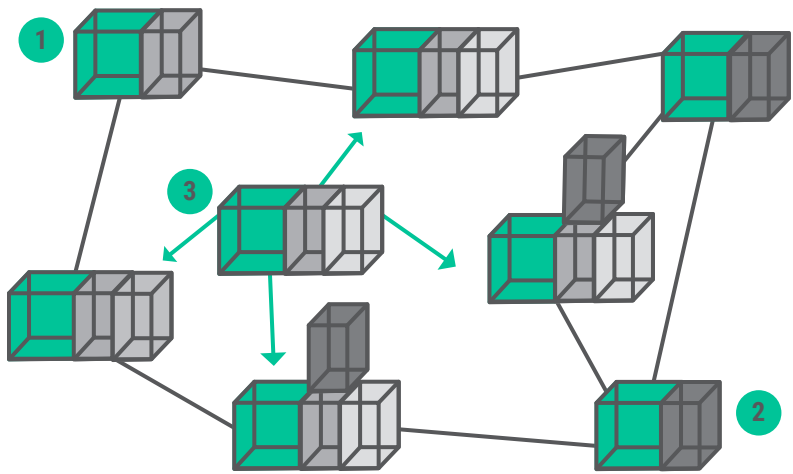
82. Les graphiques concernant le *Fork* sont inspirés de ceux de l'ouvrage *Mastering Bitcoin* d'Andreas Antonopoulos, O'Reilly, 2017, 2e éd., p. 241-246, chapitre « *Assembling and Selecting Chains of Blocks* ».

À l'étape 2, la Blockchain est divisée en deux états : d'une part, les nœuds qui ont reçu comme nouveau bloc valide l'information du nœud numéro 1, et d'autre part, ceux ayant reçu l'information du nœud numéro 2. À ce stade, aucune de ces deux versions ne pourrait être considérée comme la bonne ou la mauvaise : chaque nouveau bloc a bien été validé *via* un processus de preuve de travail. Bien que deux versions de la Blockchain cohabitent momentanément, le processus de création de blocs continue *via* le minage d'un nouveau bloc. Le nœud qui arrivera à résoudre en premier la nouvelle preuve de travail validera le chemin à prendre pour la Blockchain.

À l'étape 3, le nœud numéro 3 a trouvé la solution le premier pour miner un nouveau bloc. Comme il avait reçu l'information du bloc numéro 1 en premier lors de la dernière itération, il propagera cette information dans le réseau. La règle étant que la chaîne de blocs la plus longue fait foi : les nœuds qui avaient reçu l'information du nœud numéro 2 en premier sont contraints d'accepter la nouvelle chaîne de blocs. L'information se propage ainsi de proche en proche pour harmoniser l'information contenue dans la Blockchain pour finalement arriver à un consensus.

ÉTAPE Nº 3 : UN NŒUD MINE UN NOUVEAU BLOC ET LE PROPAGE

Le nœud n°3 avait reçu le bloc
du nœud n°1 en premier.
Il considère donc que c'est
le bloc parent qui est valide.

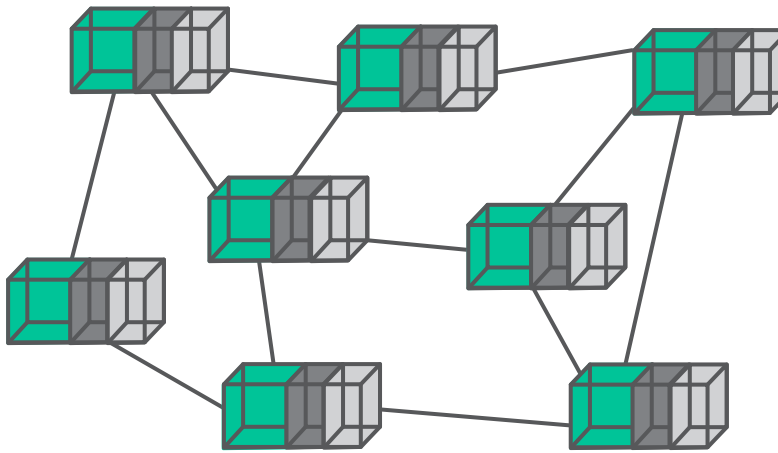


Un nœud doit valider
en priorité la chaîne de blocs
la plus longue. Il révise ainsi
son historique de bloc.

En théorie, il est possible qu'à l'étape 3, deux nœuds résolvent encore de manière quasi simultanée l'algorithme de consensus. Dans ce cas peu probable, une nouvelle itération est nécessaire pour arriver à un consensus.

Conclusion : la mise en place de cible et de variable de consensus permet de créer une concurrence entre les nœuds du réseau Blockchain pour valider les nouveaux blocs. Le fait d'horodater cette création permet de créer un continuum historique et de garder l'ensemble des transactions dans leur chronologie. Enfin, la règle de propagation dans le réseau permet d'harmoniser l'information dans la Blockchain et de se prévenir contre toute tentative de dépenses doubles.

ÉTAPE Nº 4 : L'INFORMATION EST HARMONISÉE DANS LA BLOCKCHAIN



II.3 Les clés cryptographiques comme réponse à la contrainte de confidentialité

Chaque utilisateur du réseau possède deux clés cryptographiques : une clé privée et une clé publique. Ces deux clés cryptographiques pourraient être assimilées à l'IBAN *(International Bank Account Number)* et le code confidentiel pour se connecter aux données de son compte en banque. La clé publique, comme son nom l'indique, permet de transmettre des

bitcoins entre utilisateurs. La clé privée permet à un utilisateur de créer de nouvelles transactions. Plus simplement, le couple clé privée/clé publique peut être assimilé au fonctionnement d'une boîte aux lettres : mon adresse publique me servira à recevoir des paiements (comme on déposerait une lettre), que je ne peux manipuler qu'à condition de pouvoir ouvrir la boîte aux lettres, grâce à la clé privée. Cependant, si mon voisin récupère la clé de ma boîte aux lettres (ou la clé privée de mon portefeuille Bitcoin), il pourra sans problème lire l'ensemble de mon courrier.

Concrètement, lorsque j'effectue une transaction grâce au réseau Bitcoin, celle-ci est chiffrée grâce ma clé privée. Comme je suis le seul à posséder cette clé, le réseau est sûr que c'est bien moi qui ai initié la transaction. Celle-ci est ensuite déchiffrée par le réseau grâce à ma clé publique – les nœuds du réseau peuvent alors vérifier la véracité de la transaction.

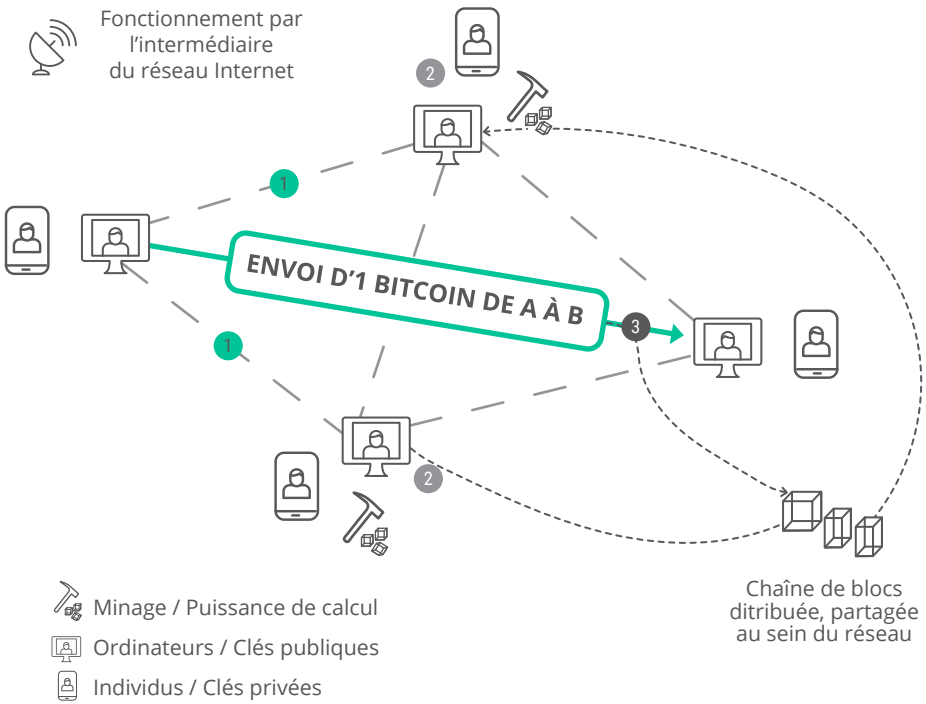
La confidentialité du protocole Bitcoin vient du fait qu'il n'y a pas de lien entre une clé publique et une identité. La clé publique joue le même rôle qu'un pseudonyme sur Internet.

En résumé, grâce à la combinaison ingénieuse du registre distribué, de la fonction *hash* (cryptographie), du mécanisme de preuve de travail, de l'existence d'une clé privée et d'une clé publique, la Blockchain, *via* le protocole Bitcoin, réussit à répondre de manière efficace aux trois principales contraintes que nous avions identifiées pour faire émerger une monnaie décentralisée et digitale, à savoir : sécurité, double dépense et confidentialité *via* l'utilisation d'un pseudonyme.

En conclusion, la technologie Blockchain sous-jacente au protocole Bitcoin est une révolution conceptuelle puisque c'est la première forme aussi achevée de monnaie décentralisée et digitale. Cette technologie permet, en effet, de répondre aux trois problématiques identifiées pour voir émerger une telle monnaie. L'originalité de cette révolution réside dans le fait qu'elle provient d'un agencement innovant de technologies préexistantes (science informatique et cryptographique).

Si la technologie Blockchain sous-jacente au protocole Bitcoin est révolutionnaire par sa démarche, il n'en demeure pas moins que la restreindre au seul protocole Bitcoin ne permet pas de saisir tout son potentiel. Par un effet de cliquet technologique, le concept initial a, en effet, laissé place à un foisonnement d'innovations dépassant largement le concept de crypto-monnaie pour former l'univers de la Blockchain 2.0, univers dont le big bang porte un nom : « Ethereum ».

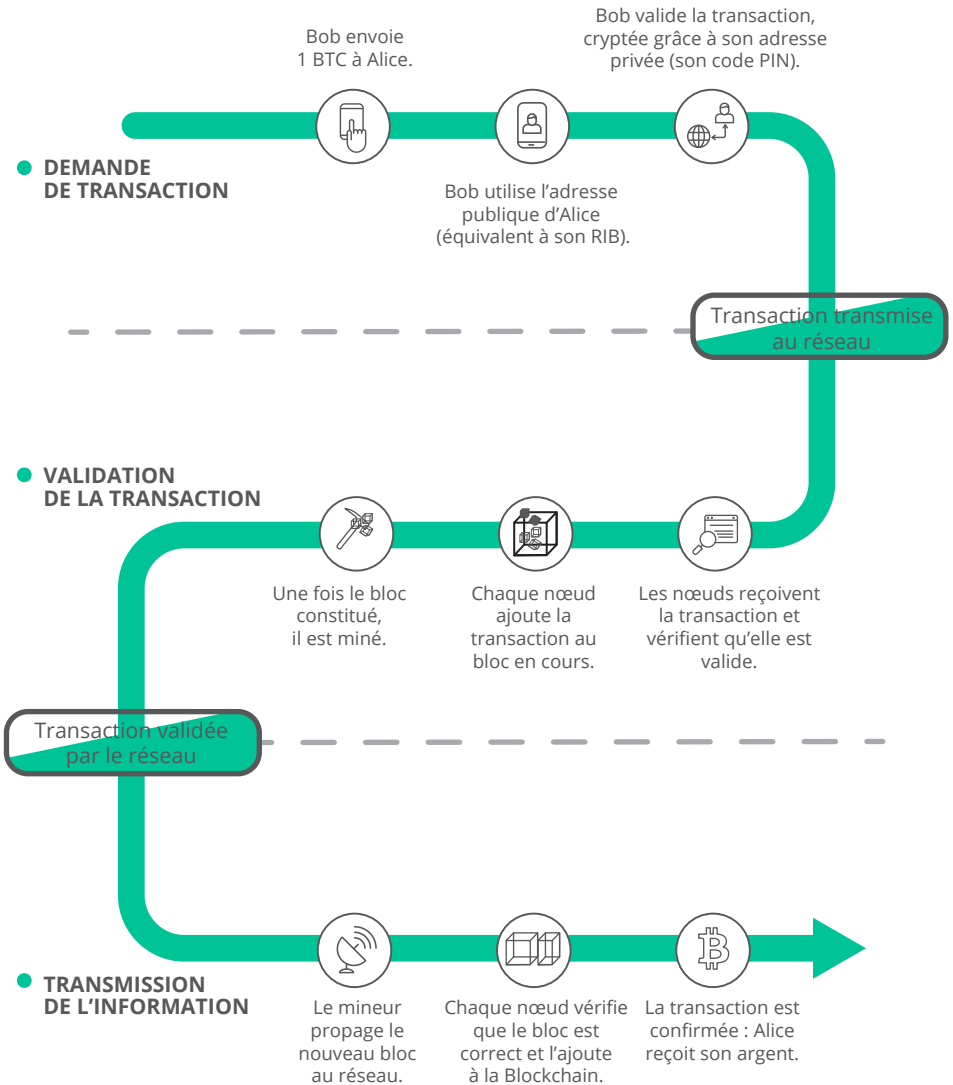
VUE SIMPLIFIÉE DU RÉSEAU BITCOIN



Suppression de la notion de confiance *intuitu personae* par la technologie

1. A envoie l'information qu'il souhaite envoyer à B 1 BTC ; cette information est cryptée et envoyée à l'ensemble du réseau.
2. Le réseau fait tourner des algorithmes de décryptage permettant de valider la transaction. Les hommes ne jouent aucun rôle dans ce processus de minage une fois les algorithmes et les ordinateurs configurés : c'est la puissance de calcul qui est différenciante.
3. B reçoit 1 BTC. La transaction est enregistrée dans une chaîne de blocs, registre infini distribué et décentralisé auprès des différents nœuds, la rendant infalsifiable et inviolable.

SYNTHÈSE DES ÉTAPES D'UNE TRANSACTION UTILISANT LE PROTOCOLE BITCOIN



III.
L'ère de la Blockchain 2.0 : un big bang nommé Ethereum[83]

III.1 Ethereum : quelles évolutions pour quels usages ?

Pour bien mesurer l'impact d'Ethereum sur l'écosystème de la Blockchain, repartons de l'analogie avec Internet : le réseau ARPANET et les protocoles TCP/IP étaient en rupture avec les systèmes de communication des années 1960-1980. Néanmoins, ce qui a permis à Internet de changer de dimension et de toucher un public plus large, fut incontestablement la création du Web. En effet, c'est *via* le Web que le grand public et les entrepreneurs ont pu, peu à peu, s'approprier les potentialités d'Internet : création de nouveaux canaux de vente pour les entreprises grâce au e-commerce, création de nouveaux moyens d'interagir entre individus grâce aux réseaux sociaux… Le Web est la brique technologique d'Internet qui a rendu possible le changement d'échelle. Le protocole Ethereum est la brique technologique de la Blockchain qui permet à cette dernière de changer d'échelle.

Le Livre blanc du protocole Ethereum a été publié en décembre 2013 par Vitalik Buterin[84] qui, à la différence de Satoshi Nakamoto, n'a pas souhaité rester anonyme. Pour développer cette technologie, la fondation Ethereum a lancé, début 2014, une ICO *(Initial Coin Offering)*[85] qui lui a permis de lever près de 18 millions de dollars. À la suite de cette ICO, plusieurs mois de développement ont été nécessaires pour que le protocole Ethereum et sa technologie Blockchain sous-jacente soient mis en service, sous le nom de *Frontier* en juillet 2015.

Le protocole Ethereum a, en effet, été conçu comme une plate-forme permettant à tout le monde de développer des applications. Ces applications fonctionnent de manière sécurisée, transparente et décentralisée,

83. Lien : https://www.ethereum.org/
84. Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, 2013.
85. Nous étudierons le concept d'ICO dans les parties suivantes. Néanmoins, pour en avoir une compréhension rapide, il faut l'assimiler à une IPO *(Initial Public Offering)* ou introduction en bourse. Sauf qu'à la différence de celle-ci, ce sont des jetons (*tokens*) qui sont émis et non des actions. Dans le cadre d'Ethereum, ce sont des « ethers » qui ont été émis. Ces ethers sont aujourd'hui négociables sur toutes les plates-formes d'échange des crypto-monnaies.

reprenant ainsi les piliers conceptuels de la technologie Blockchain. L'originalité du projet Ethereum est que celui-ci dépasse la simple ambition technologique : autour de lui s'est constituée une communauté de développeurs, très active, proposant des innovations et définissant de manière collaborative la gouvernance du protocole. Il n'en demeure pas moins que le protocole Ethereum a connu un développement constant, favorisant l'émergence de nouveaux concepts et de nouvelles applications. Pourquoi le développement d'applications ne pouvait pas être effectué *via* le protocole Bitcoin ? Quelles sont les évolutions techniques liées au protocole Ethereum ? Répondre à ces questions demande de se plonger dans la science informatique et de clarifier les notions de langage « Turing Complet » et « d'état ».

III.2 Le protocole Ethereum repose sur la notion d'état

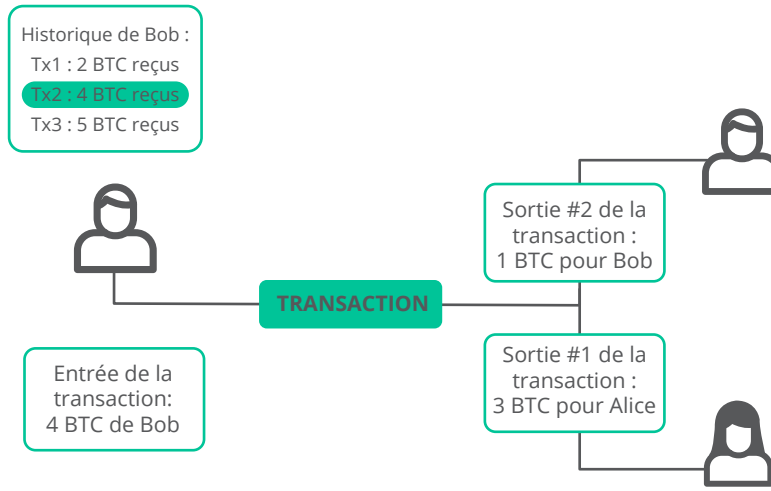
La grande évolution apportée par l'Ethereum est l'intégration de la notion d'état dans le langage informatique du même nom. Dans le protocole Bitcoin, pour un instant donné, le solde d'un compte Bitcoin n'est pas défini en tant que tel. Le seul moyen de connaître le solde d'un compte est de le calculer en totalisant l'ensemble des transactions effectuées depuis la même adresse publique (plus exactement depuis le même *wallet*). Les comptes en banque que nous utilisons usuellement proposent des soldes de compte dynamiques où le montant disponible s'effectue en lecture directe. Toute dépense, ou tout revenu, vient réduire, ou augmenter, le montant du solde qui s'actualise et nous permet de connaître immédiatement notre solde disponible.

Le mécanisme de solde de compte propre au protocole Bictoin, est moins linéaire que celui avec lequel nous avons l'habitude de fonctionner. En effet, lorsqu'un utilisateur dépense des bitcoins, le montant dépensé est calculé comme la différence entre la somme des bitcoins reçus et ceux non dépensés, d'où la notion d'*Unspend Transaction Outputs*, abrégé en Utxos.Pour bien saisir la particularité de la notion d'Utxos, plaçons-nous dans l'exemple suivant : Bob souhaite effectuer une transaction de 3 bitcoins vers Alice. Bob possède un identifiant lui permettant de se connecter à la Blockchain Bitcoin. En observant son historique, on peut lire qu'il a reçu trois transactions :

- Transaction #1 : 2 bitcoins reçus ;
- Transaction #2 : 4 bitcoins reçus ;
- Transaction #3 : 5 bitcoins reçus.

Si Bob possédait un compte en banque classique avec un solde de compte dynamique, ce dernier s'élèverait donc à 11 bitcoins, soit la somme de trois paiements reçus. La transaction de 3 bitcoins qu'il souhaite effectuer pour Alice viendrait immédiatement réduire son compte à 8 bitcoins sans qu'il soit nécessaire d'effectuer une opération supplémentaire. Mais comme nous l'expliquions précédemment, la notion d'Utxos empêche de calculer de manière additive un solde de compte. Par conséquent, pour effectuer le virement de 3 bitcoins vers Alice, Bob doit utiliser une de ses trois transactions reçues et non dépensées. Si Bob choisit d'utiliser la transaction #2 (de 4 bitcoins) pour transférer 3 bitcoins à Alice, il doit créer une seconde transaction de 1 bitcoin pour lui-même afin de ne pas « perdre » le bitcoin supplémentaire de la transaction #2. Cette limite s'explique par le fait que les Utxos sont binaires et, par conséquent, n'acceptent que deux états : dépensés ou non dépensés.

EXEMPLE DE TRANSACTION AVEC LA CONTRAINTE DE UTXOS



Ce principe fonctionne très bien dans le cas du protocole Bitcoin mais rend impossible le développement d'applications plus complexes. En effet, dans le cadre du protocole Bitcoin, il est difficile de définir en lecture directe, à un instant donné, le solde de plusieurs comptes. De plus, il est très difficile de configurer des contrats mettant en jeu plusieurs intervenants, avec des conditions de versement plus avancées qu'un simple transfert de valeur. Le protocole Ethereum propose de dépasser la notion d'Utxos qui s'appuie sur des soldes de transactions, en se structurant autour de la notion d'état qui permet de connaître en lecture directe le solde d'un compte.

III.3 Ethereum repose sur un langage Turing Complet

Ethereum propose deux évolutions techniques par rapport au protocole Bitcoin. La première réside dans le fait qu'il propose un langage de programmation dit « Turing Complet ». Sans entrer dans les détails techniques, il faut comprendre que le langage Ethereum facilite grandement le travail des développeurs informatiques puisqu'il permet à ces derniers d'utiliser l'ensemble des fonctionnalités habituelles, par exemple les boucles, simplifiant l'implémentation de tâches répétitives.

La seconde évolution est que chaque nœud, en participant au réseau, utilise un logiciel appelé l'EVM (*Ethereum Virtual Machine*). De manière simplifiée, ce logiciel imite le fonctionnement d'un ordinateur et permet d'exécuter une série d'instructions informatiques.

Les deux principales évolutions technologiques du protocole Ethereum sont donc l'introduction d'un langage Turing Complet couplé avec l'utilisation de la notion d'état. Cette articulation de ces deux notions lui permet de proposer le développement d'applications. Cependant, ces éléments ne nous permettent pas de saisir les spécificités de fonctionnement du protocole Ethereum.

III.4 Deux familles de comptes dans Ethereum

Le protocole Ethereum, nous l'avons vu, est structuré autour de la notion de compte et non pas de transactions. Cette notion de compte se scinde en deux familles : les *Externally Owned Accounts* et les *Contract Accounts* :

- les *Externally Owned Accounts* (ci-après EOA) sont contrôlés par des personnes physiques[86] et sont accessibles *via* une clé privée. De la même manière qu'un compte Bitcoin, ils peuvent servir à effectuer des transactions en ethers (la crypto-monnaie sous-jacente au protocole Ethereum). Comme nous l'expliquions précédemment, à la différence des comptes Bitcoin, les comptes Ethereum offrent un solde de tout compte en lecture directe ;

- les *Contract Accounts* sont des comptes que l'on pourrait comparer à des personnes morales ou des robots informatiques. Ces robots informatiques permettent une interaction avec les EOA. Cette

86. Ou des personnes morales avec l'utilisation de l'*Internet Of Thing* (IoT).

interaction prend la forme d'exécution automatique de transactions dont les paramètres sont envoyés par les EOA[87].

L'existence de ces deux types de contrat permet de créer des interactions dynamiques dans la Blockchain Ethereum. L'existence de robots informatiques apporte, en effet, de la fluidité à la Blockchain tout en autorisant un certain nombre d'opérations plus complexes qu'une simple transaction, comme un versement conditionnel dans le cas d'un pari. Cette complexification des usages offre la possibilité de développer des *Smart Contracts* sur la Blockchain Ethereum. Les *Smart Contracts* sont à la technologie Blockchain ce qu'est le Web à la technologie Internet : ils permettent une démultiplication des usages possibles de la technologie Blockchain et ouvrent ainsi la voie au développement d'un nouvel écosystème. Mais qu'entendons-nous par *Smart Contract* ? Quelle valeur apportent-ils à l'écosystème Blockchain ?

III.5 Les *Smart Contracts*, les contrats de demain ?

Les *Smart Contracts* sont une adaptation du concept de contrat, dans l'économie traditionnelle, à l'écosystème de la Blockchain.

Repartons de la définition de « contrat » donnée par le Larousse : « Convention, accord de volontés ayant pour but d'engendrer une obligation d'une ou de plusieurs personnes envers une ou plusieurs autres. » Le contrat est un objet que chacun manipule quotidiennement sans forcément en avoir conscience puisque chaque transaction commerciale, aussi simple soit-elle – une commande de café –, est un contrat passé entre un consommateur et un professionnel. Certaines transactions plus complexes nécessitent néanmoins la création d'un contrat écrit et signé entre les différentes parties prenantes dans le but d'ancrer les différentes obligations de chacun dans des termes et clauses clairement définis. La confiance donnée à un contrat est un élément fondamental dans la bonne conduite des transactions commerciales et donc, plus largement, de la vie économique. Notons toutefois que la confiance que l'on porte à un contrat est en réalité une confiance portée au système entourant et garantissant le contrat : la loi, les représentants de la loi et, plus largement, l'État. Ces entités constituent les tiers de confiance qui garantissent la sécurité des contrats.

---

87. Lien : ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#externally-owned-accounts-eoas

Les *Smart Contracts* développés sur la Blockchain Ethereum sont des contrats au sens traditionnel du terme puisqu'ils permettent de définir des obligations réciproques entre une ou plusieurs personnes. Néanmoins, ils s'inscrivent également dans l'écosystème Blockchain puisqu'ils s'appuient sur les piliers technologiques propres à la Blockchain et identifiés pour le protocole Bitcoin, à savoir : décentralisation grâce à un réseau informatique pair-à-pair, sécurité grâce à un mécanisme dit de preuve de travail (nécessitant un réseau de mineurs), et immuabilité grâce à la construction d'une chaîne de blocs s'appuyant sur des fonctions cryptographiques[88]. À cela nous pourrions ajouter un autre pilier, celui de l'automaticité qui permet au contrat d'avoir la qualité de *Smart.* Les étapes de construction et le déploiement d'un *Smart Contract* sont donc les suivantes :

- le contrat est créé à partir d'un EOA et représente un état et/ou une suite d'actions conditionnelles qui définissent son objet. Dans la majorité des cas, il est écrit dans un langage de programmation spécifique appelé Solidity ;
- le contrat est ensuite déployé sur la Blockchain et ne peut plus être modifié, y compris par l'EOA qui l'a déployé : les nœuds du réseau reçoivent l'information du contrat et le mécanisme de minage propre à la Blockchain Ethereum permettra de l'intégrer à la chaîne de blocs et d'ainsi lui garantir sécurité et immuabilité ;
- lorsque le contrat est déployé, une adresse publique lui est liée, ce qui permet de l'exécuter en pointant vers cette adresse et donc d'être certain que l'exécution des termes concernera seulement les parties prenantes du contrat ;
- lorsque les conditions sont remplies, des clauses du contrat s'activent et engendrent un changement d'état, cette information est transmise à l'ensemble des nœuds du réseau. La transition d'état est enregistrée dans le bloc en cours puis est validée par minage.

Pour comprendre concrètement l'utilité des *Smart Contracts*, prenons l'exemple d'un contrat d'assurance couvrant contre un risque de mauvais temps pendant des vacances programmées au soleil. Usuellement, la charge de la preuve incombe au consommateur, qui devra en plus faire toutes les démarches administratives auprès de son assureur pour faire valoir ses droits. Plaçons-nous désormais dans le cas où le contrat aurait été contracté sous la forme d'un *Smart Contract* déployé sur la Blockchain Ethereum. En cas de mauvais temps, les clauses du contrat se déclenchent automatiquement et l'assuré n'a plus à apporter la charge de la preuve ni à faire de démarche administrative.

---

88. Henning Diedrich, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, 2016.

Cet exemple simple soulève néanmoins une question : comment la Blockchain arrive-t-elle à intégrer l'information selon laquelle la météo aurait été capricieuse ? Répondre à cette question nécessite d'introduire la notion d'« oracle ». Dans l'écosystème Ethereum, un oracle est une source extérieure qui vient fournir des informations permettant l'exécution de certains termes du contrat. Dans notre exemple précédent, le rôle d'oracle pourrait être joué par des stations météo connectées à la Blockchain Ethereum et fournissant toutes les heures des données météorologiques.

La notion d'oracle fait émerger un certain nombre de paradoxes et de contradictions :

- le réseau décentralisé d'exécution du contrat qu'est la Blockchain dépend d'une source centralisée pour son fonctionnement ;
- le réseau sécurisé qu'est la Blockchain dépend d'une source dont on ne peut, *a priori*, garantir avec le même niveau d'exigence la fiabilité ;
- plus largement, une des ambitions de la technologie Blockchain est de supprimer le tiers de confiance, la nécessité d'un oracle ne constitue-t-elle pas un déplacement du tiers de confiance ?

Pour répondre à ces paradoxes, nombre de solutions sont envisagées : multiplier les oracles pour une même information afin de pouvoir confronter les données et garder un certain niveau de décentralisation, avoir recours à des services dit *provable-honest* qui permettent de s'assurer que les données envoyées par l'oracle à la Blockchain sont bien similaires à celles présentes dans les bases de données Internet de l'oracle. À cet égard, la société Oraclize propose une solution permettant de vérifier que la donnée entrée dans la Blockchain est identique à celle présente sur Oraclize. La preuve de l'exactitude de la donnée est publique ; dès lors, si Oraclize introduit des données erronées, l'ensemble du réseau pourra s'en apercevoir et apporter les modifications nécessaires[89].

III.6 Du *gas* dans le minage

Le protocole Ethereum, nous l'avons vu, repose sur les mêmes piliers technologiques que le protocole Bitcoin. Ainsi, tout comme pour le protocole Bitcoin, la sécurité, la fiabilité et donc la viabilité de la Blockchain Ethereum nécessitent l'existence d'un réseau d'ordinateurs connectés mettant à disposition une puissance de calcul afin de réaliser la preuve de travail

89. Lien : https://dev.oraclize.it/

ou minage. Le minage, sur le protocole Ethereum, reprend le même principe que sur le Bitcoin : c'est une compétition entre les nœuds du réseau pour la résolution d'une équation cryptographique à caractère aléatoire. Le nœud gagnant emporte la mise et se voit rétribuer sous forme d'ethers.

L'usage de l'ether est néanmoins différent de celui du bitcoin. Ce dernier, purement monétaire, est centré sur le transfert et l'échange d'actifs digitaux. Cela explique pourquoi la rémunération des mineurs se fait soit par le processus de création monétaire soit par l'apparition de frais de transaction et s'apparente ainsi à un fonctionnement bancaire dans l'économie traditionnelle. L'ether, en revanche, a un usage centré sur la mise à disposition d'une infrastructure informatique permettant le développement de *Smart Contracts*. Pour faire vivre cette infrastructure et la rendre rentable d'un point de vue économique, il faut que son utilisation soit payante en fonction de l'usage qu'on y fait. C'est pourquoi toute action sur la Blockchain Ethereum est payante, en ethers : du déploiement d'un *Smart Contract* à la réalisation d'une simple addition dans un autre contrat. Ce prix est variable et dépend de la complexité de la tâche à réaliser, ainsi que de la puissance de calcul nécessaire à sa réalisation. Pour déterminer le prix d'une action, chaque tâche se voit attribuer une consommation de *gas*. Le *gas* est donc l'unité de mesure des ressources de calcul nécessaire pour réaliser une opération sur la Blockchain Ethereum. Cette unité de mesure est associée à un *gas price* en ethers. Ainsi, pour chaque opération effectuée qui nécessite une quantité G de *gas* pour un *gas price* en ethers de P, est associé un montant en ethers égal à G x P qui sera reversé au mineur ayant résolu l'équation cryptographique. Le montant de *gas* nécessaire pour chaque opération (addition…) est public et défini par la communauté.

Si ce fonctionnement peut, de prime abord, sembler difficile à appréhender, il est similaire au mode de calcul de notre facture électrique : à chaque utilisation d'un équipement d'une maison (four, chauffage, plaque à induction, lumière) est associée une consommation électrique exprimée en kilowattheure (le *gas* pour le protocole Ethereum). Le kilowattheure a un prix équivalent en euro (le *gas price* pour le protocole Ethereum), qui nous permet d'en déduire le prix de notre consommation : Kilowattheure * Prix du Kilowattheure (G x P pour le protocole Ethereum).

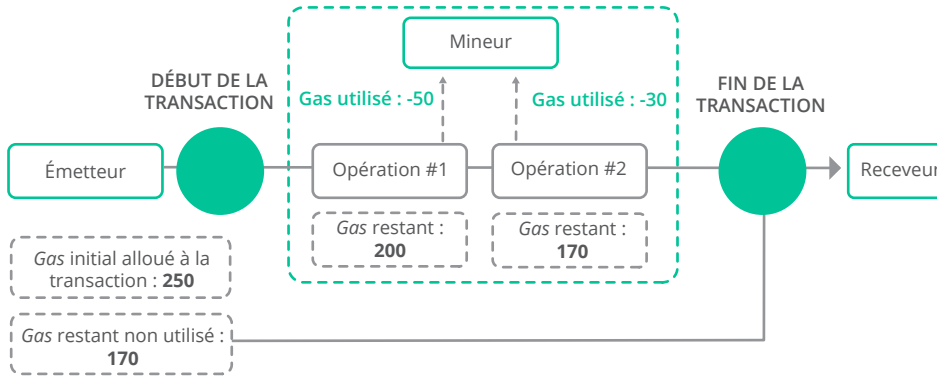
D'un point de vue concret, le déploiement d'une transaction sur le protocole Ethereum suit les étapes suivantes :

- Avant chaque transaction, l'expéditeur doit préciser la quantité de *gas* limite employée, c'est-à-dire la quantité de ressources de calcul maximale que l'exécution peut consommer. Cette quantité doit couvrir la lecture des données, l'exécution par l'EVM.

- L'utilisateur renseigne ensuite le prix associé au *gas*. Lors du lancement de la version actuelle d'Ethereum, un *gas price* par défaut a été défini (5.10^-8 ETH ~ 0,00005 dollar américain aujourd'hui). Ce prix, purement indicatif, est maintenant fixé par le marché. L'utilisateur peut choisir d'associer un prix plus élevé s'il veut que sa transaction soit validée plus vite par les mineurs qui cherchent, en tant qu'agents rationnels d'un marché, à maximiser leur gain. L'utilisateur peut également décider d'associer un prix plus faible, mais il existe alors un risque que sa transaction ne soit pas prise en compte par les mineurs.

- Le nœud du réseau qui mine le bloc (donc qui est le premier à résoudre l'équation cryptographique) contenant la transaction est rémunéré par le montant en ethers correspondant au *gas price* fois la quantité de *gas* utilisée pour cette transaction.

EXEMPLE DE TRANSACTION AVEC CONSOMMATION DE *GAS*



- S'il reste du *gas* par rapport au montant prévu par l'expéditeur de la transaction, il lui est reversé. C'est pourquoi la majorité des utilisateurs préfèrent prévoir un montant total de *gas* supérieur à leurs besoins réels.

- Au contraire, si la transaction n'aboutit pas, ou si le montant limite de *gas* est dépassé, l'exécution est annulée. Le mineur du bloc touche néanmoins la totalité des *gas* liés au message de l'émetteur[90].

90. Gavin Hood, Andreas Antonopoulos, *Mastering Ethereum*,O'Reilly, 2018. Lien : https://ethereumbook.info/

III.7 Les évolutions technologiques du protocole Ethereum

Bien que beaucoup plus abouti que Bitcoin, le protocole Ethereum présente aujourd'hui encore quelques limites technologiques, sur lesquelles la communauté Ethereum, très active, cherche et propose des solutions. Exemple ? La consommation d'énergie. Pour éviter de centrer la compétition autour de la mise à disposition d'une puissance de calcul toujours plus importante (et donc énergivore), une nouvelle forme de validation est en cours de développement : le *proof-of-stake*.

Pour réduire la consommation d'énergie du réseau, Ethereum compte changer son algorithme de minage, en passant du *proof-of-work* au *proof-of-stake*. Le *proof-of-stake* (preuve d'enjeu) repose sur la nécessité pour les mineurs, appelés validateurs dans ce contexte, de prouver qu'ils ont mis sous séquestre une certaine somme en ethers pour pouvoir valider un bloc :

- les mineurs déposent un montant d'ethers sur un compte séquestre utilisé dans le cadre du processus de *proof-of-stake*. Ces mineurs sont alors considérés comme des validateurs ;
- un algorithme choisit aléatoirement un validateur avec la règle de sélection suivante : plus un validateur a déposé d'ethers sur le compte séquestre, plus il a une probabilité forte d'être sélectionné ;
- une fois le validateur sélectionné, il peut procéder au minage.

Le *proof-of-stake* définit un ensemble de règles auquel les validateurs sont soumis : interdiction de voter sur deux blocs concurrents, de proposer un bloc invalide… Si des validateurs ne respectent pas ces règles, ils perdent le montant d'ethers qu'ils avaient mis sous séquestre.

Le *proof-of-stake* engendre ainsi une compétition centrée sur la possession d'ethers et non plus sur la puissance de calcul disponible. Cela permet d'éviter une sorte de course à l'armement où chaque nœud cherche à avoir le meilleur matériel informatique afin de disposer d'une puissance de calcul toujours plus importante, dans le but d'avoir les meilleures chances de remporter la mise. Cette « course à l'armement » informatique est une des raisons de la grande consommation énergétique qu'implique l'utilisation du *proof-of-work*.

Le protocole Ethereum s'appuie sur les mêmes piliers technologiques que le protocole Bitcoin tout en proposant une innovation structurante : les *Smart Contracts*. L'intérêt de ces contrats est de permettre des cas d'usage de la technologie Blockchain dépassant largement le

simple transfert d'argent : ils ouvrent au développement d'applications et d'usages nouveaux en lien avec la technologie Blockchain. Parmi ces potentialités offertes par le protocole Ethereum se trouvent deux concepts nouveaux et aux potentialités importantes : les DApps *(Decentralized Applications)* et les DAO *(Decentralized Autonomous Organizations)*.

IV.
Les DApps et les DAO, de nouveaux systèmes d'organisation

IV.1 Les DApps, les applications de demain ?

Les DApps (*Decentralized Applications*) sont des applications fonctionnant sur la technologie Blockchain. Pour bien comprendre leurs caractéristiques, il est nécessaire, une fois de plus, de faire le parallèle avec les applications fonctionnant sur la technologie Internet.

Ces dernières sont composées d'une interface utilisateur (ou *frontend*) et de serveurs (ou *backend*) dans lesquels sont stockées les données et informations relatives au bon fonctionnement de l'application.

Dans le cas d'une DApp, la partie *backend* fonctionne sur un réseau décentralisé pair-à-pair permettant l'utilisation de *Smart Contracts*, comme Ethereum. Une DApp présente donc l'ensemble des avantages de la technologie Blockchain (traçabilité, transparence, immuabilité…) tout en proposant une interface utilisateur qui permet à ce dernier d'en avoir une utilisation similaire aux applications que l'on connaît aujourd'hui. En effet, tout l'enjeu d'une technologie, quelle qu'elle soit, réside dans sa capacité à être adoptée par le plus grand nombre. Pour ce faire, il faut qu'elle soit facile d'accès et d'utilisation. À date, la plupart de ces applications n'ont pas encore trouvé leur marché, soit parce que l'interface ne permet pas une expérience client suffisante, soit parce que les infrastructures sous-jacentes ne sont pas encore pleinement stabilisées. L'émergence de projets fonctionnels dans l'industrie du jeu et du pari est toutefois prometteuse.

Aujourd'hui, la plupart des personnes utilisent quotidiennement des applications mobiles sans maîtriser la technologie sous-jacente. Les DApps apportent la promesse de fournir aux utilisateurs des interfaces faciles d'accès tout en s'appuyant sur la puissance de la technologie Blockchain. Les DApps sont à la Blockchain ce que sont les applications (comme Uber par exemple) sont au Web. L'exemple le plus connu de DApps est EtherDelta qui est une plate-forme d'échange de crypto-monnaies décentralisée. Elle propose un fonctionnement entièrement basé sur des *Smart Contracts* permettant l'échange de monnaies compatibles avec Ethereum[91] de manière complètement décentralisée et parfaitement sécurisée.

IV.2 Les DAO, le mode d'organisation de demain ?

Le concept de décentralisation du fonctionnement d'une application peut également s'appliquer avec la décentralisation de la gouvernance d'une entreprise *via* les *Dencentralized Autonomous Organizations* ou DAO.

Une DAO est une entreprise dont les règles de gouvernance sont inscrites sur un *Smart Contract*. Cela permet d'imaginer des entreprises, et, plus largement des modes d'interactions humaines, où les décisions prises sont accessibles par tous partout dans le monde. L'application de ces décisions devient automatique et ne nécessite plus de contrôle puisque la confiance est placée dans le réseau et dans l'automatisation de l'exécution des termes du *Smart Contract*. Ce mode de fonctionnement favorise aussi un processus de décision plus horizontal où chaque membre de la DAO se voit attribuer des droits de vote. Les choix des votes sont directement dans les *Smart Contracts* et permettent de déterminer de manière sécurisée et automatique le résultat de ces votes.

La seule initiative d'envergure à ce jour, nommée « The DAO », a été créée par la start-up slock.it[92]. L'objectif était de créer un fonds de financement, pour des projets de toute nature, reposant sur deux volets :

- les projets sont évalués et soumis à la DAO, s'ensuit une décision prise collectivement entre les détenteurs de jetons de la DAO pour choisir de financer ou non ce projet ;
- les bénéfices ou pertes de chaque projet sont distribués.

91. Les crypto-monnaies compatibles avec Ethereum sont dites ERC20.
92. Il en existe de taille plus « modeste » à date : Aragon, Colony.

Malheureusement, peu de temps après sa levée de fonds (de 150 millions de dollars), la DAO s'est fait attaquer à cause d'une faille dans le code, ce qui a stoppé net son développement. Après cette attaque, les projets lancés par la communauté ont préféré se financer seuls, *via* les ICO *(Initial Coin Offering)*.

V.
Les Blockchains publiques, permissionnées et privées

Dans ce qui précède, nous avons présenté la technologie Blockchain comme registre décentralisé et distribué dans une communauté d'utilisateurs ouverte à tous : toute personne, physique ou morale, peut devenir membre du réseau et consulter l'information contenue dans la Blockchain. Or, il existe une typologie des Blockchains où les droits pour devenir membre du réseau et/ou consulter les informations contenues dans la Blockchain peuvent varier d'un utilisateur à l'autre.

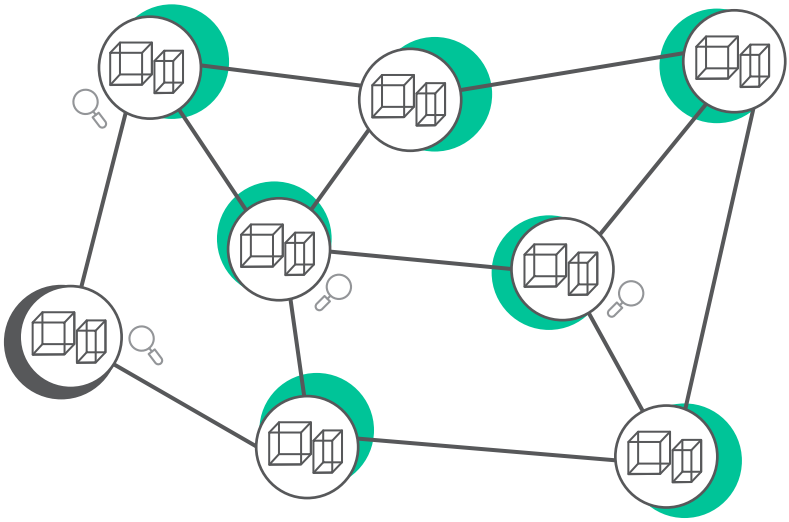
V.1 Les Blockchains publiques

Les Blockchains publiques sont celles que nous avons étudiées jusqu'à présent. Elles se caractérisent par :

- un réseau ouvert à tous sans restriction ;
- une donnée consultable par tous sans restriction ;
- une donnée inscrite dans la Blockchain, qui est indélébile et ne peut être modifiée *a posteriori*.

Les Blockchains publiques pourraient être comparées à une place de marché ouverte à tous : toute personne est autorisée à ouvrir une échoppe pour y vendre ses produits. Aucune restriction n'existe quant aux allées et venues des visiteurs pour regarder les produits disponibles dans les échoppes.

FONCTIONNEMENT D'UNE BLOCKCHAIN PUBLIQUE



Le réseau est ouvert à toute personne, physique ou morale.

L'information est consultable par tous les membres du réseau sans restriction.

Tous les membres du réseau détiennent une copie de la Blockchain et participent au consensus de validation.

V.2 Les Blockchains permissionnées

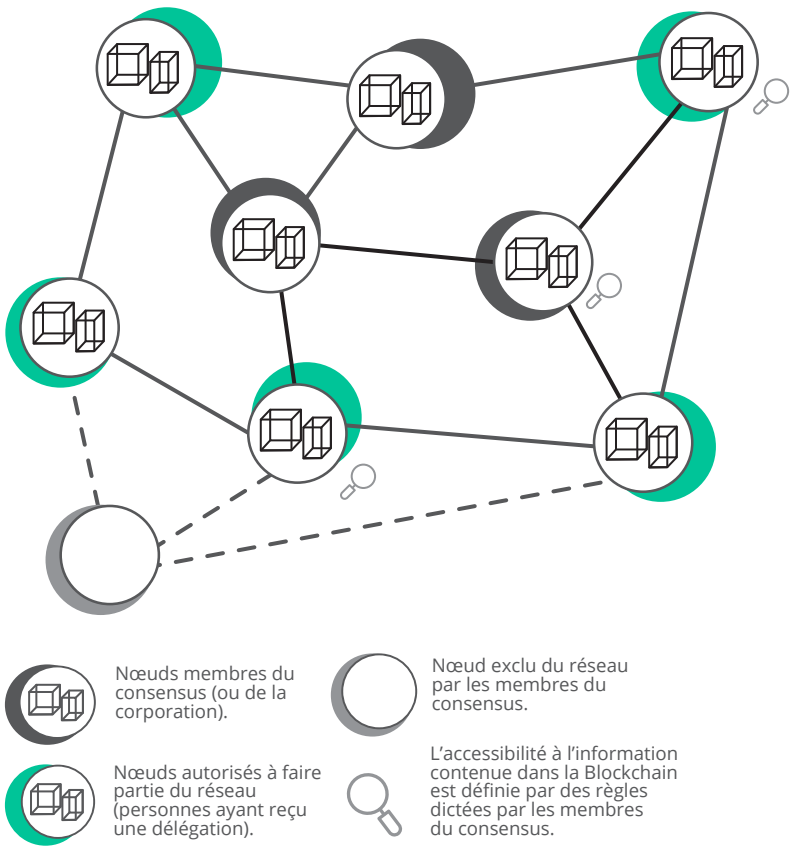
Les Blockchains permissionnées sont partiellement décentralisées et se différencient des Blockchains publiques par un réseau accessible à un nombre limité d'utilisateurs. Les nouveaux entrants doivent être validés par les nœuds, membres du consensus. L'accessibilité de la donnée dépend également des droits d'accès de chaque nœud.

Les Blockchains permissionnées pourraient être comparées à une place de marché corporative : seuls les membres de la corporation sont autorisés à ouvrir une échoppe pour y vendre leurs produits. Cependant, une dérogation peut être accordée par la corporation à certaines personnes pour ouvrir d'autres échoppes. Les allées et venues dans ce marché sont restreintes par les règles définies par la corporation. La recherche menée par le *Japan Exchange Group* pour comprendre et tester les impacts de la technologie Blockchain sur l'infrastructure des marchés

financiers, notamment en ce qui concerne les activités de postmarché, est un bon exemple de déploiement et d'application de Blockchain permissionnée[93].

Avec plus de 12,5 milliards d'euros de capitalisation au 31 décembre 2018[94], la solution Ripple[95] est probablement la Blockchain de ce type la plus connue ; elle propose une sorte de solution Swift (réseau international de communication électronique entre acteurs des marchés), nouvelle génération, dédiée aux banques et institutions.

FONCTIONNEMENT D'UNE BLOCKCHAIN PERMISSIONNÉE

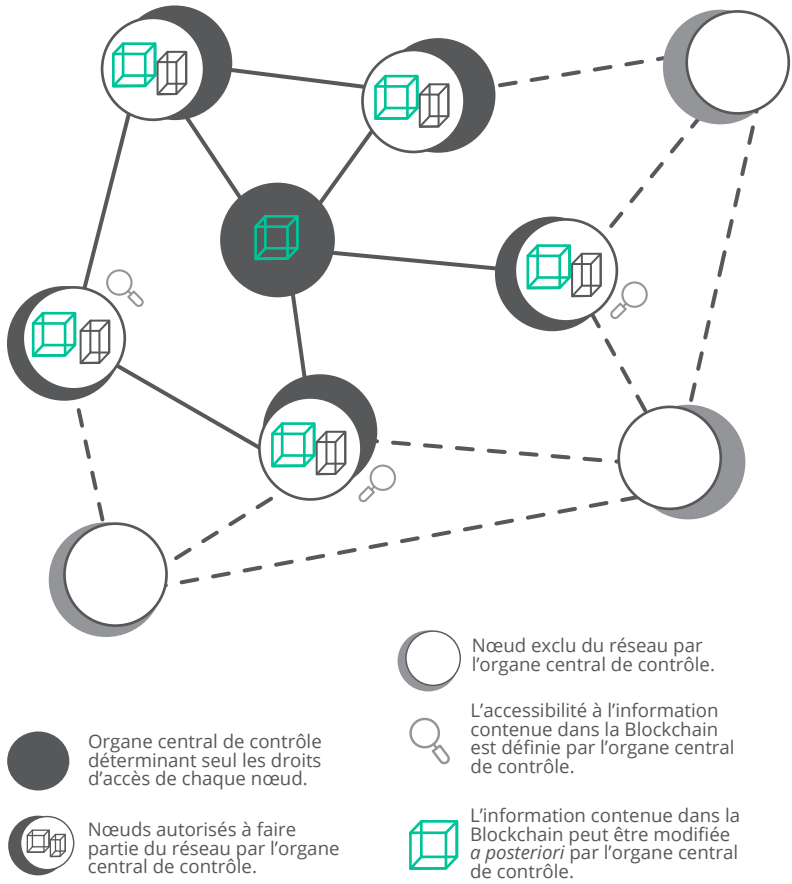


93. Lien : www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_Vol22.pdf
94. Source : coin marketcap. Lien : https://coinmarketcap.com/fr/currencies/ripple/
95. Lien : https://ripple.com/

Notons que la plupart des Blockchains permissionnées et de consortiums fonctionnent selon le système de « *proof of authority* ». Il s'agit d'un algorithme de consensus fondé sur l'identité des nœuds. Les blocs et transactions sont alors validés par certains comptes, dits « validateurs ». Le consensus est critiqué par les puristes puisqu'il demeure fortement centralisé.

V.3 Les Blockchains privées

FONCTIONNEMENT D'UNE BLOCKCHAIN PRIVÉE



Les Blockchains privées sont assimilables à des bases de données distribuées et se différencient des Blockchains publiques :

- le réseau est accessible à un nombre limité d'utilisateurs. Les nouveaux entrants doivent être validés par un organe central décisionnaire ;
- l'accessibilité de la donnée dépend des droits d'accès de chaque nœud, définis par l'organe central décisionnaire ;
- le consensus sur une Blockchain privée repose sur la confiance dans les nœuds validateurs dans leur ensemble.

Les Blockchains privées pourraient être comparées à une place de marché où tous les membres autorisés à ouvrir une échoppe pour y vendre leurs produits font partie de la même entreprise. L'entreprise-mère, ou organe central de contrôle, est la seule à décider qui peut vendre des produits ou faire des allées et venues.

Les Blockchains privées sont assimilables à des bases de données distribuées dans une société. Elles peuvent s'avérer utiles pour partager des données importantes et/ou confidentielles avec les différentes entités du groupe.

En synthèse, si les Blockchains permissives et privées peuvent être utiles pour certains cas d'usage précis, nous sommes convaincus que la « véritable disruption » provient du Bitcoin et des Blockchains publiques, qui reposent sur une philosophie collaborative et distribuée.

V.4 Une synthèse des idées clés

Comprendre le fonctionnement de la technologie Blockchain est un exercice difficile puisqu'elle introduit de nombreux concepts nouveaux qui s'articulent les uns avec les autres. Il est possible d'avoir une compréhension moins technique de la Blockchain, tout en gardant les idées clés de son fonctionnement, en s'autorisant la métaphore suivante : la Blockchain pourrait être comparée à un train circulant à vitesse constante auquel est ajouté un wagon à intervalles de temps réguliers. Dans l'image ci-après, un wagon correspond à un bloc qui est ajouté à la chaîne de blocs (le train). Cet accrochage du wagon se fait en plusieurs étapes :

- La création du wagon (ou création du nouveau bloc) : chaque mineur composant le réseau construit de son côté un wagon vide.

LA BLOCKCHAIN, UN TRAIN CIRCULANT À VITESSE CONSTANTE

1 Création d'un wagon (ou du bloc contenant les transactions)

Chaque mineur du réseau construit un nouveau wagon vide.

2 Stockage des marchandises (ou des transactions)

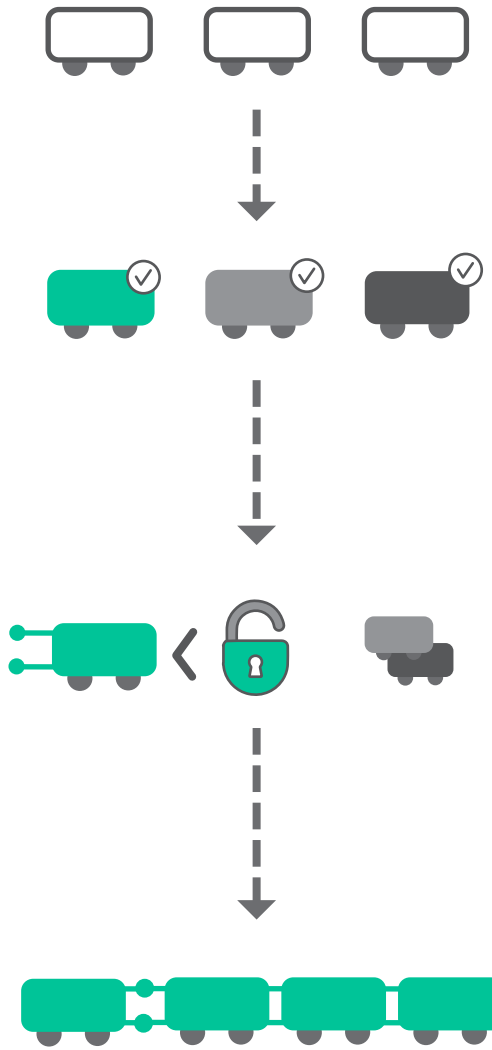
Pour chaque mineur, les marchandises (ou les transactions en cours) y sont stockées après vérification. Dans la Blockchain, la vérification des transactions valides se fait par clé cryptographique.

3 Accrochage du wagon (ou du bloc contenant les transactions)

À chaque intervalle de temps, un wagon doit être créé pour compléter le train. Les mineurs sont en compétition pour accrocher leur propre wagon au train. La compétition réside dans la résolution d'un puzzle cryptographique assurant à la Blockchain une sécurité maximale. Le premier qui résout le puzzle accroche son wagon.

4 La Blockchain contient toutes les informations

Les wagons de ce train sont inamovibles. Une clé cryptographique empêche les wagons fixés au train de se détacher. En passant d'un wagon à l'autre, un passager peut consulter l'ensemble des informations contenues dans la Blockchain.



- Le stockage des marchandises (ou des nouvelles transactions) : pour chaque mineur, une fois le nouveau wagon vide créé, les marchandises y sont stockées à condition de respecter le cahier des charges. Dans la Blockchain, la vérification des transactions valides se fait par clé cryptographique.

- L'accrochage du wagon (ou bloc contenant les nouvelles transactions) : à chaque intervalle de temps, un wagon doit être créé pour compléter le train. Les mineurs sont en compétition pour accrocher leur propre wagon au train. La compétition réside dans la résolution d'un puzzle cryptographique assurant à la Blockchain une sécurité maximale. Le premier qui résout le puzzle accroche son wagon.

- Le train est composé d'un wagon supplémentaire comportant de nouvelles transactions (ou la Blockchain contient un nouveau bloc qui contient les nouvelles transactions effectuées dans l'intervalle de temps) : les wagons de ce train, une fois liés les uns aux autres, sont inamovibles. En effet, une clé cryptographique empêche les wagons fixés au train de se détacher. En passant d'un wagon à l'autre, un passager peut consulter l'ensemble des marchandises stockées dans le train. Dans la Blockchain, en consultant l'ensemble des blocs la composant, un utilisateur peut retracer l'ensemble des transactions la composant.

VI.
Une introduction au *token*

Dans ce qui précède, nous avons centré nos explications sur le fonctionnement de l'infrastructure de la technologie Blockchain. Or, ce dont on entend le plus souvent parler lorsqu'on évoque la technologie Blockchain sont les crypto-monnaies, également appelées *tokens* (« jetons ») ou crypto-actifs. De façon générale, un *token* peut être défini comme une valeur digitale (représentant des droits ou des actifs de toute nature stockés dans un registre), échangeable. Nous nommerons dans les pages suivantes les fameux *tokens* de façon indifférenciée lorsque nous les évoquerons : *tokens*, jetons, crypto-monnaies et crypto-actifs. Mais, puisque les mots ont un sens, nous nous arrêterons sur ces différentes appellations et ce qu'elles représentent d'un point de vue économique et financier (partie F). Nous

avions volontairement laissé de côté cet autre aspect essentiel de la Blockchain jusqu'ici, mais il est à présent impossible de comprendre son fonctionnement sans appréhender le concept de *token*. Ce dernier, en effet, est le média d'échange circulant sur l'infrastructure proposée par la Blockchain. Il est indispensable à son fonctionnement et le reflet de la valeur associée à un protocole ou à la donnée stockée dans le registre. Ainsi, le bitcoin est le *token* permettant d'échanger des valeurs sur le protocole Bitcoin. Pour comprendre le lien entre le bitcoin et le protocole Bitcoin, il faut, encore, user de métaphore.

Le protocole Bitcoin est un système permettant de mettre en place une infrastructure d'échange. Cette infrastructure pourrait être comparée à une autoroute. Le seul moyen d'accéder à cette nouvelle infrastructure autoroutière est de payer un frais de péage, réglable uniquement en bitcoins. Le bitcoin est donc le seul moyen d'avoir un usage du protocole Bitcoin. Dès lors, il n'est pas possible de dissocier le bitcoin de son protocole puisque les deux sont intimement liés : l'un ne peut aller sans l'autre. De plus, le *token* est l'objet qui permet de faire vivre le réseau puisque c'est grâce à lui que peuvent être créés des systèmes de récompenses pour les mineurs mettant à disposition leur puissance de calcul pour faire vivre le réseau.

En conclusion, la technologie Blockchain, sous-jacente au protocole Bitcoin a été pensée pour répondre aux limites d'Internet afin de créer une monnaie digitale et décentralisée. Le défi, pour la création d'une telle monnaie, était de taille puisqu'il fallait une technologie capable d'assurer l'infaillibilité du système, de répondre à la problématique des dépenses doubles et de garantir la confidentialité des utilisateurs. À ces défis technologiques s'ajoutaient les problématiques usuelles des monnaies, notamment en ce qui concerne le contrôle de la création monétaire. Problématique d'autant plus importante pour une monnaie sans organe central de contrôle décidant de la politique à mener. Mais grâce à une combinaison astucieuse de concepts préexistants dans les domaines de la cryptographie (fonction *hash*), de la théorie des jeux *(proof-of-work)* et de l'informatique (réseau pair-à-pair), la technologie Blockchain, *via* le protocole Bitcoin, a réussi à répondre de manière efficace à ces différentes problématiques.

Si la création d'une monnaie digitale et décentralisée était déjà en soi unique dans l'histoire des innovations, le potentiel permis par la technologie Blockchain semble aussi prometteur que celui d'Internet au début des années 2000. En effet, depuis l'apparition du Bitcoin en 2008, un écosystème dense, créatif, et en pleine croissance, s'est déployé en seulement dix ans. De nouveaux concepts (comme les *Smart Contracts*) sont apparus, de nouvelles idées aussi, et le champ d'application de la technologie Blockchain semble s'étendre de jour en jour. De plus,

cette technologie soulève d'autres questions plus fondamentales, comme notre rapport à la confiance, notre rapport à la confidentialité ou un certain nombre de paradigmes économiques que nous pensions acquis (la légitimité de battre monnaie, la nécessité de certains tiers de confiance…).

Cependant, si le bitcoin réussit à résoudre les défis posés par la création d'une monnaie décentralisée et digitale, comment fait-il pour résoudre les défis que pose chaque monnaie, soit la maîtrise de la création monétaire ? De plus, nous l'avons souligné, la présence d'un réseau de nœuds actifs est importante pour faire vivre le réseau. Comment créer un mécanisme d'incitation attractif afin de garantir un réseau de nœuds suffisamment consistant pour que la Blockchain puisse se développer ?

En conclusion de la première partie, nous avions souligné le fait qu'il était difficile de déterminer une valeur économique à une technologie porteuse d'une idéologie forte. L'intérêt de se questionner sur cette idéologie a ainsi permis de faire la part des choses entre la valeur idéologique en tant que telle, non mesurable, et la valeur technique. Cette dernière se mesure quant à elle à l'aune de l'apport technologique de la Blockchain ainsi que dans ses potentialités. Or, contrairement à ce que certains prétendent[96], il est possible de soutenir que cette nouvelle infrastructure, permettant de faire circuler des valeurs par le biais du *token*, a une valeur intrinsèque. La difficulté que pose la question de la valeur technologique de la Blockchain réside dans l'évaluation de la valeur d'une *general purpose technology*, c'est-à-dire d'une technologie dont les usages sont potentiellement infinis et s'appliquent à tous les secteurs. S'interroger sur la valeur économique de la technologie Blockchain reviendrait ainsi à s'interroger sur la valeur économique du protocole ayant rendu possible le développement du Web et donc Internet. Ce type de questionnement trouve rapidement ses limites.

---

96. En novembre 2017, Jean Tirol déclarait : « Le bitcoin n'a aucune valeur intrinsèque ». Lien : https://www.lesechos.fr/30/11/2017/lesechos.fr/030957836512_pour-jean-tirole----le-Bitcoin-n-a-aucune-valeur-intrinseque--.htm

D

BLOCKCHAIN : LA RENCONTRE DE L'ÉCONOMIE ET DE LA TECHNOLOGIE AU SERVICE DU DÉVELOPPEMENT ?

Le Bitcoin, et les autres Blockchains qui l'ont suivi, dépassent la contrainte des dépenses doubles d'Internet et permettent pour la première fois dans l'histoire de réaliser et d'enregistrer de façon complètement décentralisée des transactions (y compris sur des actifs non digitaux), libellées dans une monnaie d'une nouvelle forme, dont la création elle-même échappe aux pouvoirs centralisés. Cette possibilité technique fait appel, pour exister, à des mécanismes économiques utilisés dans ce cadre spécifique. Les initiatives de 2e et 3e générations vont plus loin avec la création de *Smart Contracts*, correspondant à une séquence d'occurrences et de transactions programmées puis exécutées automatiquement avant d'être stockées dans une Blockchain. Quels sont les mécanismes économiques qui sous-tendent le Bitcoin et la Blockchain ? Quels impacts pour la science économique, et le système économique dans lequel nous vivons ?

I.
La Blockchain comme objet d'étude économique

Si elle est neutre dans son exécution, la technologie Blockchain trouve ses racines dans le protocole Bitcoin qui s'appuie sur une communauté initialement chargée idéologiquement. Sa création s'inscrit en effet – en 2008 – dans un contexte de défi aux pouvoirs centralisés sur fond de crise mondiale. Si le Bitcoin s'est démocratisé au-delà de la communauté fondatrice, il repose toujours sur des valeurs profondément libertaires. Plus globalement, l'écosystème Blockchain[97] dans son ensemble est marqué par des valeurs économiques libertariennes fortes, extension du libéralisme philosophique autour de la liberté, de la responsabilité et de la propriété. Socioéconomiquement, la Blockchain pourrait donc n'avoir de valeur que dans la continuité des thèses libérales, posant dès lors un prérequis idéologique et un parti pris forts. Compliqué, donc, à première vue, pour un communiste stalinien ou un colbertiste d'être un admirateur de la Blockchain et de ses promesses.

La liberté d'échanger librement (permise par un système neutre) et d'entreprendre (tout le monde peut devenir mineur de Bitcoin ou

97. Le périmètre « écosystème Blockchain » n'intègre pas ici les acteurs traditionnels.

souscripteur/émetteur d'ICO, sans barrière à l'entrée, à la seule condition de disposer d'une connexion Internet) est au cœur des fondements de la Blockchain. Pour ses défenseurs, « plus libéral » n'est cependant pas nécessairement synonyme de « plus injuste », dans la mesure où elle serait fortement inclusive. Les *whitepapers* des initiatives Blockchains (Bitcoin, Ethereum…) soulignent davantage la capacité d'autorégulation de leur écosystème qu'ils ne font mention de l'intervention de l'État dans l'économie. Ces écrits et les logiques qu'ils décrivent ne sont pas sans rappeler les thèses de l'école autrichienne, portées notamment par Friedrich Hayek puis Pascal Salin, pour ne citer qu'eux, au XXe siècle.

La Blockchain et ses implications peuvent ainsi être étudiées à l'aune des théories économiques, tendant à démontrer si cette dite révolution parvient à repousser les limites de l'équilibre général[98] (« met en lumière la manière dont les marchés et les prix assurent la coordination des activités économiques[99] ») et de l'optimum de Pareto (situation économique dans laquelle il n'est pas possible d'augmenter le bien-être d'un acteur sans réduire celui d'un autre).

Si l'hypothèse que la Blockchain révolutionne à terme la vie économique est une possibilité, qu'elle constitue un nouveau champ d'étude économique est un fait. Qu'on l'appelle *cryptoeconomics* (Pilkington, Zamfir), *cryptoeconomy* (Babbit et Dietz), *token economy* ou *Blockchain economy*, ce nouvel ordre ne remet toutefois pas en cause les fondements de la science économique néoclassique mais, au contraire, les exploite et les combine. Comme l'expliquent Sinclair Davidson, Primavera De Filippi et Jason Potts, l'application formelle et universitaire des thèses microéconomiques à la Blockchain est très récente, puisqu'elle remonte à 2015 avec la définition par Pilkington et Zamfir d'une nouvelle discipline : *cryptoeconomics*[100]. Ce terme est défini par ses créateurs comme « la discipline formelle analysant les protocoles gouvernant la production, la distribution et consommation de biens et services dans une économie digitale décentralisée. La *cryptoeconomics* est une science pratique centrée sur la construction et la caractérisation de ces protocoles. » Cette définition placerait la discipline comme branche du *mechanism design*, lui-même branche de la microéconomie[101]. Babbit et Dietz (2015) définissent à leur tour la *cryptoeconomy* comme « une économie non contrainte sur le plan géographique ni par des institutions politiques et légales, au sein de laquelle la Blockchain gère et conserve les transactions dans un registre public décentralisé, au détriment des tiers de

98. K. J. Arrow, G. Debreu, « Existence of an equilibrium for a competitive economy », *Econometrica: Journal of the Econometric Society*, 1954.
99. Lien : https://www.universalis.fr/encyclopedie/microeconomie-theorie-de-l-equilibre-general/
100. Sinclair Davidson, Primavera de Filippi, Jason Potts, *Economics of Blockchain*, 2016.
101. *Idem*.

confiance[102]. » Si ces réflexions « *cryptoeconomics* » concernent essentiellement la microéconomie, nous compléterons notre approche d'une analyse macroéconomique, vue sous l'angle de l'impact de la Blockchain sur l'économie dans son ensemble.

II.
Microéconomie et *cryptoeconomics*

II.1 Le cadre néoclassique

Le cadre d'analyse proposé s'inscrit dans un cadre néoclassique : les huit premiers des dix principes de l'économie[103], décrits par Gregory Mankiw (les deux derniers faisant référence à des notions économiques étatiques) sont pris comme des hypothèses. Selon Mankiw, « les gens doivent faire des choix, le coût d'un bien est ce à quoi on est prêt à renoncer pour l'obtenir, les gens rationnels pensent en termes marginaux, les gens réagissent aux incitations, l'échange enrichit tout le monde (à la fois partenaires et concurrents) et le gouvernement peut parfois améliorer les résultats du marché (efficacité et justice pour compenser les défaillances de marché). » L'hypothèse économique la plus fondamentale concerne l'efficacité supposée du marché : « En général, les marchés constituent une façon efficace d'organiser l'activité économique. » Les prix sont un mécanisme issu de forces d'offre et de demande qui s'équilibrent, favorisant l'émergence de résultats favorables, selon la thèse d'Adam Smith (« main invisible »). L'information est reflétée dans un marché par les prix, qui permettent de guider les acteurs dans l'allocation des ressources rares et ainsi de coordonner implicitement les activités de centaines de milliers d'acteurs aux goûts et dons différents. En économie, les marchés produisent la quantité de biens qui optimise les surplus du consommateur et du producteur. La demande reflète la valeur accordée par le consommateur au produit et l'offre reflète les coûts de production du producteur.

Dans les théories néoclassiques de Walras et Pareto, ce sont les prix qui informent les demandeurs potentiels sur la qualité, quantité des biens

102. Dave Babbitt, Joel Dietz, « Cryptoeconomic design: a proposed agent-based modelling effort », SwarmFest 2014.
103. Gregory Mankiw, *Principes de l'économie*, Economica, 1998.

et services disponibles. Ils informent l'offre de l'ampleur de la demande pouvant exister pour leurs biens ou services. Les souhaits d'achat et de vente varient donc en fonction des prix proposés[104]. Ces théories ne sont valables qu'en situation de concurrence pure et parfaite, atteinte sous quatre conditions : atomicité du marché (tous les agents sont des preneurs de prix, ils sont trop nombreux pour pouvoir influencer le prix individuellement), produits homogènes (niveau de qualité dont la différence ne conduit pas à segmenter le marché), libre entrée et sortie (absence de barrière à l'entrée ou la sortie), mobilité parfaite des facteurs, information parfaite (absence d'asymétrie d'information). On pourrait ajouter à ces quatre hypothèses une conséquence directe induite : des coûts de transaction nuls puisqu'il n'y a plus besoin de lever l'asymétrie d'information. Plus tard, le concept de concurrence pure et parfaite a été « adouci » par d'autres économistes comme Knight et Baumol, dans les années 1920, avec l'émergence de la théorie des marchés contestables. Selon eux, seul le critère d'absence de barrière à l'entrée sur le marché est clé[105].

Le concept de concurrence pure et parfaite n'est pas directement observable empiriquement, mais constitue néanmoins un cadre d'analyse fondamental de l'analyse économique et des marchés. Sous le postulat néoclassique que l'équilibre de marché maximise le bien-être de l'économie, la concurrence pure et parfaite est un facteur d'optimisation du marché (transparence, liberté d'entreprendre et circulation de l'information).

Alors en quoi la Blockchain pourrait-elle constituer un facteur de rapprochement du marché de la concurrence pure et parfaite ? La Blockchain pourrait résoudre des problèmes d'asymétrie d'information et réduire les barrières à l'entrée sur certains marchés.

II.1.a La Blockchain réduit les asymétries d'information

Introduite par le prix Nobel Kenneth Arrow en 1963, avec l'exemple de l'assurance santé, l'asymétrie d'information correspond à une distribution non homogène de l'information entre des agents économiques. Autrement dit, l'information n'est pas publique et partagée par tous. Cet état induit deux conséquences en termes de fonctionnement économique : l'aléa moral, consistant à faire évoluer négativement son comportement une fois une transaction effectuée (par exemple ne pas rembourser un crédit volontairement après son octroi) et l'antisélection, lorsque l'information cachée/non révélée impacte les échanges de commerce. L'économiste Georg Akerlof a brillamment théorisé l'antisélection en démontrant

104. Alain Bienaymé pour l'*Encyclopedia Universalis* en ligne.
105. W. J. Baumol, « Contestable Markets: an Uprising in the Theory of Industry Structure », *American Economic Review*, vol. 72, n° 1, 1982.

qu'elle peut aller jusqu'à supprimer l'existence même du marché. Dans son article, « *Market of lemons* » – pour lequel il obtient le prix Nobel d'économie en 2001 –, Akerlof prend l'exemple d'un marché de voitures d'occasion composé de véhicules pour moitié de bonne qualité (valeur de 15 000 euros), pour moitié de mauvaise qualité (valeur de 5 000 euros). Seuls les vendeurs savent à quel groupe appartient leur voiture. Les acheteurs sont au fait de la distribution de la qualité dans la population de véhicules à vendre mais incapables d'identifier séparément les véhicules de bonne ou de mauvaise qualité. Contrairement à la première intuition, le prix ne tend jamais vers la moyenne *i. e.* 10 000 euros puisqu'à ce prix les vendeurs des bons véhicules perdent 5 000 euros et les retirent par conséquent du marché. Ne restent que les voitures en mauvais état, délaissées par les acheteurs. Le mécanisme d'antisélection décourage dans ce cas les transactions, allant jusqu'à la suppression du marché.

L'existence d'un « signal » (Spence, 1973[106]) permet de limiter l'antisélection et l'asymétrie d'information. L'auteur applique à l'époque la problématique d'asymétrie d'information à l'éducation en indiquant que l'employeur va chercher à maximiser son investissement en observant des signaux lui permettant d'anticiper la productivité du collaborateur (le CV ou le diplôme par exemple, tout en mettant en exergue à l'époque le risque de falsification). Dans le cas du marché automobile secondaire, les certificats d'immatriculation, le contrôle technique permettent de la même façon de limiter l'asymétrie d'information entre le vendeur et l'acheteur, réduisant le risque de ce dernier. L'effet sur la formation des prix est immédiat, puisque – *ceteris paribus* – l'acheteur sera prêt à payer plus cher un véhicule ayant passé le contrôle technique que celui ayant échoué.

Au global, si l'on s'en tient au cas extrême d'Akerlof, l'économie non « blockchainisée » semble plutôt bien maîtriser l'asymétrie d'information et l'antisélection puisque, factuellement, les marchés d'échange sont nombreux, des crédits et contrats d'assurance sont émis, alors même que les contreparties pourraient être tentées de ne pas respecter volontairement leurs engagements.

Mais à y regarder de plus près, notre système ne fonctionne pas de manière optimale au sens des économistes néoclassiques : il intègre des coûts importants pour corriger imparfaitement une asymétrie d'information bien réelle (pourtant supposée négligeable dans la théorie des marchés optimaux). En effet, les nombreux signaux émis doivent être suffisamment forts, avoir une intensité suffisante pour guider les acteurs dans leurs choix rationnels d'allocation de ressources et permettre une formation des prix reflétant le maximum d'information. Pour être forts,

106. M. Spence, « Job Market Signaling », *Quarterly Journal of Economics*, 1973.

ces signaux doivent être émis par une forme d'autorité reconnue largement, qu'elle soit publique ou privée. Dans ce dernier cas, elle requiert une réputation assise, et coûteuse au sens économique puisqu'elle suppose généralement une taille importante. Dans le premier cas, l'autorité publique a un coût, plus indirect, lié au risque de manipulation du signal et donc de corruption. La maîtrise de l'asymétrie d'information et des signaux la réduisant est, de manière générale, une fois de plus à la main de tiers de confiance, en qui les acteurs ont été contraints de déléguer la confiance qu'ils portèrent jadis directement à leur contrepartie bien connue car géographiquement proche.

Les banques et les assurances ont typiquement fait de ce rôle leur cœur de métier. Schématiquement, leur fonction consiste à prendre des risques rémunérés et mutualisés, les risques assurantiels et de crédit comportant une large part d'aléa moral potentiel (non-remboursement volontaire de crédit, fausses déclarations de sinistre…). Elles ont développé des capacités internes leur permettant de bénéficier d'une information plus précise sur certains acteurs et d'orienter leur comportement, dans un cadre donné. Le développement de systèmes de notation basés sur des informations données par le client (signal forcé) et permettant ou non l'octroi d'un crédit, à des taux différenciés, en est un bon exemple. La prise de collatéral est de la même façon un moyen de discriminer mécaniquement deux populations – bon payeur et mauvais payeur – et de minimiser le risque d'aléa moral (Bester 1987[107]). Selon ces thèses – schématiquement – les mauvais payeurs ne prendront pas le risque de perdre leur maison. Les exemples sont nombreux au-delà de la bancassurance : contrôle technique, vérification du bureau Veritas, normes ISO…

Même dans la nouvelle économie, les échanges dits pair-à-pair – de biens physiques ou services – se font par le biais d'un intermédiaire : le site d'achat Leboncoin garantit l'existence d'un jeu répété et limite le nombre de fraudes (vendeur banni en cas de fraude, en ligne avec la théorie d'Abreu sur la coopération en cas de sanction) ; Uber sélectionne ses chauffeurs et propose un système de notation ; Particulier à particulier (PAP) impose un minimum de renseignements nécessaires pour forcer l'émergence de l'information.

La complexification des échanges, liée à une spécialisation croissante, ne permet plus la gestion *intuitu personæ* des asymétries d'information et nécessite donc l'industrialisation d'un système de signaux délégué à des tiers, par définition coûteux.

---

107. Bester, « The role of collateral in credit markets with imperfect information », *European Economic Review*, vol. 31, 1987. Lien : www.sciencedirect.com/science/article/pii/0014-2921(87)90005-5

C'est précisément ici que la Blockchain a un rôle central à jouer. Au sens de la théorie microéconomique, elle pourrait en effet réduire le coût d'émergence et de découverte de l'information, et accroître de manière générale la transparence du marché. La réduction de ce coût se traduirait par un rééquilibrage du mécanisme de formation des prix, structurant dans la répartition de la valeur. Outil technologique de la transparence, la Blockchain peut en effet apporter une traçabilité absolue, permettant de générer une information – presque – parfaitement neutre.

Reprenons le cas des *lemons* d'Akerlof. Si l'ensemble des informations relatives au véhicule était enregistré dans une Blockchain publique, immuable et infalsifiable, le coût de découverte de la qualité intrinsèque du véhicule deviendrait quasi nul. L'acheteur pourrait proposer une offre, en toute connaissance de cause. Pour reprendre la thèse de Spence sur l'éducation et la théorie du signal, plusieurs projets dont le Français BCD diploma, offrent des services d'enregistrement sur la Blockchain des diplômes. De la même manière, les biens de luxe souffrent de la contrefaçon qui pourrait, en théorie et sans moyen de détection opérant (coûteux), conduire à une version *bis* du marché des *lemons*. Là encore, autoriser le consommateur à discriminer de manière certaine et rapide, seul, le bon grain de l'ivraie, réduit drastiquement l'asymétrie d'information (la Blockchain représentant le seul signal absolu). Les cas sont nombreux et se multiplient. Le diamantaire De Beers travaille, par exemple, à la création d'un registre sécurisé recensant l'ensemble des diamants, et leurs parcours. « Imaginez un monde où le parcours unique d'un diamant, depuis ses débuts – un don de la nature sous sa forme brute – jusqu'à son achat ultime comme symbole des moments les plus importants de la vie, puisse être capturé d'une façon aussi éternelle que le diamant lui-même », rêve déjà son CEO, Bruce Cleaver[108].

Autre exemple : Carrefour vient de communiquer sur la mise en place d'une solution Blockchain pour assurer au client une transparence quasi parfaite des denrées alimentaires au long de la *supply chain*.

Derrière ces exemples concrets, se cache la possibilité de rebattre la distribution de l'information et par déduction du mécanisme de formation des prix. C'est une grande partie de la valeur cumulée de l'économie qui pourrait être réallouée. Le consommateur accéderait *in fine* à une information de meilleure qualité, et moins chère.

Cela ne signifie pas que la Blockchain sera une sorte de grand livre parfaitement transparent pour tout le monde, sur lequel il ne serait plus possible de protéger des données personnelles, des secrets industriels

108. Lien : www.rubel-menasche.com/fr/industrie/entreprises/de-beers-tire-parti-de-blockchain-pour-le-suivi-des-diamants

ou tout autre type d'informations dont la circulation doit se faire au sein d'un groupe limité d'intervenants. Seuls les éléments relatifs aux clés publiques sont effectivement consultables. Plus globalement, la Blockchain constitue un outil optimisé d'articulation des informations entre plusieurs parties. Le *Zero knowledge* (ZK) *proof* (preuve à divulgation nulle de connaissance), classiquement utilisé en cryptographie, en est une illustration ; il permet à un acteur de démontrer à un autre qu'il détient une information, sans la produire. Par exemple, Alice peut prouver à Bob qu'elle a découvert l'emplacement de Charlie dans un jeu « Où est Charlie ? », mais sans trahir la position de ce dernier.

II.1.b La Blockchain réduit les barrières à l'entrée

La Blockchain peut permettre la réduction des barrières à l'entrée.

a. La réputation est l'un des premiers facteurs constitutifs de barrière à l'entrée. En effet, les relations commerciales reposent sur la confiance, et donc sur la répétition historique des échanges, permettant à l'acteur d'acquérir une légitimité et un capital-confiance. Avec la Blockchain, on peut imaginer que la technologie réduira drastiquement l'asymétrie d'information, dès la première interaction, du fait que la confiance entre les deux acteurs ne sera plus nécessaire, déléguée au code.

b. Les acteurs ont désormais accès à des infrastructures à moindre coût, du fait de la logique *open source* de nombreuses initiatives. Un entrepreneur peut par exemple choisir d'intégrer le protocole Bitcoin dans sa chaîne de valeurs pour réaliser des transferts d'argent, sans avoir à payer un droit d'accès (autre que celui du coût de la transaction).

c. Les ICO constituent un moyen d'accéder massivement aux capitaux pour concurrencer un acteur établi, voire remettre en cause un monopole.

d. La Blockchain peut permettre de réduire les coûts de lancement de certaines activités, constituant une barrière majeure à l'entrée. À titre d'exemple (nous reviendrons sur le marché des transferts d'argent), le principal coût de lancement d'une activité de transfert d'argent est la constitution d'une réserve de devises d'un côté et de l'autre du « corridor » créé (dans deux pays), pour permettre la compensation en devises des montants transférés et éviter de transférer effectivement les sommes. Avec le Bitcoin, la vitesse de transaction permet de réaliser la transaction dans les faits, et donc d'éviter les coûts de constitution de cette réserve.

II.2 Optimum de Pareto, optimum social et théorie des jeux

II.2.a Théorie des jeux et Blockchain

« La théorie des jeux se définit généralement comme l'outil mathématique permettant d'analyser les interactions stratégiques entre les individus, en particulier lorsque ces derniers ont des intérêts divergents. Elle s'intéresse à toutes les configurations dans lesquelles la situation de chacun dépend du comportement de tous et constitue donc la théorie mathématique des comportements stratégiques », selon l'économiste Nicolas Eber[109].

Le marché permet, d'après les thèses néoclassiques, d'atteindre une forme d'optimum, soit une situation dans laquelle il n'y a pas d'alternative qui permettrait à un acteur individuel de maximiser davantage son utilité (optimum de Pareto). L'apport de la théorie des jeux consiste à mettre en lumière que, dans certains cas, il est impossible de concilier optimum de Pareto et optimum social. En d'autres termes, la poursuite par les individus de choix rationnels individuels pourrait conduire à une situation collective moins favorable que si les agents s'étaient coordonnés. Le cas le plus connu est celui du dilemme du prisonnier d'Alfred Tucker. Deux prisonniers, Bonnie and Clyde, sont arrêtés par la police et sont interrogés séparément. Si Bonnie dénonce Clyde et que ce dernier se tait, Bonnie est libre et Clyde est condamné à cinq ans de prison ; et vice-versa. Si les deux se dénoncent mutuellement, ils écopent de trois ans de prison chacun ; si les deux se taisent, ils écopent d'un an de prison chacun.

SYNTHÈSE DU DILEMME DU PRISONNIER (SELON LA THÉORIE DES JEUX)

		CLYDE	
		Dénonce (D)	Se Tait (ST)
BONNIE	Dénonce (D)	3 ans de prison chacun	Bonnie : libérée Clyde : 5 ans
	Se Tait (ST)	Bonnie : 5 ans Clyde : libéré	1 an de prison chacun

109. Nicolas Eber, *Théorie des jeux*, Dunod, 2013, 3e éd.

L'optimum social (du point de vue des deux suspects) serait bien sûr de se taire tous les deux pour minimiser globalement le nombre d'années d'emprisonnement. En revanche, la rationalité individuelle pousse les deux individus à dénoncer (stratégie dominante dans le langage des économistes de la théorie des jeux) ; que Clyde la dénonce ou non, Bonnie ne regrettera jamais de l'avoir trahi. Dans ce cas, l'équilibre de Nash, la situation dans laquelle aucun joueur ne regrette le choix qu'il a opéré, compte tenu du choix de son adversaire, ne constitue pas l'optimum social, à savoir la meilleure option collective pour les individus.

Dans la continuité de ces travaux, d'autres auteurs ont démontré l'existence d'une coopération lors de la répétition du dilemme du prisonnier sans communication entre les participants (Luce et Raiffa 1957) mis en exergue le rôle de la sanction dans l'émergence de la coopération (Abreu) ou souligné la réciprocité dans les relations (stratégie *Tit-for-Tat* théorisée par Axelrod[110]). Globalement, le difficile alignement entre intérêts personnels et collectifs, est au cœur de nombreux enjeux actuels ou historiques, qu'ils soient sportifs (cas du dopage), économiques (situation oligopolistique), philosophiques, géopolitiques (guerre froide) ou stratégiques. Certains auteurs considèrent d'ailleurs que c'est pour faire face à ce type de problématique que les normes sociales, institutions et lois ont été mises en place[111].

« La Blockchain permettrait d'échapper au dilemme du prisonnier sans nécessité de consolidation, de coûts élevés de coordination et de complexité additionnelle », selon Ildar Fazulyanov, fondateur de la start-up Well, dans un article dédié à l'analyse de l'équilibre de Nash[112] et de la Blockchain dans le secteur de la santé[113]. Certains écosystèmes Blockchain permettraient donc, de manière décentralisée et presque parfaitement autorégulée, de réconcilier systématiquement les optimums de Pareto et équilibres de Nash. Dit autrement, la Blockchain servirait l'émergence de l'optimum social, résultante des choix rationnels privés.

II.2.b *Mechanism design* et Blockchain

Revenons à la définition de la *cryptoeconomics* comme branche de la discipline du *mechanism design*, ramification de la théorie des jeux, elle-même ramification de la microéconomie.

---

110. Axelrod, *The American Political Science Review*, American Political Science Association, 1981.
111. Nicolas Eber, *Théorie des jeux*, Dunod, 2013, 3e éd.
112. Situation dans laquelle aucun joueur ne regrette son choix, au vu du choix des autres participants.
113. Article d'Ildar Fazulyanov (créateur de la start-up Well, plate-forme globale pour des soins de qualité), septembre 2017. Lien : https://medium.com/@ildarfazulyanov/Blockchain-and-nash-equilibrium-in-healthcare-oh-my-1-6ba0e80ea03b.

Qu'est-ce que le *mechanism design* ? Le *mechanism design* vise à répondre à la difficulté de trouver des mécanismes permettant simultanément d'obtenir des décisions collectivement optimales et de maximiser la situation d'acteurs individuels agissant librement au gré d'incitations[114]. En d'autres termes, il s'agit d'exploiter la matrice de la théorie des jeux dans une situation donnée en partant du résultat final souhaité (quelle situation finale est préférée). Analytiquement, des gains (*payoffs*) sont déduits pour garantir que l'équilibre de Nash ne puisse être que l'optimum social. Le mécanisme d'incentive permet d'obtenir la distribution de *payoffs* nécessaire.

Prenons l'exemple le plus connu : l'enchère de Vickrey, dite au second prix, mécanisme utilisé dans les adjudications des commissaires-priseurs (eBay utilise un système proche). Tous les participants doivent inscrire sur une feuille le prix qu'ils seraient prêts à payer pour l'acquisition d'un bien considéré. Après dépouillement, une première option est d'attribuer l'enchère au joueur ayant offert le prix le plus élevé, proposé sur sa feuille. Ce mode de fonctionnement n'incite pas à faire dévoiler par l'acheteur sa réelle perception du prix, puisqu'il va chercher à anticiper le prix qu'indiqueront ses concurrents. Vickrey propose une enchère au second prix : le candidat ayant fait l'offre la plus élevée remporte toujours la propriété du bien, mais paye le montant indiqué par la seconde offre. Ce changement – infime de prime abord – change drastiquement l'incitation de l'acheteur qui n'a plus besoin d'anticiper le prix que mettront ses adversaires. S'il indique son prix de réservation (par exemple 100) et que le second indique 90, il obtiendra une utilité de 10. Si, dans le cas contraire, un autre joueur a proposé plus que 100, il ne regrette pas car le prix proposé reviendrait pour lui à « acheter à perte » (prix de vente supérieur à son prix de réservation). La structure du jeu conduit les acteurs à « dire les vérités » et proposer leur « juste » prix ; l'équilibre créé est optimal collectivement.

La plupart des écosystèmes Blockchain reposent très largement sur ce type de mécanisme d'incitation, permettant de maximiser l'alignement d'intérêts.

Là encore, le moyen le plus efficace pour maximiser la compréhension est de remonter à l'épicentre : le Bitcoin. Satoshi Nakamoto n'a pas seulement compris la théorie des jeux, mais l'exploite brillamment pour garantir la soutenabilité de son système autorégulé.

---

114. Mathew O. Jackson, *Mechanism Theory*, 2014. Lien : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2542983

II.2.c Le système Bitcoin : code, *mechanism design*, incitations et usages

L'*economics* du Bitcoin

Le Bitcoin est souvent vu comme un outil purement technologique de transfert mécanique de valeurs de pair-à-pair, un peu comme la puce d'une carte bleue permet techniquement le paiement sur un terminal. Le Bitcoin revêt en réalité une dimension plus complexe que cela : il parvient à naturellement coordonner les actions de milliers d'individus inconnus et ne partageant rien ou peu, de façon totalement autorégulée et décentralisée.

Inutile de revenir ici sur le mécanisme technique complet d'exécution et d'enregistrement des transactions, déjà largement développé précédemment. Pour rappel et en synthèse, lorsqu'Alice souhaite envoyer un bitcoin à Bob, l'information de sa transaction est envoyée à l'ensemble des nœuds du réseau qui prévalident la transaction. Après réception d'un nombre suffisant de transactions permettant de constituer un « bloc », seul un nœud (sélectionné pseudo-aléatoirement parmi l'ensemble) est autorisé à accrocher son bloc au bloc précédent (ce que l'on appelle le minage) par la réalisation d'un challenge mathématique cryptographique, validant ainsi définitivement la réalisation et l'enregistrement de la transaction d'Alice vers Bob. Quelle que soit la puissance des algorithmes mis en place, le protocole repose sur la puissance de calcul mise à disposition par les mineurs – qui ne sont en réalité que des individus derrière un ou des ordinateurs. L'analyse la plus aboutie des seules techniques informatiques et cryptographiques/mathématiques ne permettrait pas de comprendre l'essentiel : pourquoi les mineurs minent-ils ? Pourquoi un individu rationnel investirait-il du temps, du matériel et de l'électricité dans la mise à disposition de puissance de calcul pour valider la transaction au bout du monde de deux individus qu'il ne connaît pas ?

Plus globalement, rappelons-nous que le *mechanism design* consiste à créer un système basé sur l'incitation dans lequel le comportement d'agent rationnel ne peut mener qu'au résultat collectif escompté par le créateur du jeu.

Qu'a voulu faire Satoshi Nakamoto, créateur du jeu Bitcoin, avec son système *proof-of-work* ? Quels mécanismes économiques a-t-il mis en place pour créer un système de transfert de valeur de pair-à-pair, sécurisé, autorégulé et décentralisé ? Il n'est pas possible d'interroger Satoshi Nakamoto sur sa création. Notre approche – fidèle au *mechanism design* –

consiste à analyser son *whitepaper*[115] et interpréter les caractéristiques techniques connues du Bitcoin comme des moyens d'arriver au résultat pensé par Satoshi Nakamoto.

En reprenant la première phrase du *whitepaper*, on pourrait résumer l'objectif général du Bitcoin par la séquence suivante : créer une monnaie digitale pair-à-pair, sécurisée, décentralisée, neutre et désarrimée des pouvoirs centralisés[116]. Par conséquent, et en déduction des caractéristiques techniques connues, nous interprétons quatre objectifs-clés : garantir le lien absolu entre individu et propriété de bitcoins dans un cadre semi-confidentiel, permettre aux transactions d'exister sans intervention centralisée, rendre la chaîne inviolable et généraliser *in fine* l'utilisation du bitcoin *via* une demande soutenue (dont la nature et l'ampleur peuvent elles-mêmes être questionnées).

a. Garantir le lien absolu entre individu et propriété de bitcoins dans un cadre semi-confidentiel : le détenteur de bitcoins possède une clé privée (son identifiant personnel) et une clé publique (son identifiant sur le marché). Le détenteur est le seul à connaître le lien entre sa clé personnelle et sa clé publique.

b. Permettre aux transactions d'exister : cette affirmation peut à première vue paraître absurde mais si aucun mineur ne se connecte au réseau, aucune transaction ne peut avoir lieu. Il n'existe pas d'entreprise, pas de chiffre d'affaires, pas de salariés ni de hiérarchie permettant d'obtenir l'*output* d'une tâche en échange d'une rémunération. Il faut donc de façon autorégulée conduire des agents qui ne se connaissent pas à coopérer naturellement, par la seule poursuite de leurs intérêts rationnels individuels. Le bitcoin, unité de compte du protocole Bitcoin, constitue un moyen de les inciter à miner. En effet, à chaque bloc validé, le mineur reçoit à la fois une *transaction fee* (payée par l'utilisateur) et une quantité de bitcoins appelée *minting* créée par le protocole. Le mineur mine si l'espérance de gain est supérieure au coût d'extraction de ce gain. Il s'agit d'une forme de mécanisme automatique, régulé et figé, de création monétaire. La quantité de bitcoins rémunérant la création du bloc étant fixée dès le départ (divisée par deux tous les quatre ans) tout comme le rythme d'allongement de la chaîne (un bloc ajouté toutes les dix minutes), la trajectoire d'offre de l'unité bitcoin est donc connue depuis la mise en place du protocole (capée à 21 millions). Le bitcoin est donc intrinsèquement déflationniste, c'est-à-dire que sa valeur augmente mécaniquement à mesure

115. Un *whitepaper* correspond à la présentation d'un projet Blockchain, rédigée par les fondateurs et accessible en ligne par tous.

116. « Une vision purement pair-à-pair de la monnaie électronique autoriserait les paiements en ligne à être envoyés directement d'une personne à l'autre sans avoir à passer par une institution financière. » *in* Satoshi Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*, 2008.

que son usage croît (pour rappel, l'augmentation de la masse de monnaie en circulation entraîne à l'inverse une dévaluation de sa valeur et se traduit par une inflation).

c. Rendre la chaîne inviolable pour faire du Bitcoin le moyen de transfert et d'enregistrement le plus sûr au monde (facteur différenciant par rapport aux systèmes de transfert de valeurs traditionnels centralisés). D'un point de vue technique, une transaction n'existe que si elle appartient à un bloc, lui-même accroché au précédent (en d'autres termes, elle n'existe que si elle appartient à la chaîne de blocs, partagée entre tous les nœuds du réseau). Le mécanisme du minage ne sert pas à vérifier la transaction (point très léger techniquement, puisqu'il s'agit simplement de déchiffrer la clé publique/privée de l'émetteur et de s'assurer qu'il dispose bien des fonds), mais à créer dans le temps une résilience aux attaques. La chaîne étant intégralement partagée entre tous les membres du réseau, il faudrait créer des blocs plus rapidement que les autres mineurs pour frauder (nécessitant une puissance de calcul énorme). De plus, plus la chaîne s'allonge, plus la fraude d'anciens blocs inscrits devient difficile, puisqu'il faudrait recréer une chaîne quasi entière pour frauder (ce qui est à ce stade techniquement impossible).

La validation d'un bloc doit donc avoir un certain coût car sinon, toute personne mal intentionnée pourrait recréer la totalité des blocs en les rendant frauduleux. Le point fondamental pour comprendre le Bitcoin et la Blockchain est le suivant : le coût de validation d'une transaction en bitcoins est donc totalement artificiel et créé de toutes pièces par le code du protocole. Le nombre de transactions à la minute est capé par le rythme figé d'ajout des blocs à l'arrière de la Blockchain (à l'image de wagons à l'arrière d'un train). Contrairement aux idées reçues, le minage – consommateur d'électricité – ne sert pas à rien puisque la sécurité du protocole repose intégralement sur lui, et justement sur son coût[117]. Si tant est qu'elle soit possible, toute décision de *hacking* ou de prise de contrôle du consensus (par une puissance de calcul de plus de 51 % sur le réseau) est finalement rendue absurde par le système, puisque les acteurs ont davantage intérêt à coopérer qu'à engager à perte des sommes colossales pour fragiliser un système constituant leur propre fortune.

Des projets sont toutefois en cours pour trouver des externalités positives à la résolution de ces challenges cryptographiques (par exemple : découverte de nouveaux nombres premiers). Ces

117. Yonathan Sompolinsky, Aviv Zohar, *Bitcoin's underlying incentives*, vol. 15, issue 5 acm queue, Association for computing machinery, 2017. Lien : https://queue.acm.org/detail.cfm?id=3168362.

externalités doivent cependant rester non directement monétisables car, dans le cas contraire, elles réduiraient le coût marginal du minage et remettraient en question l'équilibre[118]. S'il ne crée pas pour l'instant d'externalités positives, ce mécanisme de minage génère en revanche une externalité négative : la consommation d'électricité constituant un des principaux facteurs polémiques. La résolution du problème cryptographique dans un contexte de compétition, certes nécessaire à la sécurité du réseau, nécessite la mise à disposition d'une puissance de calcul massive et croissante à mesure que la demande augmente. En 2017, le protocole Bitcoin aurait consommé plus de 30 TWh, une consommation qui représente 6,74 % de la consommation électrique française ou 41 % de la consommation autrichienne. Digicomist estime que la consommation par transaction Bitcoin est 56 fois supérieure à celle de Visa (sans corriger la fréquence de transaction supérieure pour Visa[119]). Pour autant, s'ils sont très impressionnants présentés sous cette forme, ces calculs de coin de table sont difficiles à rationaliser ; le Bitcoin devrait davantage être comparé au système monétaire mondial qu'à Visa.

d. Généraliser l'utilisation du bitcoin : permettre l'existence d'une demande. Le système a été conçu pour optimiser la sécurité qui est une fonction croissante du nombre d'utilisateurs et de la demande, générant un effet de réseau vertueux dit loi de Metcalfe (loi caractérisant l'effet de réseau, argumentant que plus un réseau a d'utilisateurs, plus il a de la valeur). En effet, plus la chaîne de blocs est longue (à mesure que le nombre de transactions s'accumule dans le temps), moins sa falsification devient probable, plus sa valeur d'utilité augmente aux yeux du consommateur. Au-delà de la sécurité, ce dernier s'intéresse également à la vitesse et au coût de la transaction. À ce jour, la vitesse et le coût d'une transaction en bitcoins ne peuvent pas permettre des transactions quotidiennes de faible montant (temps de validation de 10 minutes, coût unitaire de transfert fixe allant jusqu'à 30 euros).

Y a-t-il par conséquent un « problème » de scalabilité du bitcoin comme beaucoup le prétendent ? Non, il n'y a pas de problème en soi, le fonctionnement actuel a été fabriqué par Satoshi Nakamoto et la règle des 10 minutes (en moyenne) n'a rien à voir avec une limite technique, puisqu'il l'a arbitrairement créée pour assurer l'inviolabilité du réseau. Possible qu'il y ait en revanche une incompatibilité entre un usage que certains voudraient prêter au Bitcoin et le code originel.

---

118. Birfury Group, « Proof-of-stake versus proof-of-work », *Whitepaper*, 13 septembre 2015. Lien : bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf

119. *Sciences et Avenir*, 29 novembre 2017. Lien : https://www.google.fr/amp/s/www.sciencesetavenir.fr/high-tech/la-crypto-monnaie-bitcoin-consomme-plus-d-electricite-que-159-etats-dans-le-monde_118729.amp

Le compromis sécurité et vitesse est au cœur de la problématique de validation et sécurisation des transactions, *a fortiori* dans le cadre du mécanisme de *proof-of-work*. En figeant la création des blocs à 10 minutes par l'ajustement de difficultés de minage, Satoshi Nakamoto semble avoir voulu maximiser la sécurité. Certes, il est peu probable qu'en l'état, le Bitcoin puisse être utilisé pour réaliser des échanges quotidiens puisqu'il serait trop lent et cher dans ce contexte. En revanche, il pourrait l'être pour des transactions critiques. Exprimé en des termes simples : un coût de transaction de 35 euros[120] avec une durée d'exécution de 10 minutes n'est pas compétitif pour acheter une baguette de pain mais l'est tout à fait pour un achat immobilier par exemple. La sécurité absolue constitue par ailleurs un argument de poids pour constituer une réserve de valeur et un moyen d'échange sûr. L'or, par exemple, constitue une réserve de valeur mais il est un piètre moyen de transaction au quotidien. Cette vision n'est néanmoins pas figée ; des évolutions technologiques comme le *Lightning Network* pourraient changer la donne, une fois stabilisées, en permettant une scalabilité accrue par l'enregistrement d'un nombre plus limité de transactions dans la Blockchain en fonction de leur degré de criticité. Ce dernier constitue un *second-layer*, c'est-à-dire que des transactions seront opérées en dehors de la Blockchain *via* un canal de paiement entre plusieurs acteurs. Seul le solde du canal sera enregistré dans la Blockchain à sa fermeture. À titre de comparaison, il s'agit d'une forme de réplication du mécanisme de compensation, bien connu du système bancaire. Par exemple, si la banque A doit 5 euros à la banque B et si la banque B doit 10 euros à la banque A, alors la banque B réglera 5 euros à la banque A pour éviter deux versements.

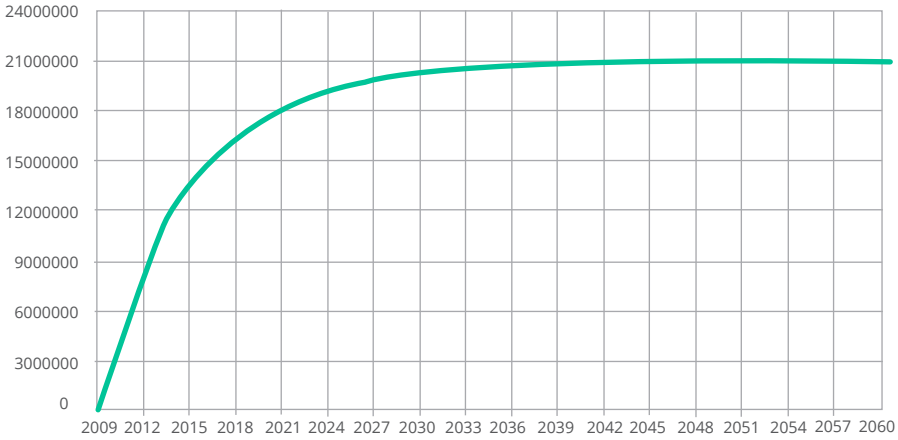
Le modèle microéconomique du Bitcoin : l'intérêt à miner

L'écosystème Bitcoin garantit donc la rémunération incitatrice, par création monétaire, des mineurs mettant à disposition leur puissance de calcul. Dans le détail, à quelles logiques économiques obéissent ces mineurs ? Le Bitcoin génère-t-il une nouvelle économie de rente chez eux ? En réalité, le minage répond à des logiques microéconomiques très classiques. La meilleure image est celle d'une mine d'or. Le vocabulaire choisi, par ses créateurs et par l'ensemble de la communauté, multiplie d'ailleurs les références à l'or et à son extraction : le Bitcoin serait pour certains l'or digital et le choix du terme « mineur » pour caractériser les individus mettant à disposition leur puissance de calcul n'est certainement pas un hasard.

120. Au plus haut enregistré, fin 2017. Source : bitcoinfees. Lien : https://bitcoinfees.info/

Le coup de maître de Satoshi Nakamoto est d'avoir réussi à reproduire les mécanismes microéconomiques d'une mine d'or par le code informatique, appliqué à la monnaie. Il brouille les frontières de définition des classes d'actifs entre monnaie et commodité notamment, en réintroduisant, dans son système monétaire *ad hoc*, une notion de rareté de l'offre (élément de plus en plus négligé dans l'économie monétaire traditionnelle). Un bitcoin est dénombrable, en unités fractionnables, jusqu'au huitième chiffre après la virgule (cette unité est appelée le Satoshi).

ESTIMATION DE LA CROISSANCE DE LA MASSE MONÉTAIRE AU COURS DU TEMPS



Comparons. D'un point de vue microéconomique, le mécanisme de minage s'apparente fortement à la logique de commodité. Le protocole Bitcoin fonctionne comme une sorte de mine d'or digitale ou usine de fabrication de monnaie, mais dont la chaîne de production s'adapterait automatiquement pour interdire dans les faits toute tentation de type « planche à billets ».

Chaque mineur de Bitcoin peut être comparé à un mineur d'or ou à un extracteur de pétrole. Pour extraire une once d'or, le mineur investit dans du matériel lui permettant de creuser ; une pioche dans le cas le plus simple, une mine entière avec des machines dans un cas plus complexe. Pour se doter de ce moyen d'extraction, le mineur réalise un investissement de départ (*capex* ou *capital expenditure,* « dépenses d'investissement ») et couvre des coûts chaque jour qu'il mine. Ces dépenses opérationnelles correspondent notamment au coût de maintenance des machines et des pioches, au pétrole permettant leur fonctionnement…

Le mineur d'or ne va employer ses facteurs de production (capital, travail) que si les revenus qu'il anticipe en *output* sont au moins égaux aux coûts de ces facteurs. Le producteur est preneur de prix *(price taker)*, c'est-à-dire que, sous l'hypothèse d'atomicité du marché, il ne peut influer sur le prix mondial de l'once d'or qui est donc une donnée exogène. Ainsi, la demande d'or, fonction des besoins industriels et des investissements financiers contracycliques, oriente-t-elle le comportement microéconomique des mineurs. En effet, plus le prix monte, plus le nombre de mineurs doit croître, attirés par l'appât du gain. Plus le nombre de chercheurs progresse, plus la probabilité de trouver facilement de l'or diminue puisque le sol en surface de la mine est foulé par davantage de chercheurs, réduisant de fait la probabilité de tomber le premier sur une once. Dans le même temps, la hausse du prix de l'or a également pour effet de rendre rentable une extraction plus coûteuse pouvant correspondre à une fouille plus profonde. Dans le cas du pétrole, des forages très coûteux dans le Grand Nord ont été commencés lors du pic du prix du baril, forages pour la plupart abandonnés car devenus non rentables avec le recul des prix du pétrole.

Le Bitcoin réplique par le code ce mécanisme. Chaque mineur investit dans du *hardware* (*capex*, l'équivalent de la pioche) puis fait face à des dépenses d'électricité nécessaire à la résolution des algorithmes.

Le rythme de création des blocs est calé en moyenne sur 10 minutes, pour garantir le coût de reproduction de la chaîne. Le système fournit donc une récompense par le mécanisme de création monétaire *(minting)* stable dans le temps en quantité de bitcoins (*modulo* la division, prévue dès le départ, tous les quatre ans du nombre de bitcoins correspondant au *reward*). Quel que soit le nombre d'utilisateurs connectés au réseau et la puissance de calcul cumulée mise à disposition, la trajectoire d'offre en unités de Bitcoin, correspondant exactement au montant en bitcoins de rémunération totale des mineurs, est donc connue depuis la création du protocole.

Comment le système se régule-t-il ? Plus la demande de bitcoins augmente (menée soit par la spéculation soit par un usage concret nécessitant de posséder du bitcoin), plus le prix augmente sous l'hypothèse de rareté programmée de l'offre. Naturellement, plus le prix du bitcoin augmente, plus la récompense du minage, stable en bitcoins, est alléchante. Par conséquent, davantage de mineurs vont se connecter au réseau pour obtenir cette récompense. Pour maintenir le rythme de production des blocs (once d'or) à 10 minutes en moyenne, le code va

automatiquement ajuster le niveau de difficulté de résolution de l'algorithme permettant la validation du bloc[121].

Quel impact concret a l'augmentation du niveau de difficulté chez le mineur ? En réalité, le niveau de difficulté se traduit par une probabilité plus faible de trouver un bloc (davantage de mineurs sont en compétition pour dénouer le bloc) à intervalle de temps fixe. C'est en fait la probabilité de trouver un bloc qui est fonction du nombre de mineurs connectés au réseau, lui-même fonction du prix de marché du bitcoin. La différence fondamentale entre l'usine Bitcoin et une usine classique est que le mineur ne fixe pas directement sa quantité de production, qui lui est donnée par l'algorithme. En revanche, à un niveau de difficulté donné, le mineur peut agir sur la probabilité de trouver un bloc par la puissance de calcul mise à disposition. Plus le *capex* investi est important, plus les chances du mineur d'obtenir un bitcoin sur un intervalle de temps fixé sont importantes.

Ces logiques répondent à un modèle microéconomique industriel classique. Le mineur est un producteur, investissant dans du *hardware* pour commencer son activité de minage. Ce coût fixe est amorti, divisé de façon cumulée par les unités supplémentaires de bitcoins extraits. Le fonctionnement nécessite également une connexion Internet et une puissance de calcul quantifiée en électricité. Ces coûts sont variables ; si je débranche le matériel pour arrêter la production, les dépenses s'arrêtent immédiatement. En revanche, elles sont stables puisque le montant d'électricité engagé est identique heure par heure : la hausse du niveau de difficulté n'augmente pas le coût de l'électricité ni la puissance nécessaire toutes choses égales par ailleurs. Elle modifie, comme évoqué, la probabilité d'obtenir un bitcoin dans un laps de temps donné pour un certain niveau de puissance. Si la consommation mondiale d'électricité s'est envolée, avec la croissance rapide du prix du bitcoin, c'est à cause de l'inflation du nombre de mineurs connectés.

Pour illustrer ces propos, plaçons-nous dans le cadre théorique suivant[122] :

- le réseau est composé de 12 mineurs dont la puissance de calcul est égale, ainsi, par bloc, chaque mineur a une probabilité de 1/12 (environ 8 %) de le miner[123] ;

---

121. Yonathan Sompolinsky, Aviv Zohar, *Bitcoin's underlying incentives,* vol. 15 issue, 5 acm queue, Association for computing machinery, 2017. Lien : https://queue.acm.org/detail.cfm?id=3168362..

122. Les hypothèses concernant le nombre de mineurs, les coûts fixes et variables, ainsi que les revenus, sont purement illustratifs afin d'avoir un modèle plus compréhensible.

123. À puissance de calcul égale, chaque mineur a autant de chances qu'un autre de trouver la solution d'un bloc, on parle d'équiprobabilité.

- un bloc est miné toutes les 10 minutes et chaque bloc offre 25 bitcoins au mineur (à date, un mineur reçoit en réalité 12,5 bitcoins par bloc miné ; pour simplifier les calculs, nous considérons le montant de 25[124]). En une journée, 144 Blocks doivent être minés[125] pour une production totale de 3 600 bitcoins ;
- les coûts fixes (le *hardware)* sont de 100 euros, les coûts variables sont de 2 euros par bloc qu'il soit miné avec succès ou pas. Ces coûts couvrent les frais d'électricité et de maintenance (supposés identiques pour tous les mineurs) ;
- les mineurs ne détiennent pas de bitcoins par ailleurs et sont preneurs de prix, c'est-à-dire qu'ils n'ont pas la capacité d'influencer le prix du bitcoin ;
- le prix d'un bitcoin sur le marché est de 2 euros (montant purement illustratif), ainsi un bloc miné rapporte 50 euros.

Considérons l'équation économique d'un seul mineur : sur les 144 blocs émis en une journée, son espérance de blocs résolus est de 12[126]. La quantité de blocs qu'un mineur peut espérer miner en une journée est donc la suivante :

QUANTITÉ PRODUITE PAR JOUR

Blocs minés avec succès (1)	BTC reçus (2)	BTC cumulés (3)
1	25	25
2	25	50
3	25	75
4	25	100
5	25	125
6	25	150
7	25	175
8	25	200
9	25	225
10	25	250
11	25	275
12	25	300

124. Montant observé entre novembre 2012 et juillet 2016. Comme expliqué précédemment, le nombre de bitcoins créé par bloc est divisé par deux tous les 4 ans.
125. 144 blocs minés = (minutes par jour)/10 = (24x60)/10.
126. Espérance blocs minés dans la journée = (nombre total de blocs émis) x (probabilité de miner un bloc) = 144 x (1/12) = 12.

Pour chaque bloc miné avec succès, un mineur subit environ 11 échecs. Par conséquent, les coûts variables associés à un bloc miné avec succès sont de 24 euros, puisqu'il faut tenter de résoudre la solution de 12 blocs pour en miner un et chaque bloc a un coût d'électricité de 2 euros. La structure de coût d'un mineur est donc la suivante :

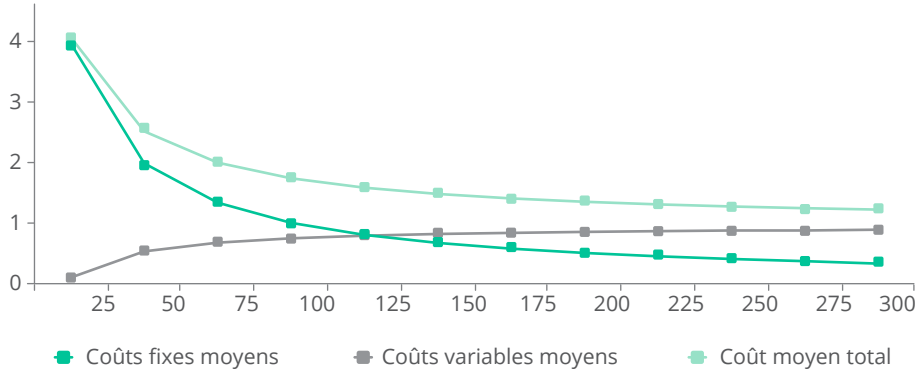
STRUCTURE DE COÛTS

Coûts fixes (4)	Coûts variables (5)	Coût total (6)=(5)+(4)	Coûts fixes moyens par BTC (7)=(4)/(3)	Coûts variables moyens par BTC (8)=(5)/(3)	Coût total moyen (9)=(7)+(8)	Coût marginal d'un BTC
100	2	**102**	4.0	0.1	**4**	**0.96**
100	26	**126**	2.0	0.5	**3**	**0.96**
100	50	**150**	1.3	0.7	**2**	**0.96**
100	74	**174**	1.0	0.7	**2**	**0.96**
100	98	**198**	0.8	0.8	**2**	**0.96**
100	122	**222**	0.7	0.8	**1**	**0.96**
100	146	**246**	0.6	0.8	**1**	**0.96**
100	170	**270**	0.5	0.9	**1**	**0.96**
100	194	**294**	0.4	0.9	**1**	**0.96**
100	218	**318**	0.4	0.9	**1**	**0.96**
100	242	**342**	0.4	0.9	**1**	**0.96**
100	266	**366**	0.3	0.9	**1**	**0.96**

Les coûts marginaux sont calculés comme le coût total d'une unité supplémentaire[127]. Comme nous l'expliquions précédemment, chaque mineur peut être comparé à une usine de fabrication de monnaies. Cette usine est composée d'une seule machine industrielle et le coût de production d'une unité supplémentaire n'est que le coût en électricité. Par conséquent, les coûts marginaux sont constants et égaux à 0,96 euro.

127. Le coût marginal se calcule comme le ratio (ΔCoût total) / (ΔQuantité BTC produits).

MODÈLE DE COÛT MICROÉCONOMIQUE DU BITCOIN



Pour chaque bloc miné avec succès, un mineur reçoit 25 bitcoins, soit 50 euros. Le revenu marginal est le revenu supplémentaire que génère le minage d'un bloc avec succès supplémentaire[128]. Le mineur a donc la structure de revenu suivante :

QUANTITÉ PRODUITE PAR JOUR

Blocs minés avec succès (1)	BTC reçus (2)	BTC cumulés (3)
1	25	25
2	25	50
3	25	75
4	25	100
5	25	125
6	25	150
7	25	175
8	25	200
9	25	225
10	25	250
11	25	275
12	25	300

STRUCTURE DE REVENU

Gains par bloc miné (2)x25€	Gains cumulés	Revenu marginal par BTC (3)
50	50	2.0
50	100	2.0
50	150	2.0
50	200	2.0
50	250	2.0
50	300	2.0
50	350	2.0
50	400	2.0
50	450	2.0
50	500	2.0
50	550	2.0
50	600	2.0

128. Le revenu marginal, dans notre exemple, se calcule comme : (Gains cumulés[n] – Gains cumulés[n-1]) / (BTC cumulé[n] – BTC cumulé[n-1]).

À niveau de difficulté stable, de la même manière que les coûts marginaux sont constants, les revenus marginaux le sont aussi. Cela peut sembler contre-intuitif par rapport au cadre classique d'analyse de la microéconomie traditionnelle. Dans une économie de production de marchandises, une augmentation de la quantité d'un produit induit une baisse du prix de celui-ci, du fait d'un excès d'offre par rapport à la demande. Dès lors, une entreprise qui augmenterait considérablement sa production verrait ses revenus unitaires baisser et donc son revenu marginal décroître. On ne peut cependant appliquer ce cadre d'analyse de la microéconomie traditionnelle dans le cas du mineur du Bitcoin. D'une part, il ne détermine pas sa production, car elle est liée au nombre de mineurs sur le réseau. D'autre part, le bitcoin, tel qu'il a été pensé, repose sur la rareté avec une quantité émise finie et connue à l'avance de tous. Dès lors, l'équation économique du Bitcoin n'entre pas dans le schéma classique d'un rapport inverse entre quantité produite et prix. Cela explique que les revenus marginaux d'un mineur sont une fonction constante dans le temps dont la valeur s'ajuste en fonction du nombre de mineurs dans le réseau.

Le cadre classique d'analyse de la microéconomie traditionnelle nous indique qu'une entreprise va essayer d'ajuster sa production afin d'arriver au point d'équilibre : Coût marginal = Revenu marginal. Comme un mineur ne peut agir sur sa production, cette équation devient caduque pour analyser son modèle économique. En réalité, un mineur va continuer à miner si, et seulement si, les revenus totaux reçus en fin de journée dépassent les coûts totaux. Or, les deux seuls facteurs qui peuvent impacter à la hausse ou à la baisse ses revenus totaux sont le prix en euros d'un bitcoin et le nombre de mineurs dans le réseau (prix x volume[129]). Comment ces deux facteurs influent-ils l'un sur l'autre ? Existe-t-il un lien de causalité ? Quelles sont les variables impactant les autres ? Pour répondre à ces questions, formalisons l'exemple précédent où nous essayions de déterminer l'équation économique d'une activité de minage sur une journée :

Notons N_m le nombre de mineurs dans le réseau. Pour rappel, plus N_m est élevé plus la probabilité pour un mineur individuel de miner avec succès un bloc est faible.

Notons B la variable aléatoire égale à 1 quand un bloc est miné avec succès et 0 sinon. Si chaque mineur possède une puissance égale dans le réseau, pour chaque bloc émis, nous avons, pour un mineur individuel :

$$P([B = 1]) = \frac{1}{N_m}$$

129. Ce dernier impacte, pour rappel, le nombre de blocs pouvant être produits.

Notons B_{ms} l'espérance du nombre de blocs minés avec succès pour un mineur individuel en une journée. B_{ms} est l'espérance d'une loi binomiale de paramètre $N=144$ et $P=1/N_m$. Nous avons donc l'équation (1) suivante :

$$B_{ms} = 144 \times P([B = 1]) = 144 \times \frac{1}{N_m} \quad (1)$$

Notons N_{BTC} le nombre de bitcoins émis par bloc. Pour rappel, ce nombre est divisé par 2 tous les 4 ans. À la date de l'écriture de ce livre, il est de 12,5. Pour des raisons de simplification mathématique, nous supposons ici qu'il est égal à 25 (soit le montant entre novembre 2012 et décembre 2016). Donc :

$$N_{BTC} = 25$$

Notons C_T le coût total de l'activité de minage pour une journée. Pour rappel, cela nécessite un coût fixe initial correspondant à l'achat du matériel, noté CF_i et un coût variable C_E correspondant à l'électricité nécessaire pour miner un bloc. Pour une journée de minage, nous avons donc l'équation (2) suivante :

$$C_T = CF_i + 144 \times C_E \quad (2)$$

Notons R_T, le revenu total en euros d'une activité de minage pour une journée. Si nous notons P_{BTC} le prix en euros d'un bitcoin, nous avons l'équation (3) suivante :

$$R_T = P_{BTC} \times B_{ms} \times N_{BTC} \quad (3)$$

Un mineur n'a d'intérêt à miner que si, et seulement si, les revenus totaux générés par l'activité de minage sur une journée sont au moins supérieurs aux coûts totaux générés par cette même activité. Soit, l'équation (4) suivante :

$$R_T \geq C_T \quad (4)$$

En utilisant les équations (2) et (3) nous avons :

$$P_{BTC} \times B_{ms} \times N_{BTC} \geq C_T$$

Soit, en réajustant et en utilisant l'équation (1) nous avons :

$$P_{BTC} \geq \frac{C_T}{N_{BTC}} \times \frac{1}{144} \times N_m$$

Nous pouvons considérer que le membre

$$\frac{CFi + 144 \times C_E}{N_{BTC}} \times \frac{1}{144} \times N_m$$

de l'équation est une constante que nous notons A, nous avons donc :

$$P_{BTC} \geq A \times N_m \quad (5)$$

Cette équation nous montre le lien de causalité existant entre le prix d'un bitcoin et le nombre de mineurs dans le réseau. D'un point de vue économique, il faut comprendre de cette équation que c'est bien P_{BTC} qui en est l'élément principal. Le prix du bitcoin est fonction de la demande de bitcoins dans un contexte d'offre limitée ; le mineur est preneur de prix. Une augmentation de P_{BTC} augmente l'intérêt économique à miner, ce qui entraîne une augmentation du nombre de mineurs dans le réseau. Néanmoins, cette augmentation ne peut dépasser le seuil P_{BTC}/A ; dans le cas contraire l'activité de minage n'est plus rentable.

En effet, si

$$\frac{P_{BTC}}{A} < N_m$$

alors

$$R_T < C_T$$

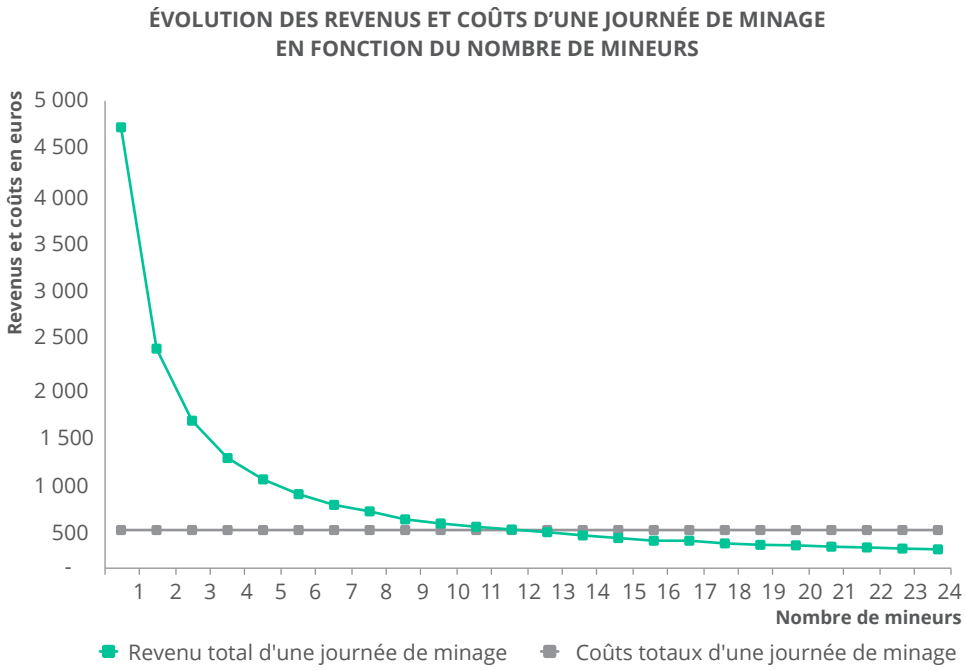
Aucun individu rationnel n'accepte de devoir payer pour entretenir le réseau donc, d'un point de vue économique, cette situation n'est pas envisageable. Cette équation nous indique également que plus le prix du bitcoin est élevé, plus le réseau est sécurisé, créant donc encore plus de confiance dans le système.

En reprenant les chiffres de notre exemple précédent, le prix du bitcoin d'équilibre est égal :

$$P_{BTC} = \frac{C_T}{N_{BTC}} \times \frac{1}{144} \times N_m$$

$$P_{BTC} = \frac{100 + 144 \times 2}{25} \times \frac{1}{144} \times 12 \approx 1{,}3 \text{ €}$$

Le graphique ci-dessous montre l'évolution des revenus et coûts totaux d'une journée de minage en fonction du nombre de mineurs pour un prix du bitcoin à 1,30 euro.



Ce graphique est une illustration de l'équation (5) précédemment trouvée : au-dessus de 12 mineurs, les revenus totaux sont inférieurs aux coûts totaux, ce qui rend l'activité de minage non rentable et réciproquement.

En synthèse, le seul et unique facteur pouvant inciter un agent économique à miner est le prix en euros d'un bitcoin. Nous proposons de rationaliser les facteurs influant sur ce prix dans la partie G, dédiée aux logiques financières de la Blockchain.

En sortant du cadre théorique, selon lequel tous les mineurs ont une puissance de calcul équivalente et un coût d'électricité similaire, un mineur peut également optimiser sa production en optant pour des *hardware*s plus performants, constituant des pools de taille importante qui mutualisent la puissance de calcul, et en s'installant dans des pays où les coûts d'électricité sont les moins chers possible. La réalité économique est donc plus complexe que notre démonstration, avec des hypothèses simplifiées à but illustratif pour comprendre les mécaniques économiques à l'œuvre. Ce raisonnement économique permet de comprendre comment la concentration croissante des nœuds brise la logique de décentralisation et d'atomicité du marché.

II.2.d Au-delà du Bitcoin : Blockchain, *cryptoeconomics* et *token*

Au-delà du Bitcoin

D'autres projets déjà évoqués ont emboîté le pas du Bitcoin et reproduisent cette même combinaison autour du *mechanism design* et du protocole consensuel. Par exemple, Ethereum reproduit la même dynamique de désincitation au piratage et à la prise de contrôle supérieure à 51 % en les rendant non rentables.

Ethereum, à l'image d'autres projets comme Neo, Cardano (entre autres), fournit un « kit Blockchain » permettant à d'autres acteurs de développer des applications, construites directement sur la plate-forme, pouvant reposer également sur des *Smart Contracts*. Ethereum facilite la création d'applications, libres de générer à leur tour des environnements nouveaux, exploitant les théories crypto-économiques du *mechanism design*.

Tous les projets de l'écosystème Blockchain (start-up ou initiatives privées) n'exploitent néanmoins pas cette combinaison entre technologie Blockchain et incentives associés. C'est l'exploitation ou non de la *cryptoeconomics* qui constitue l'axe principal d'analyse et de segmentation de la Blockchain[130], et correspond, d'une certaine manière, à opposer décentralisation et centralisation.

Cela ne signifie pas que ces projets n'ont pas de valeur, mais ils sont par nature moins complets dans leur puissance disruptive que ceux qui capitalisent parfaitement sur la technologie comme catalyseur d'alignement d'intérêts.

Blockchain publique, *tokens* et incentives : machine à *reward*

La technologie, le code et les algorithmes rendent possible la fabrication d'une machine à générer des comportements sur un réseau.

Pour poursuivre sur la logique de l'alignement d'intérêts, il est temps de revenir plus en détail sur la notion de *token* (ou crypto-monnaie, crypto-actif). À ce stade du raisonnement, il faut voir ce fameux *token* comme un simple « jeton » (comme son nom l'indique) permettant de récompenser des comportements et plus largement de répartir la valeur dans un écosystème. Nous y reviendrons à plusieurs reprises dans différents contextes, mais on peut résumer la définition du *token*

130. Lien : https://www.coindesk.com/making-sense-cryptoeconomics/

à l'unité de compte échangée sur une Blockchain[131]. Il est à la fois droit d'entrée et seule métrique qui vaille dans cet écosystème nouvellement créé. Très souvent, le *token* correspond en fait à un droit d'usage de la solution créée.

Notons au passage qu'il nous semble peu pertinent d'opposer la technologie Blockchain et les crypto-actifs (comme certains le font parfois dans le débat public). Un tel raisonnement représenterait une erreur d'analyse majeure puisqu'à l'origine, la technologie et le *token* ne font qu'un ; le protocole Bitcoin n'a pas lieu d'être sans l'unité de compte bitcoin. Il est évident que les projets de nature monétaire, comme le protocole Bitcoin, n'ont pas lieu d'être sans *token*. Pourrait-on imaginer l'économie de marché sans monnaie, ce qui impliquerait un retour au troc ?

Pour les projets dépassant la seule dimension monétaire, le *token* joue également un rôle fondamental dans l'innovation et l'émergence de la *token economy*. La puissance de la technologie prend tout son sens lorsqu'elle est combinée avec les mécanismes économiques adéquats. Le *token* a probablement davantage été créé en vue de générer les incentives nécessaires au bon fonctionnement autorégulé de l'écosystème qu'à des fins de spéculation. C'est lui qui permet aux créateurs de mettre en place des mécanismes d'incentives (correspondant aux *payoffs* : structure de gains des joueurs dans le cadre de la théorie des jeux) générant des comportements individuels rationnels ne pouvant déboucher que sur la situation collective souhaitée à l'origine.

Nier la vertu des *tokens* revient à nier la puissance disruptive, conceptuelle et révolutionnaire de la Blockchain telle qu'imaginée par ses fondateurs. L'utilisation de la seule technologie Blockchain (sans *token*) dans un cadre purement privé, voire permissif, est intéressante et très utile dans certaines industries, mais très limitée par rapport aux possibilités ouvertes par cette vague d'innovations. Certaines initiatives privées observées peuvent correspondre parfois à l'utilisation de bases de données distribuées, déjà largement présentes dans les entreprises[132].

Pour reprendre la comparaison avec Internet, ce ne sont pas les projets Intranet qui ont forgé et transformé le monde que nous connaissons aujourd'hui. Certains acteurs de l'écosystème des débuts n'envisagent d'ailleurs la Blockchain que sous sa forme publique, organisée en réseau, avec pour vocation initiale l'objectif quasi mystique de réinjecter de l'horizontalité et de la décentralisation dans les organisations

131. À date, il n'est pas possible d'échanger des *tokens* différents *via* la Blockchain (à l'exception des *tokens* ERC-20 concus sur la Blockchain Ethereum).
132. Lien : https://hackernoon.com/the-emerging-science-of-token-economics-conference-call-on-nov-6-2pm-3pm-est-c9ab3946ed6b

économiques humaines. Ils voient naturellement d'un assez mauvais œil la récupération de morceaux de cette technologie par les pouvoirs centralisés… Il convient de rappeler que l'existence d'un *token* circulant sur une Blockchain n'est cependant pas forcément synonyme de décentralisation, puisque l'on peut tout à fait imaginer la création d'une cryptomonnaie par une banque centrale.

Les cas d'application suivants d'écosystèmes décentralisés, basés sur la chaîne Ethereum et reposant sur un *token* au rôle fondamental dans la gestion des incentives, permettent de saisir facilement et concrètement le potentiel de la Blockchain. Ces exemples permettent également de comprendre le rôle de la Blockchain quant aux asymétries d'information.

L'alignement d'intérêt en réseau comme alternative aux plates-formes centralisées ?

Le projet français BTU Protocol permet de bien comprendre la vertu des modèles de *tokens*. Tout l'objet est de permettre de garantir la bonne tenue d'un marché en organisant une économie de réseaux où les acteurs vont interagir selon les règles fixées par le protocole et les mécanismes d'alignement d'intérêt. Ces derniers permettent de créer un environnement stable, sans besoin de confiance dans un tiers centralisé.

BTU propose une plateforme de réservation pour tous types d'activités (hôtels, transports, musées, etc.) et vise à remettre en cause le monopole des plateformes. Le *token* BTU sert à aligner les intérêts avec deux mécanismes :

- le dépôt de BTU *tokens* pour garantir la réservation, que touchera le fournisseur en cas d'annulation de dernière minute ;
- la récompense des apporteurs d'affaires une fois la réservation consommée.

Les marchés prédictifs catalysés par la Blockchain ?

Les cas des start-up Gnosis[133] (construites sur Ethereum) et Augur[134] autour des marchés prédictifs constituent un exemple concret en matière d'émergence décentralisée de l'information optimale dans un

133. Lien : https://gnosis.pm/. Pour situer le débat, la gnose provient du grec « connaissance » et correspond à un phénomène philosophico-religieux selon lequel le salut passe par un lien direct avec la divinité.
134. Lien : www.augur.net/

écosystème créé. Dans le cadre d'un marché prédictif, un marché de paris est ouvert autour de l'issue d'un événement futur quel qu'il soit (enjeux binaires : Trump va-t-il être réélu ? ou plusieurs *outputs*…). En fonction des informations dont ils disposent, les acteurs économiques parieront sur le résultat tel qu'ils l'anticipent[135]. Les acteurs pour lesquels l'issue est en ligne avec leurs prévisions sont rémunérés *via* le *token* créé dans l'écosystème. L'incitation économique et la décentralisation du processus permettent de faire émerger des consensus publics, dynamiques, potentiellement moins biaisés qu'un sondage classique et ne reposant pas sur des débats d'experts sélectionnés pour l'occasion. En faisant émerger *bottom-up* les meilleures informations sans aucun filtre (ne sont censés parier que les acteurs convaincus, avec une probabilité importante de détenir la vérité, si le pari est payant et/ou si un mauvais pari est facturé), le mécanisme des paris sportifs pourrait être révolutionné. En effet, la cote était jusqu'ici fournie par un bookmaker centralisé ; dans un futur proche, on pourrait imaginer un environnement de paris dans lequel la cote serait générée par le marché lui-même comme résultante de l'offre et de la demande (*i. e.* de la synthèse des anticipations dans un sens ou dans l'autre).

Concrètement, un tel mécanisme peut faciliter le processus de découverte de prix sur un marché *price discovery*, dans le cadre d'une pré-enchère par exemple. À terme, il pourrait globalement augmenter la qualité de l'information publique, voire trouver une application dans les marchés financiers.

Le concept de marché prédictif n'est pas nouveau puisque sa première réalisation date de 1988 (création du marché électronique de l'Iowa pour prédire les résultats des élections). Jusqu'à présent, les marchés prédictifs peinaient à trouver leur public, certainement pour des raisons conceptuelles mais aussi pour cause de coûts de fonctionnement et de structure trop lourds en l'absence de technologie parfaitement adaptée. Une transparence accrue, un processus plus adapté et automatisé par *Smart Contract*, des coûts fixes plus rapidement amortis du fait de la possibilité de créer un nouveau pari en API sur une plate-forme existante sont autant de facteurs qui pourraient faire de la Blockchain un catalyseur des marchés prédictifs. Signe d'un avenir potentiellement radieux pour les marchés prédictifs et la Blockchain : Gnosis et Augur cotent, au 31 décembre 2018, respectivement 12 et 88 millions de dollars[136].

---

135. Jeremy Clark (Concordia), Andrew Miller (Maryland), Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Arvind Narayanan (Princeton), *On Decentralizing Prediction Markets and Order Books*, 2014. Lien : www.econinfosec.org/archive/weis2014/papers/Clark-WEIS2014.pdf

136. Source : coinmarketcap.com le 31/12/2018

Par extension, certains penseurs (dont Vitalik Buterin, le fondateur d'Ethereum) voient dans la Blockchain et ses premières applications l'heure de gloire de la « futarchie », système inventé par Robin Hanson[137]. Pour ce dernier, le mécanisme de choix public actuel n'est pas optimal car les démocraties n'agrègent pas correctement l'ensemble des données disponibles. La futarchie consiste à voter pour des valeurs (grandes orientations), mais à parier sur des moyens concrets. Lorsque les acteurs estiment qu'une politique proposée est en ligne avec les choix votés, alors cette disposition prend forme de loi. La futarchie se veut neutre à l'idéologie et pourrait permettre la genèse de régimes de tout type, du socialisme au libéralisme extrême, au gré des votes et des marchés de paris mis en place. Nul doute que ce système, au demeurant jamais testé, est controversé et contesté d'un point de vue philosophico-politique. Le concept n'en demeure pas moins intéressant et permet d'illustrer l'impact potentiel de la Blockchain sur la gouvernance politique et la gestion publique de l'information.

II.3 Blockchain et gouvernance : la fin de l'entreprise ?

II.3.a Les preuves tangibles d'un mouvement amorcé

Le pouvoir d'évocation et la notoriété spontanée de la « marque » Bitcoin sont aujourd'hui immenses bien que difficilement quantifiables. Pourtant, cette marque, pas plus que la technologie qui la sous-tend, n'appartient à personne. Levons le doute une fois pour toutes : personne ne sait qui est Satoshi Nakamoto, il n'existe pas d'entreprise ou de marque déposée Bitcoin et aucun étudiant de Harvard n'ira jamais travailler à vélo à Bitcoin dans un immeuble vitré de Palo Alto. Il s'agit d'un protocole décentralisé, développé par des créateurs anonymes, puis mis à disposition – en langage *open source* – des utilisateurs. C'est la communauté Bitcoin qui entretient le système, selon le principe du consensus. Bitcoin est donc bien un objet nouveau, d'une nature et d'une ampleur sans précédent. Dans l'histoire, jamais aucun projet unique n'a concentré une valeur de 67 milliards de dollars[138] (la teneur et la pérennité de cette valeur ne sont pas questionnées ici) en dehors de l'entreprise. Mais comment un projet sans CEO, sans conseil d'administration, sans

137. Robin Hanson, « Shall we vote on values, but bet on beliefs? », *Economics*, George-Mason University, 2007. Lien : mason.gmu.edu/~rhanson/futarchy.pdf
138. Source : coinmarketcap.com le 31 décembre 2018.

comptabilité, sans états financiers, peut-il être valorisé (*via* les bitcoins en circulation) à plusieurs dizaines de milliards de dollars et générer plusieurs dizaines de milliers de transactions ?

Même s'ils sont décentralisés de manière moins absolue (on connaît leurs créateurs !), d'autres projets de l'écosystème se sont également organisés en dehors des structures traditionnelles, ouvrant la voie à des débats passionnants sur les formes sociales à l'ère de la Blockchain. Ethereum par exemple, valorisé 14 milliards de dollars en avril 2018[139] sur le marché des crypto-monnaies, ne comporte pas d'actions puisqu'il s'est structuré autour d'une fondation, dans laquelle œuvrent les développeurs qui ont mis en service le réseau et en assurent la maintenance. Dans cet écosystème, des centaines de free-lance du monde entier coopèrent pour faire émerger des projets qui ne comportent pour la plupart aucun salarié. Les discussions s'opèrent sur Telegram ou Slack. Et la rémunération ? *Via* le *token* émis dans le cadre du projet.

Dans les faits, l'écosystème Blockchain semble déjà avoir rebattu les cartes de la gouvernance économique en son sein. Cette mutation (révolution ?) observée constitue-t-elle un signe avant-coureur d'une révolution globale des organisations économiques, ou un épiphénomène temporaire et non généralisable ?

II.3.b Pourquoi les entreprises existent-elles ? Des coûts de transaction de marché élevés et en hausse

La question peut paraître absurde mais l'existence de l'entreprise n'est en fait pas une évidence. Les travaux de recherche sur l'économie s'intéressent aux raisons qui poussent les acteurs à se regrouper dans des entreprises plutôt qu'à réaliser des transactions atomisées sur le marché.

Les recherches de l'économiste Ronald Coase, prolongées par Oliver Williamson, reposent sur deux questions. Si le marché est efficient pour allouer les ressources, pourquoi existe-t-il alors des entreprises dont le rôle est de limiter le recours à des transactions de marché ? À l'inverse, pourquoi l'entreprise n'a pas totalement mis fin au marché ? On peut définir le marché comme un mécanisme de transfert permis par une offre et une demande se rencontrant volontairement sur un prix d'équilibre, et l'entreprise comme un mode hiérarchisé

139. Source : coinmarketcap.com le 31 décembre 2018.

d'organisation plus ou moins centralisée[140]. *In fine*, dans le jargon de la Blockchain, on pourrait à grand trait assimiler le marché à une solution décentralisée et l'entreprise à une solution centralisée.

Coase et Williamson associent des coûts aux deux fonctionnements : ceux de coordination pour l'entreprise et ceux de transaction pour le marché. Ces derniers sont supposés nuls dans la théorie néoclassique reposant sur l'hypothèse de concurrence pure et parfaite. En réalité, ils ne sont pas nuls en raison notamment des coûts :

- de découverte de l'information dans un contexte de concurrence imparfaite et d'asymétrie d'information (le prix ne reflète pas parfaitement l'information pure, situation d'incertitude) ;
- de la confiance placée dans un certain nombre d'intermédiaires ;
- de négociation de contrat ;
- de traitement de la transaction elle-même[141].

Plus les transactions sont spécifiques (lorsqu'aucune des deux entreprises ne pourrait trouver une contrepartie plus efficace), fréquentes (coûts de réécriture, multiplication des contrats), et incertaines (possibilité d'échec de la transaction, asymétrie d'information), plus le coût du contrat et de la transaction est élevé.

Pour Coase et Williamson, l'entreprise existe lorsque les coûts de coordination sont inférieurs aux coûts de transaction. Ainsi, dans la plupart des cas, l'entreprise est un moyen moins coûteux que la transaction de marché[142].

D'après les travaux de John Joseph Willis et Douglass C. North[143], les coûts de transaction aux États-Unis ont fortement augmenté au XX^{e} siècle, justifiant dès lors l'augmentation du nombre d'entreprises de taille importante. Ces travaux mesurent l'évolution des coûts de transaction en quantifiant la part que représente le secteur des transactions dans l'économie américaine (en pourcentage du PIB). Selon eux, la spécialisation croissante, l'urbanisation et la multiplication des échanges augmentent le coût du contrat à mesure que les relations *inter personæ* répétées diminuent. La complexification des échanges lointains a également nécessité le recours à des intermédiaires à qui l'information est souvent achetée (le coût de la confiance, encore). La seconde explication

140. Concept de coûts de transaction, évoqué par R. Coase, « The nature of the firm », *Economic,* novembre 1937, traduction française *Revue française d'économie II,* hiver 1987. Cité par Xavier Galiègue.
141. Williamson O. 1979, *Transaction costs economics: the governance of contractual relations, journal of law and economics*. Cité par Régis Blazy dans son cours, IEP Strasbourg, 2011.
142. Issue du cours de Régis Blazy, IEP Strasbourg, 2011.
143. Joseph Willis, Douglass C. North, *Measuring the transaction sector in the America economy,* University of Chicago Press, 1986.

concerne le progrès technique et l'augmentation de l'intensité capitalistique, qui s'est traduite par une augmentation de la taille des entreprises. La mécanisation massive génère des économies d'échelle dans le cas de production abondante en série, nécessitant un flux d'*inputs* constants et ordonnés, rendus moins coûteux dans une organisation établie.

ÉVOLUTION DES COÛTS DE TRANSACTION DANS L'ÉCONOMIE AMÉRICAINE[144]

Années	Coûts de transaction (secteur privé)	Coûts de transaction (secteur public)	% coûts de transaction dans le PNB des USA
1870	22,5 %	3,6 %	26,1 %
1890	29,1 %	3,6 %	32,7 %
1910	31,5 %	3,7 %	35,2 %
1930	38,2 %	8,2 %	46,3 %
1950	40,3 %	10,9 %	51,2 %
1970	40,8 %	13,9 %	54,7 %

Du fait de l'incertitude des relations contractuelles générant des coûts de transaction élevés, l'entreprise s'impose comme solution efficace. La théorie de l'agence explique le recours à l'entreprise en justifiant un meilleur contrôle, puisque la centralisation permet notamment une meilleure observation de l'effort de l'agent par le principal.

La théorie des contrats stipule que l'autorité, *i. e.* l'entreprise, se substitue à la renégociation des contrats, inévitable dans un contexte de contrats incomplets. La quasi-totalité des contrats existants dans l'économie sont incomplets, c'est-à-dire qu'ils ne prévoient pas la totalité des cas de figure, ne peuvent automatiquement prévoir une rémunération par *output*/état du monde et doivent être réécrits à chaque changement de paramètre. Ainsi, Grossman et Hart définissent l'entreprise comme « un nœud de relations bilatérales gérées par des contrats incomplets stipulant une relation hiérarchique ou unifiée[145]. »

144. Tableau publié dans le cours de Régis Blazy sur la gouvernance d'entreprise, IEP Strasbourg, 2011.
145. Hart Grossman, *The costs and benefits of ownership: a theory of vertical integration*, 1986.

II.3.c Que changerait la Blockchain ? *Smart Contract* et *mechanism design*

La combinaison de la transparence absolue, du *mechanism design* et de l'exécution automatique des *Smart Contracts*[146] pourrait en théorie fortement réduire le coût du contrat et les coûts de transaction (fonction de la spécificité, de la fréquence et de l'incertitude du contrat) et par conséquent rendre l'existence de l'entreprise moins compétitive[147] en faveur des échanges/transactions sur une Blockchain publique. Le *mechanism design* et la transparence peuvent en effet permettre de réduire l'asymétrie d'information (les données sont publiques et traçables) et, par conséquent, les risques d'aléa moral et d'antisélection, qui justifient dans la théorie économique le besoin de hiérarchie et de centralisation. Opérationnellement, le *Smart Contract* peut abaisser les coûts administratifs de mise en place et d'exécution d'un contrat ; des bibliothèques-types, infiniment duplicables et adaptables, pourraient par exemple être développées.

Les *Smart Contracts* constituent des contrats complets[148], qui pourraient théoriquement prévoir un *output* pour chaque état du monde de manière automatisée, dans un contexte d'aléa moral très fortement amenuisé. L'imbrication de transactions sur la Blockchain, organisées *via* des *Smart Contracts* imbriqués à leur tour dans une architecture plus large (DAO pour *Distributed Autonomous organizations*) pourrait ainsi, dans ce cadre analytique, constituer une alternative aux organisations économiques.

Prenons un exemple simple. Dans le cas d'une course en Uber, c'est la société Uber qui supprime par la centralisation et l'existence d'une entreprise tierce (tiers de confiance) l'incertitude du contrat. La société assure au chauffeur qu'il sera payé et au passager qu'il arrivera à bon port. Le rôle d'Uber pourrait dans ce cas être remplacé par un *Smart Contract*, garantissant le même niveau d'incertitude faible, mais sans entreprise centralisée. À l'entrée dans le véhicule, le contrat se met en place et déclenche automatiquement le paiement en fonction d'une série de conditions établie au préalable (par exemple, l'arrivée sain et sauf à destination).

Selon Primavera de Filippi, Jason Potts et Sinclair Davidson, la Blockchain publique ne représente pas simplement une technologie de l'information

---

146. Pour rappel, les *Smart Contracts* peuvent se définir comme « des programmes informatiques qui sécurisent, imposent et exécutent la mise en place d'accords conclus entre individus et entreprises », selon les termes de Donald et Alex Tapscott, *Blockchain Revolution*, Portfolio Penguin, 2016.
147. Sinclair Davidson, Primavera De Filippi, Jason Potts, *Economics of Blockchain*, 2016.
148. *Ibid*.

et de la communication mais une nouvelle forme de gouvernance – autour de la transaction comme unité analytique de base, compétitive de l'entreprise et du marché. La Blockchain n'est pas une organisation traditionnelle, ce n'est pas non plus un marché ; elle s'en rapproche fortement, mais le dépasse. Elle facilite en réalité les transactions et non simplement les échanges et permet un réseau de relations entre individus. Ces mêmes auteurs considèrent finalement que la Blockchain constitue une « catallaxie », concept introduit par l'école autrichienne (décidément très proche – *a posteriori* ! – de la Blockchain) et plus précisément par Hayek, dans la continuité de Ludwig Mises. Elle fait référence, selon la définition d'Hayek, à « l'ordre engendré par l'ajustement mutuel de nombreuses économies individuelles sur un marché. Une catallaxie est ainsi l'espèce particulière d'ordre spontané produit par le marché à travers les gens qui se conforment aux règles juridiques concernant la propriété, les dommages et les contrats ». Définie plus simplement par l'*Encyclopedia Universalis*, elle constitue un « mode abstrait de gestion d'informations produisant un ordre spontané optimal ». Cette ouverture philosophico-économique rappelle la puissance conceptuelle de la Blockchain, autour d'un système de valeurs, nouveau ou passé – revisité grâce à la technologie.

II.3.d Blockchain, entreprise et évolution du travail

En poursuivant le raisonnement de Coase et Williamson, opposant de façon binaire les coûts de transaction et de coordination, les briques technologiques de la Blockchain publique vont être dans le même temps récupérées par les entreprises établies, qui s'organiseront seules – par l'instauration de Blockchains privées ou en groupe d'acteurs – par le biais de Blockchains permissives. Cette appropriation par les grands acteurs de la technologie ne permettra pas seulement un choc de compétitivité (par simplification des process) mais aussi une réduction des coûts de coordination internes. L'accès à la donnée et son agencement, tout comme les modes de communication internes pourraient être recomposés en faveur d'une fluidité accrue. Ce sont à la fois les coûts de coordination internes aux entreprises et les coûts de transaction (opérés sur le nouvel objet public Blockchain) qui pourraient être réduits. Difficile dès lors de conclure si, *in fine*, nous observerions plus ou moins d'entreprises traditionnelles qu'auparavant dans un monde « blockchainisé ».

La Blockchain ne s'imposerait donc comme une révolution des organisations économiques que si le postulat de départ, selon lequel la gouvernance d'entreprise n'existe que pour suppléer à l'asymétrie d'information et compenser l'aléa moral par l'autorité, est vérifié. Comme le rappellent De Filippi, Sinclair et Potts, si l'entreprise actuelle existe

pour d'autres raisons (complémentaires ou non), la compétitivité de la Blockchain publique comme gouvernance décentralisée est moindre. Mais la fin de l'entreprise est-elle d'ailleurs souhaitable, d'un point de vue pragmatique et sociologique ? L'entreprise n'est-elle pas le garant quotidien d'une forme de lien social entre hommes et femmes dans le cadre du travail ?

Quant à l'avenir du travail, des organisations et de l'entreprise, la Blockchain s'inscrit en réalité dans un débat socioéconomique qui la précède. Avant son invention, et en lien notamment avec l'émergence des nouvelles technologies de l'information et de la communication (NTIC), de nombreux écrits avaient déjà démontré les gains possibles en matière de coûts de transaction, ou questionné l'évolution des modes de management. Dans un article de *L'Expansion management Review* de 2010, Frédéric Fréry s'interroge : « Et si l'entreprise n'avait été qu'un épisode de l'histoire[149] ? » Il anticipe (en citant Daniel Pink) la fin du salariat qui laisserait place à des agents indépendants free-lance, mis en relation par des plates-formes. Il donne l'exemple d'Amazon Mechanical Turk, permettant déjà de parcelliser les tâches entre des travailleurs et des demandeurs, mis en relation par le Web. Au global, l'auteur entrevoit, grâce au Web, la fin de l'entreprise au profit d'une « constellation de guildes de métiers, de marchands, de financiers, de fermages et de façonniers », résurgence de modes d'organisation que le capitalisme avait éclipsés. La Blockchain s'inscrit parfaitement dans ce mouvement : la technologie propose un modèle de gouvernance dépassant les places de marché proposées par Internet. Elle permet en effet la mise en relation directe entre les acteurs, sans intervention d'une place de marché centralisée. Lawrence Ludy, d'Outlier Ventures, prévoit la fin des strates intermédiaires de management, remplacées par des *Smart Contracts* qui s'assureront des *inputs* et *outputs* d'une tâche donnée[150].

Certains auteurs, comme Xavier Galiègue[151] dans la revue *Idées économiques et sociales* en 2012 (l'article n'évoque pas la Blockchain), voient en revanche ces évolutions davantage comme un facteur de changement progressif. L'émergence des firmes virtuelles, de la transformation des relations clients-fournisseurs sur les sites marchands et la multiplication des plates-formes collaboratives comme Blablacar, sont de bons exemples de la transformation complexe en cours. Les frontières entre le marché et l'entreprise sont de plus en plus floues, les

---

149. Frédéric Fréry, « Le management 2.0 ou la fin de l'entreprise », *L'Expansion Management Review*, 2010/2, nº 137, p. 130. L'Express-Roularta. Lien : https://www.cairn.info/revue-l-expansion-management-review-2010-2-page-52.htm

150. Article de Guillaume Renouard, juin 2017. Lien : https://www.google.fr/amp/s/www.numerama.com/business/271155-comment-la-Blockchain-changera-le visage-de-lentreprise.html/amp.

151. Xavier Galiègue, « L'approche de la firme par les coûts de transaction », *Idées économiques et sociales*, 2012/4, n° 170, p. 80. Lien : https://www.cairn.info/revue-idees-economiques-et-sociales-2012-4-page-16.htm

modes d'agencement du travail humain de plus en plus diversifiés, les distinctions entre marchand et non-marchand, plus difficiles à établir. Xavier Galiègue ne projette pas la fin de l'entreprise, mais anticipe plutôt une complexité accrue des formes d'organisation et des relations entre entreprises, qui dépassera l'opposition polaire [de Williamson] entre entreprise et marché à un continuum toujours plus riches de formes intermédiaires.

Si des contre-exemples existent, la révolution Internet n'a, dans les faits, refondé la gouvernance d'entreprise qu'en surface. Comme indiqué par Don Tapscott, « si les travailleurs de la Silicon Valley ont troqué le costume-cravate contre le jean-T-shirt, la nature de leurs entreprises demeure peu ou prou la même que celle des entreprises traditionnelles[152] ». En sera-t-il autrement pour la Blockchain ? Empiriquement, il n'est pas certain que nous observions un jour une disparition généralisée de l'entreprise, comme forme d'organisation économique de référence, du fait de la Blockchain. Des questions restent ouvertes, sur le plan de la faisabilité technique et optimisée des *Smart Contracts*, mais aussi sur le plan juridique et légal. Quel statut et quelle reconnaissance juridique pour ces *Smart Contracts* ? Il n'existe à notre connaissance à ce stade, aucune définition relative au *Smart Contract* en droit positif, les prises de position se limitant à des points de doctrine. Dans son *whitepaper* d'août 2017, « *Smart Contracts and distributed ledger – a legal perspective* », l'ISDA définit le *Smart Contract* comme suit : « Le *Smart Contract* est un contrat automatisable et exécutoire. Automatisable par ordinateur, bien que certains aspects puissent requérir une intervention et une vérification de l'homme. Exécutoire, soit par la mise en vigueur légale des droits et obligations, soit *via* la preuve d'exécution inviolable du code de l'ordinateur ».

En conclusion, le scénario du big bang apparaît peu plausible. Il est plus probable que l'on assiste à une mutation, profonde et passionnante, des modes d'organisation existants et à une coexistence plus ou moins harmonieuse entre l'entreprise, le marché et des écosystèmes construits autour de Blockchains publiques.

---

152. Don Tapscott, Anthony O. Williams, *Wikinomics*, 01/06/2018, cité par *Numerama*. Lien : https://www.google.fr/amp/s/www.numerama.com/business/271155-comment-la-Blockchain-changera-le-visage-de-lentreprise.html/amp

III.
Blockchain et macroéconomie

Au sens le plus strict, la Blockchain est donc une technologie permettant de transférer et d'enregistrer des transactions de toute nature de pair à pair. Par les mécanismes d'incentives qu'elle actionne, la Blockchain est bien plus qu'une nouvelle technologie de communication puisqu'elle permet la création de nouvelles formes de gouvernance pour orchestrer les échanges entre les hommes[153]. Selon Vitalik Buterin, le fondateur d'Ethereum, « les Blockchain n'ont pas pour but de définir un *set* de règles prédéfini, elles créent la liberté de créer des nouveaux mécanismes avec leurs propres règles de manière très rapide. Il s'agit d'un "*Lego mainstorm*[154]" pour la construction d'institutions économiques et sociales[155]. »

La macroéconomie est éminemment politique, notamment dans sa forme actuelle, largement keynésienne et structurée autour de la « politique économique ». Quelle est la meilleure combinaison des politiques monétaire et budgétaire[156] pour atteindre l'optimum ? La définition de ce dernier répond d'ailleurs à des considérations quasi philosophico-politiques, s'appuyant sur différentes théories déjà évoquées (optimum de Pareto selon les écrits néoclassiques, optimum social issu de la théorie des jeux…). En poussant le raisonnement à l'extrême, le bitcoin supprime l'essence même de la politique keynésienne, en réduisant à néant toute possibilité de politique monétaire. Aucune modularité dans le processus de création monétaire n'est possible puisque la trajectoire de croissance du nombre de bitcoins en circulation est connue dès le départ et gravée dans le code. Tout est lié : à ses origines, la technologie Blockchain sert une vision du monde libérale, ouverte, décentralisée, horizontale et à certains égards aux antipodes du système actuel. La Blockchain fait donc davantage référence à une proposition de système de valeurs qu'à une simple évolution des arts et techniques.

D'un point de vue macroéconomique, quel questionnement pose la Blockchain publique, quelles opportunités porte-t-elle, pour quels risques ? Quelle valeur économique lui accorder à l'échelle globale ?

---

153. Davidson, De Filippi, Potts, *Economics of Blockchain*, Public choice, 2016, cité par Darcy William Allen (assistant de recherche au hub d'innovation Blockchain de la RMIT, université de Melbourne), *Discovering and developing Blockchain cryptoeconomy*.
154. Jeu de construction et de robotique créé par Lego en 2006.
155. Lien : www.ethdocs.org/en/latest/
156. Selon la fameuse courbe IS/LM, qui rappellera certains souvenirs aux étudiants en économie…

III.1 Les Blockchains publiques controversées car elles touchent à l'essence monétaire

III.1.a Des débats ancestraux cristallisés dans la Blockchain

Au-delà de la technologie, le sujet Blockchain cristallise avec une ampleur sans précédent de nombreux débats et oppositions théoriques, voire idéologiques : économie dirigée *vs* libéralisme, centralisation (Jacobins) *vs* décentralisation (Girondins), monnaies souveraines *vs* concurrence des monnaies… En adressant la problématique des transactions et de leurs enregistrements, la Blockchain touche à ce qui fonde notre économie, nos racines et nos valeurs (rappelons-le, l'écriture a été inventée pour matérialiser et sécuriser l'existence d'une opération de commerce). La transaction est elle-même indissociable de la monnaie. Les économistes, les politiques et les citoyens s'écharpent depuis des lustres à propos de la politique à mener la concernant : adeptes du *quantitative easing* et de la politique expansionniste contre monétaristes, défenseurs de l'euro contre fans du franc… Relations entre inflation et chômage, théorie quantitative de la monnaie, impacts positifs ou négatifs d'une dévaluation/dépréciation de la monnaie : autant de concepts non tranchés qui animent les débats d'experts et irriguent par capillarité la sphère publique et politique. Mais la monnaie revêt bien d'autres dimensions qui dépassent de loin la thématique économique. Elle est attachée au plus profond de nos valeurs et représente un ancrage historique autour de la matérialisation, de la quantification des choses, et des gains réalisés par l'Homme. Le fait que l'expression « être riche comme Crésus », fasse écho en 2018 à un fait hérité de l'Antiquité en est une bonne illustration. La monnaie et son émission sont intimement liées au pouvoir étatique, et l'évolution des formes des uns et des autres à travers l'Histoire n'ont pas ou peu remis en question ce lien. Preuve vivante de la relation entre souveraineté nationale et monnaie, les billets de banque continuent bien souvent, à l'heure du numérique, d'être ornés de la photo d'un roi ou d'un président.

Si le Bitcoin semble s'inscrire en faux avec la théorie de Jean Bodin[157] sur la nécessaire souveraineté des États, structurée autour du pouvoir de battre monnaie, il est bien en ligne avec les thèses monétaristes de l'auteur. Connu comme un des fondateurs de ce courant de pensée économique, Jean Bodin identifie l'abondance d'or et d'argent dans le royaume comme cause majeure de l'inflation observée en France au XVI^e^ siècle. D'un point de vue monétaire, le Bitcoin et les Blockchains publiques reposent en effet sur des principes philosophiques et microéconomiques très

157. Jean Bodin, *Les Six Livres de la République*, Paris, 1576.

libéraux, proches des thèses de l'école autrichienne portées notamment par Hayek, Mises et plus tard Pascal Salin. Si le bitcoin est une monnaie, cette dernière affiche en effet un prix de marché par unité dénombrable, conformément aux thèses des mêmes économistes. Selon eux, la manipulation du prix de l'argent – à savoir les taux d'intérêt[158] – et le crédit financé par la création monétaire constituent des périls majeurs générant des illusions temporaires ne pouvant déboucher que sur des crises violentes. Hayek préconisait la concurrence des monnaies[159] : ce qui ne fut, à l'époque, qu'une vue de l'esprit est désormais concret si l'on en croit la multiplication des crypto-monnaies.

III.1.b Le bitcoin peut-il être qualifié de monnaie ?

Les étudiants en économie apprennent souvent que la monnaie a émergé au VI^e^ siècle av. J.-C. L'humanité serait donc brutalement passée du troc à l'échange médiatisé. Cette idée entretient un malentendu. Certes, il est possible que des pièces de monnaie métalliques aient été utilisées pour la première fois dans l'Antiquité grecque. Il est également possible que, rapidement, des garanties publiques aient pu « labelliser » ces pièces pour en garantir la valeur. Mais l'histoire, bien que sa connaissance soit indispensable, ne remplace pas le raisonnement économique. Nous avons en effet de bonnes raisons de penser que la monnaie est utilisée, non depuis quelques centaines d'années grâce à l'action des États, mais depuis des milliers d'années. Ce sont les théories de l'économiste autrichien Carl Menger qui expliquent le mieux pourquoi.

Né en 1840 en Pologne (dans une ville appartenant alors à l'Empire austro-hongrois), Carl Menger est, avec Stanley Jevons et Léon Walras, l'un des initiateurs du courant « marginaliste » qui a révolutionné la science économique. Jusqu'alors, l'économie classique, d'Adam Smith à Karl Marx, considérait que le prix dépendait étroitement de la « valeur travail », c'est-à-dire la quantité de travail nécessaire pour produire un bien. Cette théorie de la valeur travail a eu des implications considérables, y compris politiques, puisque c'est elle qui fonde la théorie de l'exploitation marxiste. Pour les marginalistes comme Menger, la valeur et le prix dépendent de « l'utilité marginale », c'est-à-dire du surcroît de satisfaction apporté par l'achat d'une unité du bien en question. Autrement dit, la valeur provient des évaluations subjectives des individus. C'est l'une des raisons pour lesquelles les prix varient dans le temps et dans l'espace.

---

158. Pascal Salin, *La Vérité sur la monnaie*, Odile Jacob, 1990.
159. F. Hayek, *Pour une vraie concurrence des monnaies*, traduit par G. Vuillemey, PUF, 2015.

Dans ses *Principles of Economics,* publiés en 1871, Menger, avec une grande originalité, applique la théorie de l'utilité marginale à la monnaie. Pour Menger, la monnaie est un bien que les individus se procurent sans coercition des pouvoirs publics en raison de son utilité. Cette utilité, c'est essentiellement le fait d'être un moyen d'échange. L'utilisation d'une monnaie permet de réduire les « coûts de transaction ». Le troc est un mode d'échange imaginable mais il est extraordinairement coûteux puisqu'il nécessite une « double coïncidence des volontés ». L'utilisation d'un média comme une monnaie permet de supprimer la nécessité de cette « double coïncidence ». On peut acquérir ce média en vendant un bien, l'utiliser comme une réserve de valeur, puis acheter un autre bien. La monnaie rend donc un service. Il doit être instrument d'échange et de réserve de valeur. Son utilité et sa valeur viennent de là. Pour Menger, à partir du moment où il y a échange, il est logique qu'il y ait utilisation d'une monnaie. Voilà la raison pour laquelle la monnaie a préexisté aux États et même aux pièces métalliques. Sous formes de coquillages, d'épices ou de métal, la monnaie a sans doute toujours existé. Il est d'ailleurs fascinant de voir comme la monnaie réémerge souvent spontanément.

Dans son *opus magnus, La Richesse des nations*, publié en 1776, Adam Smith donnait une magistrale leçon d'histoire de la monnaie. Il est utile de citer le texte, tant il peut nous aider à saisir la vraie nature des crypto-monnaies :

« Dans les âges barbares, on dit que le bétail fut l'instrument ordinaire du commerce ; et quoique ce dût être l'un des moins commodes, cependant, dans les anciens temps, nous trouvons souvent des choses évaluées par le nombre des bestiaux donnés en échange pour les obtenir. […] On dit qu'en Abyssinie le sel est l'instrument ordinaire du commerce et des échanges ; dans quelques contrées de la côte de l'Inde, c'est une espèce de coquillage ; à Terre-Neuve, c'est de la morue sèche ; en Virginie, du tabac ; dans quelques-unes de nos colonies des Indes occidentales, on utilise le sucre à cet usage, et dans quelques autres pays, des peaux ou du cuir préparé ; enfin, il y a encore aujourd'hui un village en Écosse, où il n'est pas rare, à ce qu'on m'a dit, de voir un ouvrier porter au cabaret ou chez le boulanger des clous au lieu de monnaie. »

Pour comprendre en quoi le bitcoin est bien une monnaie, il faut compléter les apports de Carl Menger par le théorème de régression de Ludwig von Mises (en 1912), un autre économiste autrichien. L'idée de Mises est simple à comprendre : on utilise une monnaie à l'instant *t* car on sait qu'elle a eu une valeur en *t-1* (elle a permis un échange). On l'utilise en *t-1* car on sait qu'elle a eu une valeur en *t-2*… Mais selon Mises, cette suite est forcément bornée. Il existe un moment *t-x* où la monnaie a été utilisée pour autre chose qu'un échange monétaire : elle a forcément été utile pour autre chose sinon elle n'aurait pas pu devenir une monnaie à

l'instant *t-x+1*. Sa valeur a pu dériver d'une demande industrielle ou artisanale (fabriquer un bijou avec de l'or), esthétique (ramasser un coquillage), le plaisir de fumer une cigarette… Au départ, une monnaie doit donc être autre chose qu'un moyen d'échange.

Nous allons voir que le bitcoin répond aux exigences de Menger et de Mises et peut donc être qualifié de monnaie. C'est une monnaie singulière en raison de ses caractéristiques technologiques. Il présente, pour rappel, quatre particularités qu'il faut garder à l'esprit :

- le système monétaire du bitcoin est décentralisé. Les échanges se font de pair à pair. Il n'existe pas de tiers de confiance ni de centralisation des transactions (absence de banque ou de chambre de compensation) car toutes les transactions sont enregistrées sur un registre inviolable (c'est le principe de la Blockchain) ;
- il n'existe pas de monopole de création monétaire ni même de possibilité de mener une politique monétaire. La masse monétaire maximale est fixée à 21 millions d'unités ;
- les groupes d'informaticiens qui assurent la fiabilité des transactions sont rémunérés avec des bitcoins, avec des mécanismes d'incentives et d'alignement d'intérêts puissants ;
- les logiciels qui assurent le fonctionnement du système Bitcoin sont en *open source*, ce qui assure au système une transparence et une résilience maximales.

Ces caractéristiques signifient deux choses : en premier lieu, le Bitcoin est le fruit d'une grande complexité technologique qui assure la confidentialité, non pas des transactions, mais de l'aspect nominatif des transactions (l'anonymat est assuré alors même que le système est transparent) ; en deuxième lieu, le Bitcoin est basé sur des incitations qui incitent au contrôle (décentralisé) et à la résilience. Il n'est pas besoin de placer sa confiance dans un tiers (une banque centrale ou banque commerciale) pour que le système fonctionne. La notion de distance est abolie (il suffit d'un accès à Internet pour effectuer des transactions, ce qui explique que les migrants l'utilisent beaucoup), la fiabilité tend vers l'infini (sans pouvoir évidemment l'atteindre). De fait, le système Bitcoin n'a pas encore été piraté avec succès. Utiliser le bitcoin comme réserve de valeur et moyen d'échange permet donc d'éviter des baisses de pouvoir d'achat (la quantité de bitcoins est limitée).

Pourquoi le bitcoin est bien une monnaie ? Une monnaie a trois fonctions : d'abord, elle est une réserve de valeur ; ensuite, elle est un instrument d'échange et enfin, elle est un étalon de mesure. Le

bitcoin constitue une réserve de valeur. On peut stocker son épargne en bitcoins, même si la valeur de cette épargne fluctue au gré des variations des cours de cette monnaie. Elle est un moyen d'échange, très limité mais réel. Il est par exemple possible d'effectuer des achats en bitcoins sur le site de commerce en ligne Overstock. Adam Smith citait la fongibilité de l'or comme l'un de ses atouts en tant que monnaie. « Des raisons irrésistibles semblent, dans tous les pays, avoir déterminé les hommes à adopter les métaux pour cet usage, de préférence à toute autre denrée. Les métaux ont non seulement l'avantage de pouvoir se garder avec aussi peu de déchet que quelqu'autre denrée que ce soit, mais encore ils peuvent se diviser sans perte en autant de parties qu'on veut et ces parties, à l'aide de la fusion, peuvent être de nouveau réunies en masse ; qualité que ne possède aucune autre denrée aussi durable qu'eux, et qui, plus que toute autre qualité, en fait les instruments les plus propres au commerce et à la circulation », écrivait-il. C'est encore plus vrai d'une crypto-monnaie : sa fongibilité est, en théorie, totale puisqu'elle n'a pas d'existence physique. En réalité, le bitcoin n'est pas totalement fongible puisqu'il existe des bitcoins « teintés », c'est-à-dire identifiés comme suspectés d'être issus d'activités illégales. Enfin, elle peut aussi éventuellement servir d'étalon de mesure, même si cette fonction est rendue difficile par ses fluctuations. Le bitcoin remplit donc, certes imparfaitement, des fonctions monétaires.

Mais est-elle une monnaie au sens de Menger ? Oui, car elle a émergé comme un phénomène de marché. Elle rend des services, en génère une utilité, sans pour autant avoir cours légal. Elle est utilisée comme monnaie car elle est sécurisée et elle permet des transactions pseudo-anonymes et décentralisées. Ces deux caractéristiques expliquent pourquoi elle est utilisée pour des activités de blanchiment (qui ont besoin d'anonymat) et par des migrants (qui ont besoin d'effectuer des transferts d'argent sécurisés à des milliers de kilomètres).

Répond-elle au théorème de régression de Mises ? Oui. D'où vient sa valeur originelle ? La réponse est claire : de la technologie Blockchain. C'est sa fiabilité, son inviolabilité qui ont amené les premiers utilisateurs du bitcoin à vouloir se servir de cette monnaie pour des raisons souvent idéologiques. La prime utilité du bitcoin était d'effectuer une manipulation fiable et anonymisée pour des raisons philosophiques. De la technologie Blockchain est venu le caractère militant du bitcoin, au moins dans un premier temps, et sa valeur originelle au sens de l'économiste Mises.

Pourquoi utilise-t-on massivement le bitcoin dans un pays comme le Venezuela ? Parce que la monnaie ayant cours légal (le bolivar) est émise dans des quantités immenses qui la rendent hyperinflationniste. Autrefois, dans les pays dans lesquels sévissait l'hyperinflation, on changeait la monnaie nationale contre du dollar. Aujourd'hui, on

peut la changer contre du bitcoin. C'est plus simple et cela est moins facilement repérable par les autorités.

Le bitcoin est donc bien une monnaie. C'est une monnaie numérique rare. Elle est donc déflationniste comme l'or. Imaginons que la pénétration du bitcoin augmente. Son rythme d'émission va ralentir puis tomber à 0 (rappelons que le stock maximum de bitcoin est borné par la technologie à 21 millions d'unités). Le rythme de croissance du PIB mondial deviendra supérieur à la croissance du nombre de bitcoins, ce qui signifie que la valeur du bitcoin va augmenter ou, pour le dire autrement, les prix exprimés en bitcoins vont diminuer : c'est ce qu'on appelle la déflation. Les crypto-monnaies du type bitcoin, un peu comme l'étalon-or, nous font entrer dans un monde où toutes les valeurs nominales baissent, ce qui est facilité par le fait que les crypto-monnaies sont divisibles à l'infini. Quel changement de paradigme économique qui exigerait, pour que l'économie s'équilibre, une flexibilité maximale des prix et des salaires ! Nous sommes tous habitués à l'inverse.

III.1.c Crypto-monnaies, monnaies et banques centrales

« Le Bitcoin le montre clairement : s'il a peut-être été conçu comme un système de paiement alternatif hors de toute intervention gouvernementale, il associe aujourd'hui les caractéristiques d'une bulle, d'une pyramide de Ponzi et d'une catastrophe pour l'environnement[160]. » Le responsable de la Banque des règlements internationaux (BRI), Augustin Carstens, n'a pas été tendre avec le bitcoin lors d'une conférence à Francfort en février 2018, nouvelle preuve du schisme que génère la Blockchain.

Les positions des banques centrales à l'égard du bitcoin et des crypto-monnaies peuvent diverger entre elles. Mario Draghi confirmait fin 2017 que la Banque centrale européenne détenait le monopole de battre monnaie alors que le gouverneur de la Banque d'Angleterre, Mark Carney, parle du bitcoin comme d'une « révolution en puissance », notamment pour les marchés financiers, et n'exclut pas le lancement à terme d'une livre sterling « numérique[161] ». En réalité, on peut penser que leur position est relativement alignée. S'il apparaît difficile et paradoxal pour une banque centrale de soutenir ouvertement le bitcoin, il est également compliqué de ne pas souligner les vertus technologiques des protocoles sous-jacents en ligne avec la digitalisation de la monnaie. Cela ne signifie pas que les banques centrales vont nécessairement être rayées de la

160. Lien : https://www.letemps.ch/economie/bitcoin-une-bulle-un-montage-ponzi-un-desastre-environnemental. Dépêche AFP du 6 février 2018.
161. Raphaël Bloch, « Phénomène du Bitcoin : ce qu'en pensent les banques centrales », *Les Échos*, 30 novembre 2017. Lien : https://www.lesechos.fr/30/11/2017/lesechos.fr/030951241979_phenomene-du-bitcoin---ce-qu-en-pensent-les-banques-centrales.htm

carte, mais du moins que la Blockchain leur offre un formidable outil de modernisation. Le scénario d'une compétition durable avec les crypto-monnaies (bien réelles aujourd'hui, qu'elles soient autorisées ou non) pourrait s'installer, transformant cette opportunité de modernisation en nécessité d'attractivité accrue[162]. La plupart des banques centrales travaillent sur le sujet[163], certaines envisageant déjà la création de leurs « propres crypto-monnaies ».

La création d'une crypto-monnaie par une banque centrale pourrait reposer sur un protocole directement dérivé du Bitcoin, mais sa philosophie serait en réalité diamétralement opposée. Pour rappel, l'objectif principal de départ du protocole est la décentralisation. L'application de la technologie par une banque centrale (ou tout autre pouvoir centralisé) ne pourrait, par définition, se traduire que par davantage de centralisation, permise par des gains de compétitivité et une traçabilité accrue (aux mains du même pouvoir centralisé et non du réseau de façon plus ou moins anonyme comme sur la Blockchain publique). D'aucuns craignent de regretter le temps de l'argent liquide, et l'anonymat des besoins de consommation qu'il procure. Des gains de productivité et une traçabilité accrue auraient néanmoins pour mérite d'augmenter l'efficacité du système et de faciliter l'identification de l'origine des fonds, minimisant le risque de blanchiment ou de financement du terrorisme. Si elle peut poser question du point de vue des libertés individuelles (nous n'entrerons pas dans ce débat qui relève de la conviction personnelle), une telle initiative aurait également des conséquences structurantes pour le système macrofinancier et bancaire. La création d'une crypto-monnaie émise par une banque centrale reviendrait à donner un accès direct aux usagers à un compte hébergé par cette dernière, générant de fait une forme de désintermédiation des banques privées commerciales. Les banques assurent en effet à date l'interface entre les acteurs économiques et l'origine de la monnaie (aucun acteur privé non bancaire ne peut détenir directement un compte auprès de la banque centrale). Comme le mentionne le gouverneur de la Banque centrale japonaise, « l'émission de devises numériques au grand public reviendrait à ouvrir l'accès des banques de la banque centrale à tout le monde [nécessitant] d'abord de revoir le rôle et les prérogatives d'une banque centrale[164] ». Une chose est sûre, l'ampleur de cette conséquence induite doit être mesurée avant toute décision.

---

162. Huw Van Steenis, « La morsure du Bitcoin ou pourquoi les banques centrales devraient sévir contre les crypto-monnaies », *Les Échos*, 12 octobre 2017. Lien : https://www.lesechos.fr/idees-debats/cercle/cercle-174777-la-morsure-du-bitcoin-ou-pourquoi-les-banques-centrales-devraient-sevir-contre-les-crypto-monnaies-2121730.php.
163. Marie Charrel, « Les banques centrales ont-elles peur des cryptomonnaies ? », *Le Monde*, 17 mars 2018. Lien : www.lemonde.fr/economie/article/2018/03/17/les-banques-centrales-ont-elles-peur-des-cryptomonnaies_5272495_3234.html.
164. Raphaël Bloch, *op. cit.*

III.1.d Peut-on réellement se passer de banque centrale avec le bitcoin ?

Tel qu'évoqué par la journaliste du *Monde*, Marie Charrel, le rôle des banques centrales que nous connaissons ne se limite pas à leur fonction de maîtres du processus de création monétaire. À celui-ci s'ajoutent « la gestion des taux d'intérêt, de la liquidité, la supervision financière ou encore le rôle de prêteur en dernier ressort[165] ». En fait, le bitcoin se moque de ces aspects puisqu'il propose une vision orthogonale à celle-ci. Création monétaire mécanique gravée dans le code : nul besoin de gestion des taux d'intérêt ni de liquidité, ni même de supervision financière à effectuer ou de prêt en dernier ressort à octroyer. D'ailleurs le bitcoin n'est pas, contrairement à l'euro, une monnaie d'endettement.

Le « système », tel qu'il existe, et la politique économique menée ont bien des défauts ; trappe à liquidité, scénarios japonais, abondance extrême de liquidité avec un risque de bulle… Mais il est difficile d'imaginer ce qui se serait passé en 2009 si les banques centrales n'avaient pas injecté de la liquidité sur le marché interbancaire. Que se serait-il passé si la Fed n'avait pas mené de politique monétaire expansionniste *(quantitative easing)* ?

Certains auteurs et économistes considèrent les politiques monétaires menées comme la cause des cycles économiques (école autrichienne). « Dieu rit des gens qui déplorent les effets dont ils chérissent les causes », nous enseigne Bossuet. Un système monétaire plus fractionné, reposant sur des sous-ensembles restreints, serait selon ces thèses plus résilient. La Blockchain, en générant des écosystèmes autoportés mais interconnectés, s'inscrit parfaitement dans ce type d'argumentaire.

Du côté des pays développés, la perte de confiance dans l'économie, les pouvoirs en place et la monnaie officielle ne semble pas un sujet majeur (stabilité politique, élections libres, inflation maîtrisée…). Il n'est donc pas étonnant que les pouvoirs centralisés, garants de la stabilité et de la soutenabilité de l'économie et de la monnaie, soient *a minima* prudents envers le bitcoin et les crypto-monnaies. Au-delà de la défense de leurs prérogatives (et de leur activité-cœur), le risque de quitter la proie pour l'ombre et de sauter dans l'inconnu, alors que leur système n'apparaît pas en péril, peut être légitimement questionné. À partir de quelle capitalisation les crypto-monnaies représenteraient-elles un risque systémique ? Avec une capitalisation totale comprise entre 120 et 300 milliards de dollars ces six derniers mois, nous en sommes vraisemblablement loin.

---

165. Marie Charrel, *op. cit.*

Mais pourquoi utilise-t-on (certes encore modérément) le bitcoin en Europe et aux États-Unis si le facteur déclencheur semble être l'inflation ? Pour deux raisons. D'une part, parce que le dollar et l'euro sont aussi des monnaies inflationnistes, même si cette inflation n'est pas visible de tous. La mondialisation dans laquelle sont engagés ces pays et, plus particulièrement, la compétition avec les pays émergents maintiennent les prix des biens et des services à des niveaux relativement bas. L'inflation classique est donc quasiment éradiquée. Les augmentations de la masse monétaire, qui ont été massives après la crise financière de 2008, ont donc été absorbées, non par les prix des biens et des services, mais par les prix des actifs (financiers et immobiliers). C'est l'une des raisons pour lesquelles les prix des actions cotées sont aujourd'hui élevés et les taux d'intérêt de long terme (qui sont inversement proportionnels aux prix des obligations) sont bas, parfois proches de 0. Les personnes qui disposent d'un peu de culture économique et financière savent donc que, même chez nous, l'inflation existe. D'autre part, les États-Unis et la plupart des pays européens souffrent d'endettement public élevé. Les économistes évoquent à ce titre la notion « d'équivalence ricardienne ». L'idée sous-jacente est la suivante : quand les pouvoirs publics sont très endettés, les ménages anticipent des hausses d'impôt et épargnent en conséquence. Autrement dit, moins le public épargne, plus le privé le fait. Mais dans ce cas, autant le faire avec une épargne qui est invisible, et donc non taxable par les États. Les crypto-monnaies comme le bitcoin constituent des produits indiqués pour faire cela.

Pour un cerveau sensé, une admiration et une passion pour les possibilités nouvelles et infinies apportées par le Bitcoin, et d'autres Blockchains publiques, n'est donc pas incompatible avec la compréhension de la position prudente des régulateurs et banques centrales (tout comme leur intention d'utiliser la technologie sous-jacente pour être plus efficaces). Réfléchir à la Blockchain induit une forme de tiraillement intellectuel, entre admiration et réalisme, soif de renouveau et peur de l'inconnu.

La notion de confiance, supprimée entre les hommes par la Blockchain, est en réalité déplacée vers la technique elle-même. Pour effectuer une transaction en bitcoins, je n'ai pas besoin de faire confiance à ma contrepartie mais je dois avoir confiance dans la technologie et son fonctionnement. La monnaie revêt une caractéristique intrinsèque virtuelle puisqu'elle ne vaut que la valeur commune que ses utilisateurs lui accordent. Le bitcoin et le dollar seraient les unités de mesure de systèmes monétaires (voire de valeur) en compétition, dont la valeur refléterait la confiance relative que les usagers leur conféreraient. Dans cette perspective, le Bitcoin pourrait être vu comme un thermomètre de confiance dans le système et les monnaies traditionnelles. Si le contexte

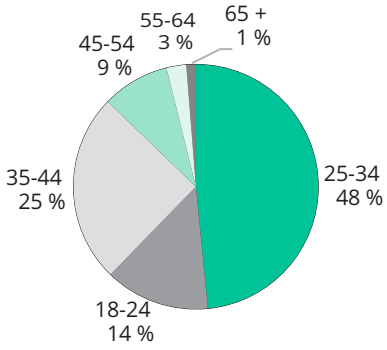
est aujourd'hui bien différent, rappelons que la création du bitcoin date de 2008 au cœur d'importants soubresauts, dans un climat de défiance.

III.2 La Blockchain : mode passagère ou espoir de développement économique ?

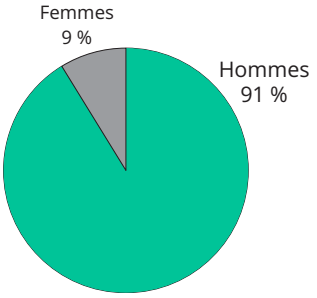
III.2.a Le Bitcoin est plutôt une affaire d'hommes, jeunes et occidentaux

Le Bitcoin et les Blockchains publiques sont souvent pensés avec le biais du regard occidental. Ils ne seraient qu'une folie passagère des jeunes générations et populations *trendy*, *digital friendly* européennes et américaines, attirées par l'appât du gain, la valeur de la norme sociale (effet de mode) et le « FOMO » (*fear of missing out* : peur de rater quelque chose). Ce stéréotype n'est d'ailleurs pas totalement invalidé dans les faits. L'analyse de la courbe de prix du bitcoin et de l'ensemble du marché des crypto-monnaies est très représentative des phénomènes de bulle. La trajectoire de prix du bitcoin suit par ailleurs une tendance comparable à celle du nombre de recherches du mot « Bitcoin » sur Google. Démographiquement, le bitcoin est effectivement plutôt l'affaire de jeunes hommes, en majorité dans les pays occidentaux (les États-Unis concentrent le plus grand nombre de transactions en bitcoins) et plutôt *geeks*[166].

RÉPARTITION DES USAGERS DU BITCOIN PAR CLASSE D'ÂGE EN DÉCEMBRE 2018[167]

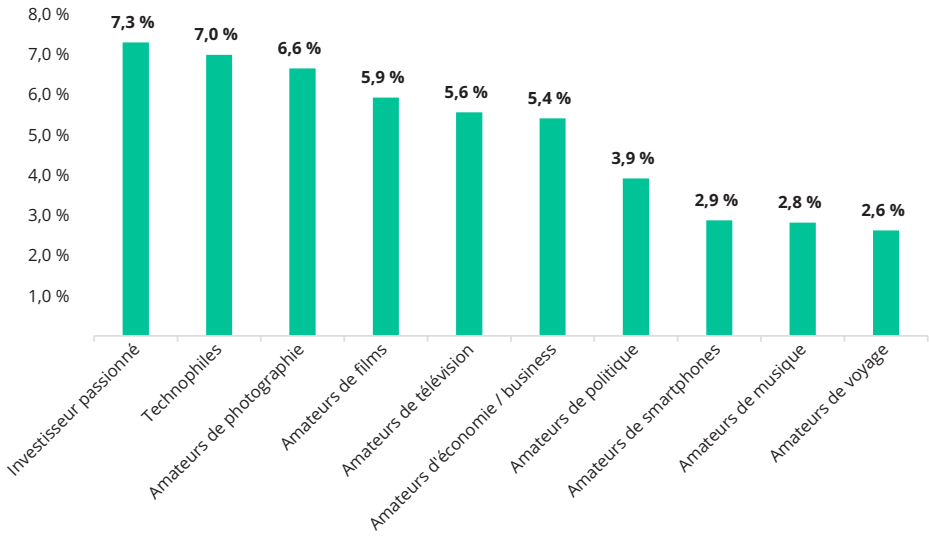


RÉPARTITION DES USAGERS DU BITCOIN PAR GENRE EN DÉCEMBRE 2018[168]

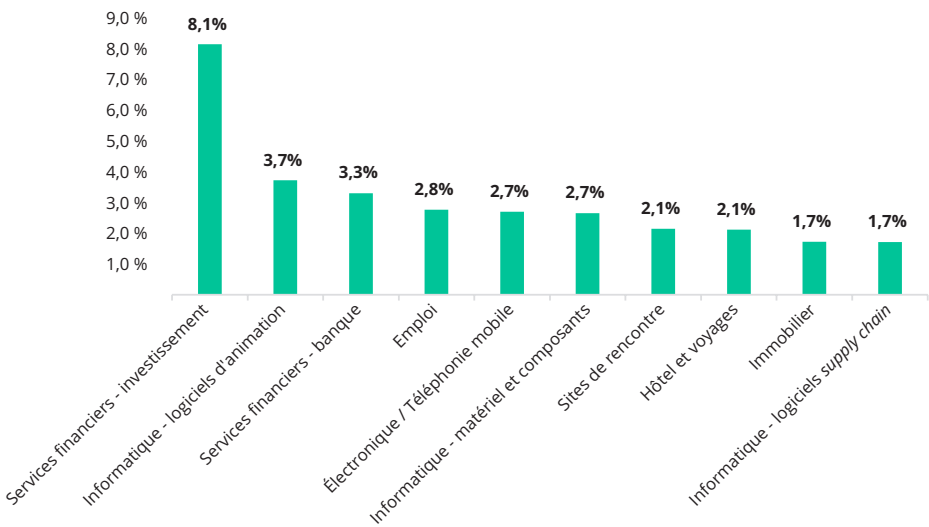


166. Source : Coin Dance.
167. Source : Coin Dance.
168. Source : Coin Dance.

RÉPARTITION DES USAGERS DU BITCOIN PAR PROFIL D'AFFINITÉS[169]



RÉPARTITION DES USAGERS DU BITCOIN PAR PROFIL SOCIOLOGIQUE[170]



169. Source : Coin Dance. Ce graphique et le suivant présentent les principaux profils d'usagers (supérieurs à 1 %). Les autres pourcentages, minimes, n'y seront pas représentés.
170. Source : Coin Dance.

III.2.b Dépasser le risque pour comprendre les enjeux

« Les problèmes auxquels est confronté le bitcoin à date sont limités face à ceux que connaissent les différents systèmes financiers en Afrique », selon Madame Rossiello, CEO de Bitpesa (Fintech africaine spécialisée dans le transfert d'actifs *via* Blockchain[171]).

Les crypto-actifs ne sont pas que l'affaire des pays développés

L'évolution relative du volume de transactions Bitcoin démontre certes la domination des États-Unis et du Royaume-Uni mais met également en exergue la large part des pays et zones en voie de développement (Nigeria, Asie du Sud-Est et Amérique du Sud notamment). Autre élément clé : en tendance, on observe une réduction de la part relative des États-Unis, au profit de la Russie notamment. La part relative des transactions est par ailleurs aussi importante en Asie du Sud-Est qu'en Europe (hors Royaume-Uni). Derrière chaque pays et chaque zone, se cache en fait un rationnel économique explicatif du volume de transactions en bitcoins (*a priori* davantage guidé par la réserve de valeur qu'il peut constituer que par sa valeur de transaction, mais les deux ne sont pas exclusifs).

Classiquement, les pays en voie de développement souffrent notamment de monnaies faibles, soumises aux taux de change internationaux et fragilisées par l'inflation, de capitaux et d'infrastructures limitées, de taux de bancarisation faibles (transactions essentiellement *cash*, peu d'épargne et de crédit), de flux de capitaux entre diasporas coûteux alors qu'ils constituent une part importante du PIB (transfert d'argent et contrôle des changes) et d'une gouvernance fragile et instable.

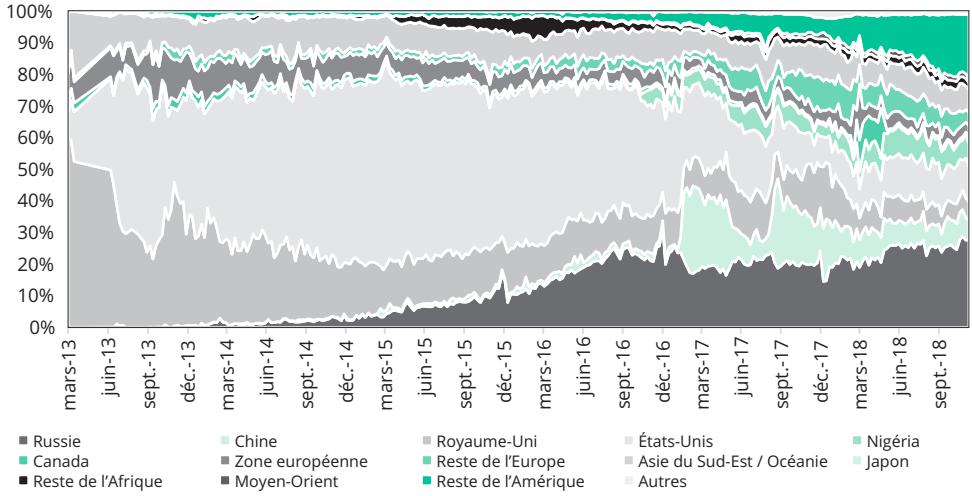
« Au Zimbabwe, les difficultés profondes du système financier traditionnel ont fait du bitcoin une alternative crédible », estime dès lors l'universitaire Lorenzo Fioramonti dans un article de *Quartz Africa*[172]. Ce lien direct peut-il être établi et généralisé ? Et en quoi la Blockchain peut-elle constituer une réponse à chacune de ces problématiques ?

---

171. Kyle Torpey (contributeur), « BitPesa CEO: Bitcoin's Issues Are Tiny Compared To The Problems With Banking In Africa », *Forbes*, 31 décembre 2017. Lien : https://www.forbes.com/sites/ktorpey/2017/12/31/bitpesa-ceo-bitcoins-issues-are-tiny-compared-to-the-problems-with-banking-in-africa/2/#47932b3636c4

172. Article de Lorenzo Fioramenti, professeur à l'université d'Heidelberg, juillet 2017. Lien : https://qz.com/1021155/bitcoin-is-being-taken-up-in-zimbabwe-nigeria-south-africa-and-venezuela-among-developing-countries/.

ÉVOLUTION RELATIVE DES TRANSACTIONS (VOLUMES) EN BITCOINS PAR ZONE GÉOGRAPHIQUE[173]



Les crypto-monnaies : des valeurs monétaires refuges ?

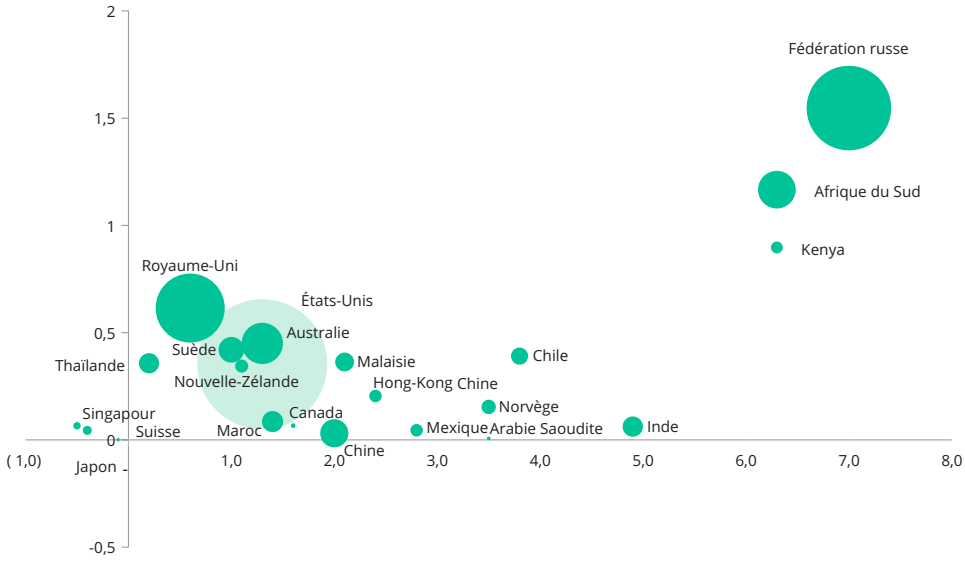
La comparaison géographique du volume de transactions par habitant (population de 2016) en bitcoins (2016) rapporté au PIB (PIB de 2015 ajusté en parité de pouvoir d'achat[174]) met en évidence la domination des États-Unis et le Royaume-Uni, mais également la présence en tête d'affiche de pays en voie de développement. La Russie, le Nigeria, l'Afrique du Sud et l'Argentine affichent par exemple des ratios de transactions très élevés : le volume moyen par habitant du Nigeria est par exemple supérieur à celui observé au Canada[175].

L'analyse géographique croisée entre le volume de transactions par habitant en bitcoins rapporté au PIB ajusté et le taux d'inflation sur l'année 2016 semble faire également apparaître une légère corrélation entre les deux facteurs. Il apparaît que le niveau d'inflation soit un facteur déclencheur du nombre de transactions en bitcoins. Lien fortuit ou logique économique ? On peut penser que l'émergence d'une monnaie alternative aux monnaies nationales revêt un attrait particulier pour un habitant d'un pays en développement, marqué par une gouvernance fragile et une inflation galopante.

---

173. Source : Coin Dance.
174. Volume absolu / (population * PIB par tête du pays / PIB par tête du monde).
175. Données économiques : source Banque mondiale. Données Bitcoin : source Coin Dance. Lien : https://coin.dance/volume/localbitcoins

POSITIONNEMENT DE PAYS EN FONCTION DU VOLUME DE TRANSACTIONS EN BITCOINS PAR HABITANT (EN PARITÉ DE POUVOIR D'ACHAT) ET DE L'INFLATION



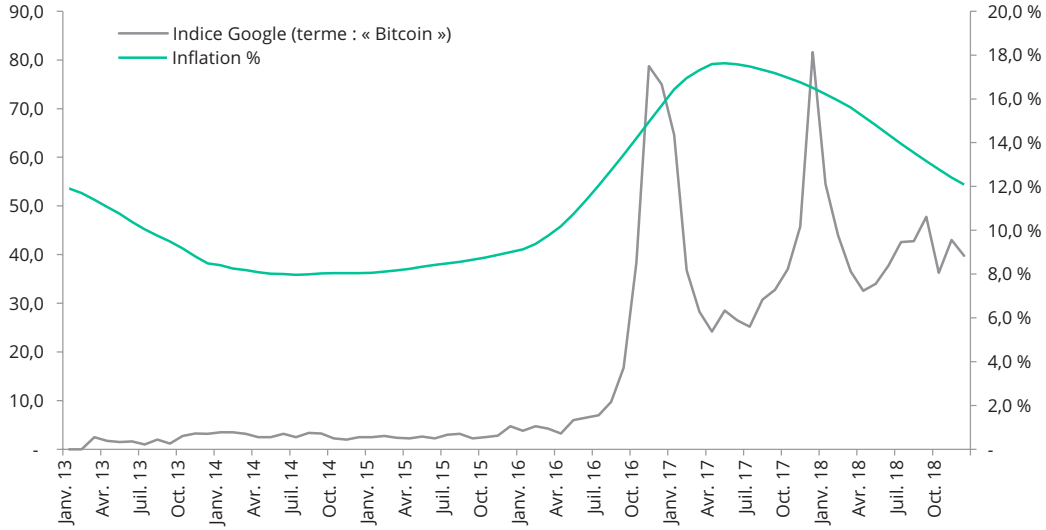
Prenons l'exemple du Nigeria et de la Russie. La comparaison entre l'évolution du taux d'inflation au Nigeria et la popularité relative de la recherche du mot « Bitcoin » sur Google (indice Google[176]) permet d'identifier un bond des deux grandeurs au même moment. Le Nigeria, ex-première puissance africaine, s'enfonce depuis 2016 dans une crise économique majeure, expliquée par la chute des prix du pétrole dans une économie dépendante à 70 % de l'or noir, sur fond de crise politique et sécuritaire (attaques régulières d'installations pétrolières par des factions rebelles[177]). La baisse des exportations s'est traduite par un recul majeur des entrées de devises, avec pour conséquence l'effondrement du taux de change. Ces difficultés ont entraîné un quasi-doublement de l'inflation entre janvier 2016 (moins de 10 %) et avril 2017 (près de 18 %). De mars à octobre 2016, l'indice Google explose et passe de presque 0 à

176. Indice Google : les valeurs sont calculées sur une échelle de 0 à 100, où 100 représente le pays dans lequel la popularité est la plus importante, exprimée en fraction du nombre total de recherches.

177. Le Monde.fr – AFP, 21 novembre 2016, 17 h 14. Lien : www.lemonde.fr/afrique/article/2016/11/21/la-crise-economique-s-installe-au-nigeria_5035376_3212.html#Kv34xjTmJAIxbwcP.99

80 en quelques mois[178]. Les Nigérians auraient-ils compté sur le bitcoin pour protéger leur épargne et garantir leur capacité à régler des biens et services sur les marchés internationaux ?

ÉVOLUTION RELATIVE AU NIGERIA DE L'INDICE GOOGLE (TERME : « BITCOIN ») ET DE L'INFLATION

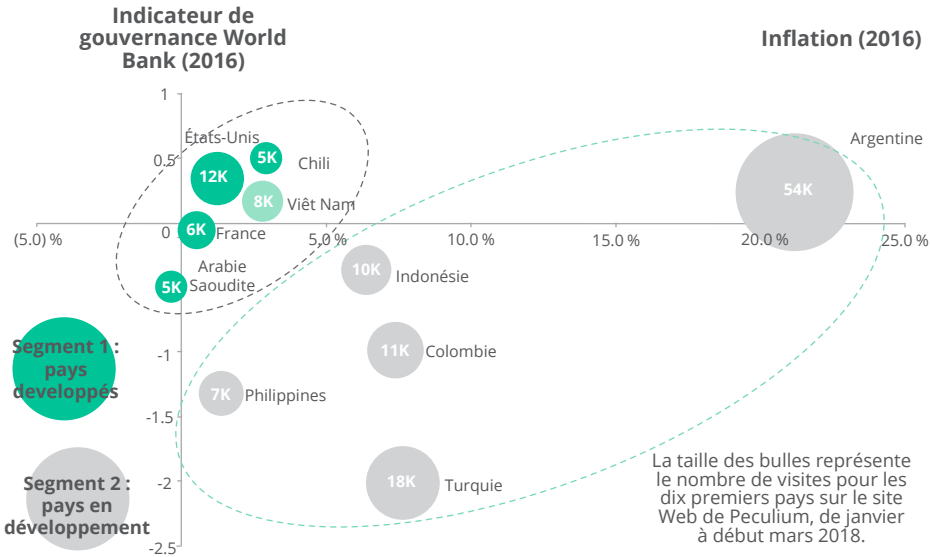


La start-up Peculium est un exemple d'initiative dans le domaine de l'épargne de crypto-actifs basée sur l'Intelligence Artificielle. La distribution du nombre de visites sur leur site Internet entre le 1er janvier et le 8 mars 2018[179] est édifiante d'un point de vue stratégique et segmentation client. Les 216 000 visites se répartissent en deux groupes : les pays développés et le Viêt Nam et les pays en voie de développement. Pour les pays développés, la demande semble guidée par un besoin de rendement retrouvé et d'innovation dans le domaine de la gestion d'actifs. Pour les pays en développement, l'intérêt pour Peculium semble en revanche répondre à un besoin de sécurisation de l'épargne alternative au système monétaire du pays considéré, fragilisé par une inflation forte[180] et/ou une gouvernance instable[181]. L'Argentine, avec un

178. Une valeur plus importante signifie une plus grande proportion de recherches et non une valeur absolue plus importante.
179. Source : Google analytics.
180. Source : Banque mondiale.
181. Illustrée par l'indicateur de gouvernance de la Banque mondiale (agrégat constitué à partir de six dimensions : responsabilité, stabilité politique, absence de violence et de terrorisme, efficacité du gouvernement, qualité de la régulation, État de droit et applicabilité de la loi, contrôle de la corruption).

taux d'inflation de plus de 20 % en 2017 représente par exemple le principal foyer de visites (54 000 visites du 1er janvier au 8 mars 2018).

CARTOGRAPHIE DU NOMBRE DE VISITES SUR LE SITE DE PECULIUM PAR ZONE GÉOGRAPHIQUE EN FONCTION DE L'INDICE DE GOUVERNANCE DE LA BANQUE MONDIALE ET DE L'INFLATION



Des valeurs refuges et/ou un moyen de contournement du contrôle des changes ?

L'argumentaire précédent suggérait un besoin de réserve de valeur, mais il est en réalité difficile de statuer sur les réelles motivations de ces mouvements. Il est probable que des opérations soient réalisées dans le but de contourner les contrôles des changes en place dans certains pays.

Par exemple, l'économie vénézuélienne souffre d'une problématique d'inflation et de change quasi structurelle. Les dollars sont distribués au compte-gouttes dans un contexte de multiples taux de change (taux de change clandestin, taux de change étatiques…) et l'inflation galopante fragilise l'épargne et les salaires. Nul doute que des solutions permettant de transférer de façon plus ou moins anonyme des bolivars en dollars à des taux de marché plutôt qu'à des taux fixés arbitrairement par l'État, trouvent leur public.

La start-up Air Tm[182] s'est par exemple spécialisée dans la démocratisation et la simplification de l'accès aux monnaies fortes pour les investisseurs et particuliers résidant dans des pays à fort contrôle de change et forte inflation, comme le Mexique ou le Venezuela. La start-up revendique 168 000 utilisateurs vénézuéliens résidents et 40 000 à l'étranger. Récemment, elle a noué un partenariat avec Zcash, une crypto-monnaie entièrement anonyme, mais l'utilisation semble faible si l'on en croit le même article de Coindesk (500 utilisateurs de Zcash ont réalisé un total de 1 000 transactions du 8 mars au 9 avril 2018[183]).

En synthèse, la Blockchain semble répondre à des besoins très différents dans les pays occidentaux et dans les pays en développement. Pour les premiers, sa valeur est assurément plus incrémentale que pour les seconds, puisqu'elle s'inscrit davantage dans la continuité du mouvement – certes puissant – de digitalisation et de mode autour de l'innovation, que dans une velléité généralisée de contester des pouvoirs centralisés plutôt efficaces. Dans les pays en développement, elle semble de fait constituer une alternative à l'épargne monétaire nationale rongée par l'inflation et un moyen d'échapper au contrôle des changes. Par des coûts réduits, grâce à la technologie, et une accessibilité accrue, la Blockchain offrirait des solutions démocratisées de gestion d'actifs.

Des biens communs pour des pays limités en capital fixe ?

Selon les théories classiques, le développement d'une économie repose sur sa capacité à maximiser ses facteurs de production : travail, capital, investissement. L'accumulation de capital fixe et de connaissances est donc au cœur de l'économie du développement. Le modèle de Barro[184] (1990) suppose par exemple que les dépenses d'infrastructures ont un effet positif sur la productivité, de même que la connaissance. Les dépenses d'infrastructures généreraient un cercle vertueux, le renforcement des facteurs consolidant la production au service de l'accumulation de capital, lui-même réinvesti en infrastructures. Les connaissances, quant à elle, permettent d'accroître la productivité, et donc de faire progresser la production à infrastructures constantes, avec un impact naturel sur le capital accumulé. Cette économie de la connaissance génère des équilibres multiples marqués par un schisme entre les pays riches qui ont activé le cercle vertueux (la connaissance favorise la production, qui renforce l'accumulation du capital et l'investissement en infrastructures)

182. Lien : https://www.airtm.io
183. Lien : https://www.coindesk.com/anti-petro-zcash-throwing-venezuelans-lifeline/, Michael del Castillo, 9 avril 2018.
184. R. Barro, « Government spending in a simple model of endogenous growth », *Journal of political economy,* 1990. Il s'agit ici d'un exemple d'écrit sur ce sujet, les travaux sur ce point sont nombreux et vastes.

et les pays pauvres. Ces derniers souffrent de ce que Barro appelle « la trappe à pauvreté ». Dans ce modèle, l'État doit jouer un rôle d'amorçage, en stimulant l'apprentissage par le biais de l'investissement en capital fixe. Avec un investissement massif, la production peut croître et l'expérience progresser au service de gains de productivité, permettant de sortir de la trappe à pauvreté et de s'inscrire dans le cercle vertueux présenté précédemment. Les aides au développement des institutions internationales s'inscrivent d'ailleurs dans cette logique, en finançant des infrastructures massives, point d'ancrage du développement.

Le Bitcoin remettrait-il en cause la théorie de la trappe à pauvreté en représentant une forme de bien commun, produit et gouverné par l'initiative privée ? De manière générale, le Bitcoin et la Blockchain publique s'inscrivent en ligne avec l'économie collaborative, structurée autour de l'*open innovation*. Le code Bitcoin, de même que celui d'Ethereum sont *open source*, téléchargeables et modifiables. L'utilisation du code en lui-même est donc gratuite.

Le protocole Bitcoin *open source* a été développé par une initiative privée. Les dépenses nécessaires au fonctionnement du Bitcoin n'ont nécessité aucun apport étatique ni aide d'institutions internationales. L'investissement de départ, majoritairement de la R & D (recherche et développement) et donc du temps humain, a été supporté par ses créateurs qui ont mis à disposition du monde une solution permettant les échanges décentralisés (leur rémunération provient de l'appréciation du bitcoin dont ils ont retenu une part lors de sa mise en circulation).

Les frais de maintenance sont naturellement assurés par la communauté détentrice de bitcoins, intéressée à sa survie. Les coûts de fonctionnement du Bitcoin sont quant à eux atomisés et diffus, construits de façon décentralisée. Les mineurs (les acteurs qui valident et sécurisent les transactions) décident librement de commencer cette activité ; ils en reçoivent les gains mais en assument les coûts (dépenses d'investissement en matériel informatique pour accéder au réseau et résoudre les algorithmes et dépenses courantes d'électricité). En d'autres termes, un Nigérian qui réaliserait une transaction en bitcoins ne supporterait aucun coût d'infrastructure, et n'engagerait que des coûts de transaction n'intégrant à aucun moment l'amortissement des coûts fixes liés à la mise en place du protocole. Sa transaction peut être validée par un mineur chinois à l'autre bout du monde, mais disposant de capital mis à disposition d'un projet d'investissement (ferme de minage).

Ce prisme macroéconomique du développement met une fois de plus en lumière le génie d'alignement d'intérêts du système Bitcoin. Tous les acteurs ont intérêt à agir individuellement comme ils le font, au service rationnel de l'intérêt commun d'un écosystème mondial autorégulé.

Les créateurs l'ont développé pour maximiser leurs gains par l'appréciation du bitcoin, les mineurs sont des producteurs classiques guidés par la recherche de rentabilité, et les utilisateurs, des consommateurs qui exploitent librement un service. Le tout avec un minimum de coûts de friction. Le protocole Bitcoin est mondial, et la seule condition pour accéder à la Blockchain est d'avoir un accès Internet.

Là encore, l'intérêt de la sphère économique sur le sujet est croissant. Selon Sinclair Davidson, Primavera De Filippi et Jason Potts, le Bitcoin et la Blockchain constituent des biens communs de 3e génération[185], dans la continuité des travaux de Oliver Williamson et Elinor Ostrom[186]. Comme relayé par Guillaume Holland et Omar Sene dans la *Revue d'économie politique* en 2010, Elinor Ostrom démontre « comment les copropriétés peuvent être efficacement gérées par des associations d'usagers », en remettant en question « l'idée classique selon laquelle la propriété commune est mal gérée et doit être prise en main par les autorités publiques ou le marché[187] ». Dans cette perspective, le Bitcoin serait un exemple type d'une association d'usagers gérant efficacement une propriété commune (celle du protocole).

Les écrits de Darcy Allen[188] inscrivent également le rôle de la Blockchain dans l'économie du développement, dans la continuité des thèses des économistes émettant des doutes quant à la pertinence du rôle de l'État dans le développement. L'auteur cite notamment William Easterly qui caractérisait par exemple en 2006 la théorie du *big push* (à savoir la logique d'amorçage de l'État par l'investissement) de légende. L'État et toute autre forme de planification centralisée du capital ne permettraient pas une allocation efficiente des ressources dans un contexte d'asymétrie d'information. D'après Darcy Allen, l'étude de l'économie du développement a évolué vers l'incorporation du rôle de l'action privée ; dans la continuité des travaux de l'école autrichienne (Mise) et plus précisément de la théorie de l'entrepreneuriat (Kirzner : l'entrepreneur vigilant découvre des opportunités étrangères aux acteurs précédents[189]). La mise en réseau d'acteurs entrepreneuriaux décentralisés pourrait donc permettre, selon ces thèses, en rupture ou en complément des planificateurs centralisés, de coordonner efficacement l'information imparfaite diffuse.

---

185. Davidson, de Filippi, Potts, *Economics of Blockchain*, mars 2016. Lien : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751

186. Ces travaux lui vaudront le prix Nobel d'économie en 2009.

187. Guillaume Holland, Omar Sene, « Elinor Ostrom et la gouvernance économique », *Revue d'économie politique*, 2010/3, vol. 120, Dalloz. Lien : https://www.cairn.info/revue-d-economie-politique-2010-3-page-441.htm

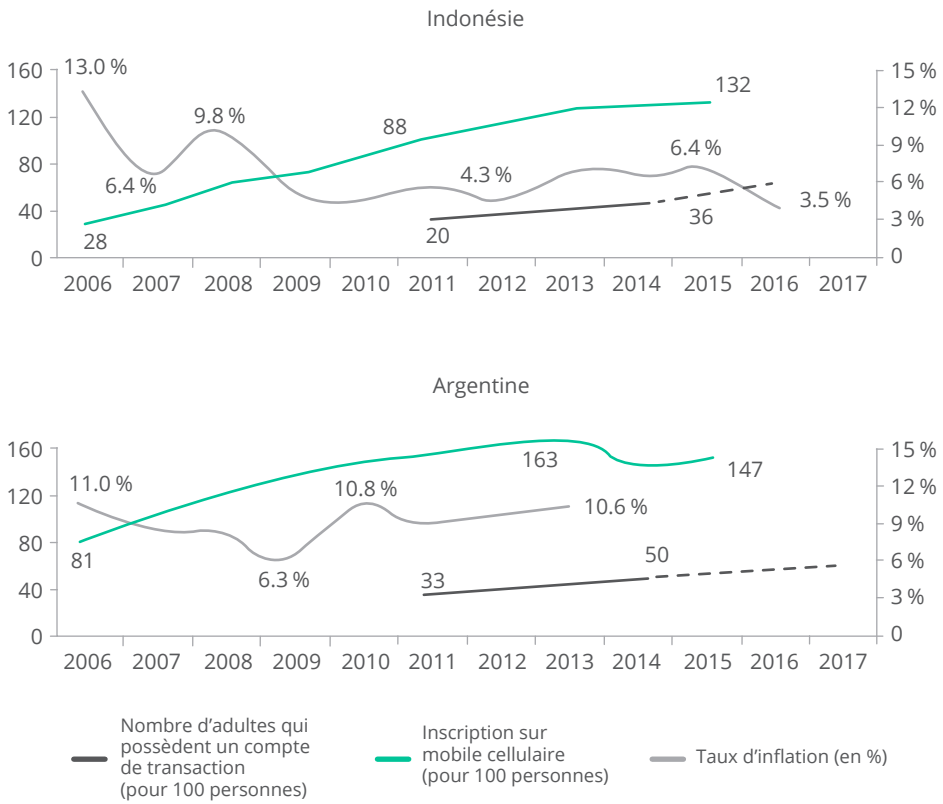
188. Darcy Allen, « Discovering and developping the Blockchain cryptoeconomy », extrait d'un chapitre de sa thèse à l'université de Melbourne : *The private governance of entrepreunership : an institutional approach to entrepreunarial discovery*. Lien : researchbank.rmit.edu.au/view/rmit:162196

189. Résumé sur www.econ.nyu.edu/user/kirzner/

Le téléphone mobile, moyen d'accès privilégié aux services financiers dans les pays en développement

La vague de Fintech qui s'est abattue dans les pays occidentaux est également d'une grande ampleur dans les pays en développement. Depuis plusieurs années, ces derniers représentent un gisement de valeur majeur dans les télécommunications. En affichant des taux de pénétration supérieurs à la bancarisation dans de nombreux pays en développement, le mobile est devenu un véritable point d'ancrage de l'accès massif aux services financiers, souvent en dehors des banques. La comparaison de l'évolution des taux de détention de smartphones et de bancarisation est en effet édifiante, présentée ici avec l'exemple de deux pays actifs dans le domaine de la Blockchain : l'Indonésie et l'Argentine.

ÉVOLUTION RELATIVE DE L'INFLATION, DU TAUX DE BANCARISATION ET DU TAUX D'ÉQUIPEMENT EN SMARTPHONES[190]



190. Source : Banque mondiale. Les pointillés représentent une extrapolation réalisée par nos soins.

En Afrique, où le mouvement est particulièrement marqué ; le trafic des données mobiles a crû de 96 % en 2016[191]. Selon le rapport « 2017 Mobile Economy report », élaboré par GSMA, le nombre d'utilisateurs de mobiles devrait s'établir autour de 500 millions en 2020. Selon GSM Intelligence, le taux de pénétration en abonnements mobiles s'élevait à près de 50 % en Afrique de l'Ouest en 2016[192]. Les applications pair-à-pair *via* mobile en Afrique sont, sans utiliser la Blockchain, déjà fonctionnelles, puissantes et significativement implantées. L'entreprise M-Pesa en est un très bon exemple. Leader kenyan en la matière (transactions, dépôts, microcrédits), elle répond à un besoin de transfert d'argent simplifié et rapide. « L'idée, explique Ronald Webb [dans un article de *Jeune Afrique*], directeur des services financiers chez Safari.com[193], c'était de permettre à quiconque possède un téléphone Safari.com d'envoyer de l'argent rapidement et surtout très simplement[194]. » L'application M-Pesa, adossée au réseau Telecom safari.com, comptabilise plus de 20 millions d'utilisateurs au Kenya soit un taux de pénétration de près de 70 % dans la population adulte. L'article de *Jeune Afrique* souligne également le processus de digitalisation de l'économie kenyane autour de M-Pesa : plusieurs enseignes de supermarché, auto-écoles, restaurants, la compagnie nationale d'électricité, permettent désormais à leurs clients d'effectuer leurs paiements directement *via* leur mobile. Le CEO de M-Pesa, Bob Collymore, prétend contribuer à hauteur de 6,5 % au PIB du Kenya. Le succès de l'entreprise tient à sa solution mobile digitale mais aussi à son réseau de distribution (agents) dans les zones rurales, permettant de retirer et déposer de l'argent sur son compte mobile.

La Blockchain s'inscrit dans la continuité des innovations portées par les Fintech

Plusieurs sociétés ont répliqué des modèles similaires en capitalisant sur la Blockchain. C'est le cas par exemple de Bit Pesa (créée en 2015), société kenyane spécialisée dans le transfert d'argent international, principalement à destination des petites entreprises à l'import et à l'export. Bit Pesa est une plateforme d'échange permettant le transfert d'argent *low cost* (frais limités à 3 %) vers et depuis l'Afrique par l'intermédiaire du Bitcoin. La société semble poursuivre un développement intéressant et revendique plus de 6 000 utilisateurs et la réalisation de plus de

191. Rapport Cisco cité par Marie Lechapelays (contributrice au *Monde Afrique*), décembre 2017. Lien : www.lemonde.fr/afrique/article/2017/12/01/au-nigeria-le-bitcoin-peut-il-devenir-une-alternative-au-naira_5223367_3212.html#KwjumEpHVM6bSooA.99

192. Lien : https://www.gsmaintelligence.com/research/?file=3e55719316df52c7235492095174949f&download

193. Réseau Telecom kenyan.

194. Laure Broulard, Mark Anderson, « *Mobile banking* : une *success-story* nommée M-Pesa », *Jeune Afrique,* 3 avril 2017. Lien : www.jeuneafrique.com/mag/421063/economie/mobile-banking-success-story-nommee-m-pesa/

17 000 transactions *via* Blockchain[195]. La pertinence du modèle est également illustrée par plusieurs levées de fonds : notamment 1,10 million d'euros auprès du fonds de capital-risque californien Pandera Capital[196] et plus récemment 10 millions d'euros auprès de Greycroft Partners[197].

Fait marquant, alors que l'on aurait pu s'attendre à une compétition entre M-Pesa et Bit Pesa, cette dernière s'est appuyée en réalité sur le réseau d'agents et les solutions mobiles de M-Pesa. Les premiers mouvements de bitcoins sur le corridor UK-Kenya se traduisaient en effet par un versement en schillings kenyans sur le mobile équipé d'un compte M-Pesa faisant office de portefeuille digital[198]. Cet exemple de coopération entre Fintech et Blockchain illustre la recomposition du paysage des services financiers en cours. Le Bitcoin et d'autres Blockchains ne sont en fait pas complètement autoportants en l'état : accès parfois complexe, peu de débouchés en bitcoins nécessitant des conversions additionnelles, plates-formes souvent adossées à des comptes en banque. Les acteurs qui émergent constituent donc des nouvelles formes d'intermédiaires au service du développement et de l'accès aux services financiers.

Ce marché du transfert d'argent représente plus de 500 milliards de dollars en 2017, soit plus de trois fois le montant total des aides au développement. Il ne constitue pas un marché mondial et obéit à des dynamiques complexes. Il apparaît ainsi segmenté en « corridors » correspondant à des flux de devises pendulaires, miroir des équilibres migratoires entre les pays. Chaque corridor répond à des mécanismes différents (profils socioprofessionnels différents, accès différenciés à la technologie, montants transférés hétérogènes…) avec pour effet des coûts de transfert très divers en fonction des zones considérées. Le transfert d'argent est intuitivement directement adressable par la Blockchain, en concurrence des acteurs majeurs : postes, banques, opérateurs mobiles et *pure players*[199] (Western Union, Moneygram et Ria, qui représenteraient plus de 25 % du volume annuel de ce type d'échanges[200]).

---

195. Oliver Dale, « Cryptocurrencies and developing countries », décembre 2017. Lien : https://blockonomi.com/cryptocurrencies-developing-countries/.
196. Aaron van Wirdum, « BitPesa raises 1.1 millions de dollars », *Daily Digest*, 10 février 2015. Lien : https://cointelegraph.com/news/daily-digest-hong-kong-issues-bitcoin-warning-russia-reconsiders-stance-and-bitpesa-raises-us11-million
197. Laura Shin, « Bitcoin payment firm BitPesa secures Greycroft as lead investor for 10 millions of euros total funding », *Forbes*, 30 octobre 2017. Lien : https://www.forbes.com/sites/laurashin/2017/08/30/bitcoin-payments-firm-bitpesa-secures-greycroft-as-lead-investor-for-10-million-total-funding/#204a63486066
198. Daniel O. Nyairo, « Kenya adopts Bitcoin with Bitpesa, Tagpesa and M-pesa », 7 mars 2015. Lien : https://cointelegraph.com/news/kenya-adopts-bitcoin-with-bitpesa-tagpesa-and-m-pesa
199. Massimiliano Varrucciu, « *Bitcoin and remittance: where are we?* », 6 juillet 2017. Lien : https://www.fintastico.com/blog/bitcoin-and-remittance-where-are-we/
200. Luis Bonaventura, septembre 2016. Lien : https://qz.com/775159/theres-a-500-billion-remittance-market-and-bitcoin-startups-want-in-on-it/

L'Asie concentre des corridors de transfert particulièrement actifs, liés à la nécessité pour les habitants d'exporter leur force de travail au plus offrant dans un contexte de bancarisation limitée (moins de 25 % en moyenne[201]). À titre d'exemple, l'Inde (62,7 milliards de dollars), la Chine (61 milliards de dollars), les Philippines (29,9 milliards de dollars) et le Pakistan (19,8 milliards de dollars) composent le top 5 des destinations de transfert en 2016 (le Mexique occupe la 4e place[202]). Le continent, et en particulier l'Asie du Sud-Est, représente par conséquent naturellement un foyer d'initiatives et d'usagers Blockchain important. Les start-up asiatiques Rebit, Bloom (transferts instantanés vers les Philippines et le Viêt Nam) et coins.ph (Philippines) en sont de bonnes illustrations et proposent des solutions de transfert d'argent sur des corridors précis, par l'intermédiaire de la Blockchain et de crypto-monnaies. Là encore, à l'image de Bit Pesa, il ne s'agit pas d'initiatives purement Blockchain, mais de Fintech exploitant les crypto-monnaies. La Blockchain promet également d'apporter davantage d'inclusion financière dans le crédit. En combinant l'alignement d'intérêt grâce aux *tokens*, l'effet de réseau et les *Smart Contracts*, des initiatives Blockchain entendent disrupter le microcrédit de façon efficiente. Les projets Bloom et We Trust en sont de bons exemples.

Le *business case* de We Trust, par exemple, est une bonne synthèse de ce que peut promettre la Blockchain par la combinaison de sa puissance technologique, de l'alignement d'intérêts et, en l'espèce, de la micro-finance. We Trust propose entre autres la création de *Trusted lending circles* (cercles de confiance pour le crédit) dans lesquels des intervenants vont librement faire circuler du capital entre eux (épargne et crédit). Ce mécanisme, capitalisant sur le levier de réputation personnelle, existe depuis des années. Il s'agit en réalité d'une ROSCA *(Rotative Savings and Credit Association)*, format digital.

Préalablement le système était ingénieux d'un point de vue financier et déjà plutôt répandu. L'économiste Bouman faisait en état en 1977 du fait que la ROSCA représentait entre 8 et 10 % du PIB éthiopien. En 1995, il estimait à plus de la moitié la part de la population rurale camerounaise utilisant ce système[203].

Le déploiement à grande échelle restait néanmoins complexe, et la transition vers la bancarisation plus traditionnelle longue et difficile. Avec sa solution, We Trust propose une industrialisation à grande échelle de la microfinance en capitalisant sur la réputation personnelle au sein de communautés. Concrètement, des individus qui souhaitent

201. Source : Banque mondiale.
202. Source : Banque mondiale.
203. Beatriz Armendariz, Jonathan Morduch, *The Economics of Microfinance*, MIT Press, 2005.

financer l'acquisition d'un même objet, créent une communauté dont ils définissent les règles (nombre de tours par mois, tickets par personne) inscrites dans une série de *Smart Contracts*. À chaque tour, chaque personne place la même somme d'argent ; le total de l'argent placé à chaque tour est attribué aléatoirement à l'un des membres du groupe créé. Cette méthode permet de rendre possible de façon sécurisée la réalisation de microcrédits et micro-épargne par l'intermédiaire de la Blockchain et des *Smart Contracts*. On peut imaginer que les individus pourront développer, à l'usage, des formes de notations, générées par leur comportement dans les différentes communautés éphémères auxquelles ils appartiendront (théorie des jeux répétés). Cela permet d'une certaine manière de mondialiser la réputation personnelle et de créer des groupes entre des individus très éloignés à plusieurs égards.

Les membres de ROSCA digitales pourraient-ils ensuite se prévaloir de la notation obtenue par ce système parallèle auprès de banques traditionnelles – dont ils auraient été exclus à la base – en limitant de ce fait l'asymétrie de l'information ? Cette hypothèse représenterait un bon exemple de l'inclusion financière, renforcée par la Blockchain, dans une logique de coopération entre les anciens et les nouveaux acteurs.

L'impact de la Blockchain dépasse la sphère économique et financière

Grâce aux mécanismes d'enregistrement sécurisé d'opérations de toute nature, de traçabilité et d'immuabilité des informations stockées, mais aussi aux *Smart Contracts*, la Blockchain est également source de valeur indirecte pour le développement économique.

En effet, elle peut permettre de sécuriser le cadre général et ainsi favoriser la croissance. Parmi les indicateurs clés retenus par la Banque mondiale, dans son indice de qualité de la gouvernance étatique, figurent notamment la stabilité politique, l'absence de corruption, la force de l'État de droit et l'efficacité du gouvernement.

La technologie peut être un moyen utile de démocratisation et de limitation de la corruption, grâce notamment à la possibilité d'opérer des votes par l'intermédiaire de la Blockchain. À titre d'exemple, la Sierra Leone a récemment réalisé des élections de cette façon[204].

204. Lien : https://www.google.fr/amp/s/www.coindesk.com/early-returns-sierra-leones-first-Blockchain-vote/amp/

Plusieurs initiatives permettant de garantir la propriété privée, notamment terrienne, ont également vu le jour, avec pour vocation de lutter contre l'expropriation. Le réseau Innocherche (réseau de veille en innovation à destination des dirigeants) estime à 10 % le pourcentage des terres dûment enregistrées en Afrique, 7 % pour la Grèce. Ce mauvais enregistrement induit un risque d'expropriation mais également une situation sous-optimale (terres non exploitées, collatéraux sous-estimés[205]…). L'économiste péruvien Hernando De Soto estime, dans des propos relayés par un article de *Forbes* en février 2017, le montant total des *dead assets* (c'est-à-dire des actifs n'étant pas juridiquement reliés à une personne morale ou physique) à plus de 20 000 milliards de dollars. L'impossibilité de falsifier des documents officiels est donc un atout majeur contribuant à une sécurité juridique accrue permise par la garantie absolue et indélébile du lien de propriété entre un individu et une chose. Le même article nous apprend d'ailleurs que la Géorgie a lancé un projet visant à utiliser le réseau Bitcoin pour valider certaines transactions impliquant le gouvernement[206].

Les possibilités sont nombreuses, tant sur l'efficacité de l'administration que sur les *civictech* (impact de la technologie sur la manière de gérer les droits civiques). Plusieurs zones sont leaders en la matière, dont notamment le canton de Zug, en Suisse, et l'Estonie[207]. Cette dernière est classée deuxième dans l'indice de progrès social[208]. Plusieurs acteurs adressent également ce marché florissant de la modernisation de l'État autour de la Blockchain ; c'est notamment le cas de la start-up parisienne 97 Network.

III.3 La Blockchain : quels facteurs clés de succès sur le plan économique ?

Le Bitcoin et la Blockchain ne peuvent toutefois pas suppléer à l'ensemble des infrastructures nécessaires au développement : autoroutes, réseaux électriques et Internet… Si le bitcoin est très utilisé par le Nigeria (ancien champion africain en crise), son développement dans les pays les plus pauvres, trop peu dotés en infrastructures de base, est

205. Lien : http://innocherche.com/la-Blockchain-pour-resoudre-les-grands-problemes-du-monde/
206. Laura Shin, « The first government to secure land titles on the Bitcoin Blockchain expands project », 8 février 2017. Lien : https://www.google.fr/amp/s/www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-Blockchain-expands-project/amp/
207. Don et Alex Tapscott, *Blockchain Revolution*, Portfolio Penguin, 2016.
208. Socialprogressimperative.org

plus compliqué. Le bitcoin ne vit pas en parfaite lévitation et nécessite *a minima* un accès Internet, dont près de la moitié de la population est toujours exclue. Mais ce constat pourrait changer : le projet *Loon* de Google a par exemple pour ambition de fournir un accès Internet aux populations les plus reculées, grâce à un réseau de ballons circulant à la limite de l'espace[209].

Par ailleurs, il faut rappeler ici que tout n'est pas « blockchainisable ». Il ne faut pas « voir de la Blockchain partout » et chercher à forcer l'application de la technologie dans tous les *business models*. Certes, les possibilités sont immenses, mais le succès des modèles proposés dépend de rationnels simples, qui restent les mêmes que dans l'économie traditionnelle. Le Bitcoin et la Blockchain revêtent une valeur quasi mystique, philosophique, identitaire et spéculative pouvant néanmoins décorréler la réalité économique pure du succès observé. Que la Blockchain émerge en tant que substitut ou complément à l'économie traditionnelle, de façon plus ou moins décentralisée, elle est et restera mise à l'épreuve des faits, du marché et de la réalité économique. Son succès dépend d'une demande, ce constat simple mérite d'être rappelé : les technologies brillantes n'ayant pas trouvé leur public sont nombreuses. Quelle valeur ajoutée, *in fine* ? De façon générale, il apparaît clair que la transition dans les pays développés prendra du temps, tant la mutation à opérer est profonde : la Blockchain doit démontrer que les gains espérés dépassent les coûts de changement. Dans les pays émergents, le constat diffère, puisque la concurrence des infrastructures existantes est beaucoup plus limitée pour des raisons évidentes.

Reste à savoir si le bitcoin est vraiment compétitif en termes de coûts et d'usage. Contrairement aux idées reçues et raccourcis qui sont monnaie courante, la compétitivité du prix du bitcoin n'est pas acquise dans l'absolu et nécessite une analyse au cas par cas. Prenons (encore) le cas du marché des transferts d'argent. Combien coûte une transaction en bitcoins pour un consommateur ? Son coût n'est pas stable dans le temps.

Reprenons l'image du train. Les wagons, ou blocs, ont une taille finie et ne peuvent donc contenir qu'un certain de nombre de marchandises/transactions. Le rythme de création des blocs étant constant, il y a un nombre maximal de transactions par seconde, gérable par le protocole Bitcoin, qu'on ne peut dépasser. Notons qu'il n'y a cependant pas de nombre de transactions minimal ; s'il n'y a aucune transaction, on peut tout à fait imaginer un wagon vide.

209. Lien : https://x.company/intl/fr_fr/loon/

Rappelons également que le revenu du mineur se décompose en deux parties :

- les bitcoins nouvellement créés lorsque le bloc est miné ;
- la somme des frais de transaction payés par les envoyeurs.

Dans le cas d'une trop forte demande de transactions, l'offre étant limitée (à la taille du wagon), le mineur qui remplit son wagon peut donc choisir les transactions qu'il y inclut. Ainsi, dans une logique économique, le mineur va intégrer en priorité les transactions dont les frais associés sont les plus importants.

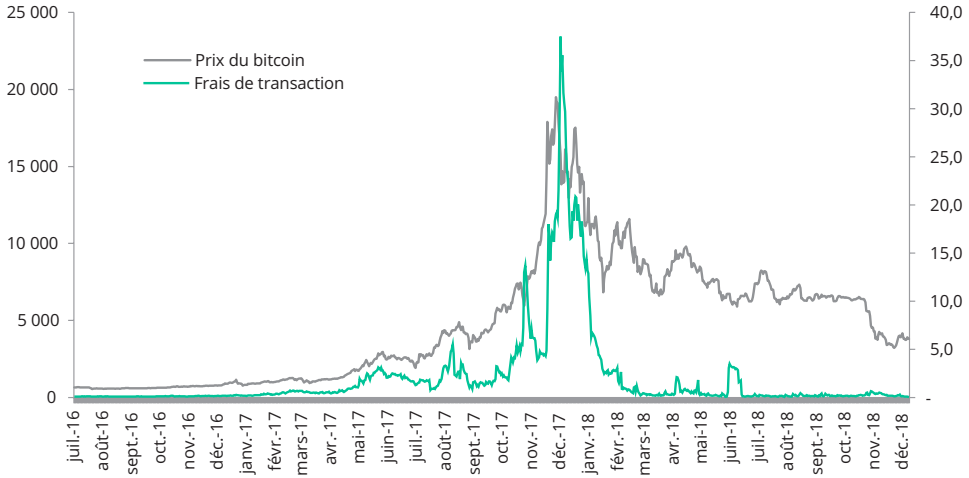
De même, l'offre peut faire varier les frais de transaction. Bien qu'en moyenne le rythme de création d'un bloc soit de 10 minutes, en pratique ce temps de validation fluctue autour de 10 minutes, avec parfois des écarts-types importants. Ainsi, si un bloc est trouvé au bout de 5 minutes, l'offre à un instant donné sera plus forte, et les mineurs accepteront les transactions avec potentiellement moins de frais.

Cette variation de l'offre et de la demande implique une grande variation dans les coûts de transaction.

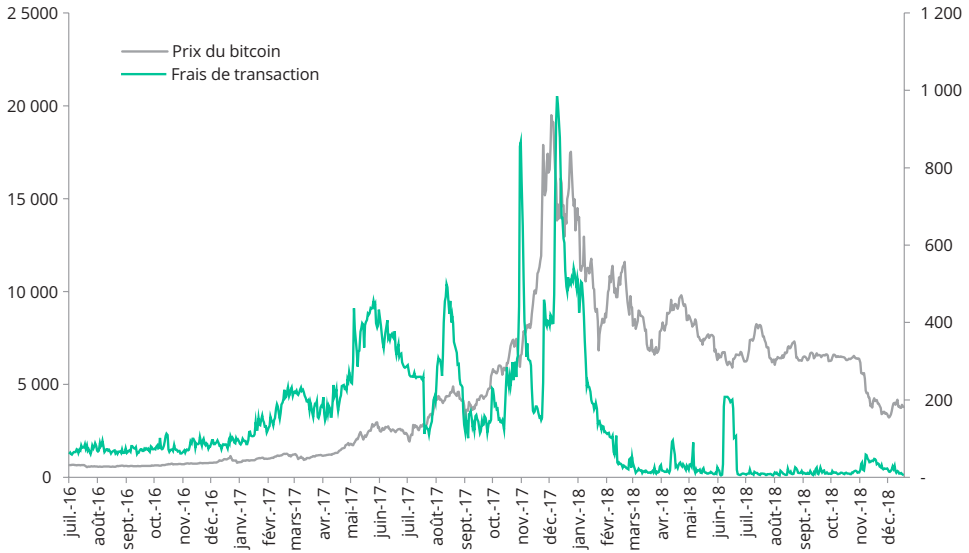
Enfin, il faut ajouter que le coût de transaction en bitcoins, qui dépend de la taille « informatique » de la transaction (selon le nombre d'UTXOs utilisées en entrée et en sortie), est exprimé en bitcoins par byte. Il est clair que, si le cours du bitcoin progresse fortement, à offre et demande constantes, le coût par transaction augmentera proportionnellement. La courbe d'évolution des frais moyens de transaction en dollars intègre donc les effets de l'évolution de l'offre et la demande ainsi que le cours du bitcoin.

Au contraire l'évolution des frais de transaction en bitcoins montre uniquement l'évolution du couple offre/demande. L'unité de l'axe de droite est exprimée en satoshi/byte, c'est-à-dire 10^-8 bitcoin/byte.

ÉVOLUTION RELATIVE DU PRIX DU BITCOIN ET DES FRAIS DE BITCOIN EN DOLLARS PAR TRANSACTION[210]



ÉVOLUTION RELATIVE DU PRIX DU BITCOIN ET DES FRAIS DE BITCOIN PAR TRANSACTION[211]



210. Source : bitcoinfees. Lien : https://bitcoinfees.info/
211. Source : bitcoinfees. Lien : https://bitcoinfees.info/

Le coût d'une transaction en bitcoins est fixe, c'est-à-dire qu'il n'est pas proportionnel au montant transféré, contrairement aux transferts traditionnels qui facturent généralement une commission variable. Un raisonnement un peu rapide pourrait conduire à la conclusion suivante. En supposant que le coût d'envoi d'un bitcoin soit de 30 dollars et qu'un transfert traditionnel facture en moyenne 7 %[212], il est tentant de considérer que le protocole Bitcoin devient compétitif à partir d'une somme de 400 dollars environ. Mais en réalité, le taux moyen facturé par les acteurs traditionnels, de type Western Union, ne correspond pas au seul mouvement de fonds mais provient de leur structure de coûts. Si de nombreuses dépenses peuvent être évitées par le Bitcoin (marketing, *risk management*, acquisition de clients…), les postes majeurs ne sont pas réellement adressables par la Blockchain. À l'image de la logistique, le dernier kilomètre est très coûteux (en 2014, la moitié des dépenses de Western Union était employée au règlement des commissions d'agents[213]). Les destinataires du transfert doivent pouvoir monétiser l'argent déplacé en liquide de la monnaie locale, la seule pour l'instant à permettre le règlement des dépenses courantes. Il semble compliqué pour le Bitcoin, dans ce contexte, de se passer d'un réseau de distributeurs locaux[214]. Le fait d'intercaler un change en bitcoins entre la monnaie de base et la monnaie de destination nécessite une conversion supplémentaire, générant par définition des coûts additionnels… Ces freins expliquent-ils l'absence à ce jour de généralisation massive des transferts d'argent par le biais de la Blockchain ?

Par ailleurs, l'argument de la vitesse de transaction n'est pas totalement pertinent. En effet, dans le cas de transferts d'argent internationaux, l'argent n'est pas effectivement déplacé : la société applique en réalité la stratégie du *pre-funding* (préfinancement) en gérant des balances de *cash* d'un côté et de l'autre du corridor. En revanche, le Bitcoin peut réduire les barrières à l'entrée et limiter drastiquement le coût de lancement d'un *business* dans le transfert d'argent. En effet, le coût de constitution des réserves évoquées est majeur et indispensable. Dans le cas du Bitcoin, l'existence de cette balance n'est plus nécessaire grâce à la rapidité du mouvement (10 minutes en moyenne). L'impact de l'innovation et de la Blockchain sur les coûts de la *remittance*[215] est donc moins évident qu'il n'y paraît. S'il est potentiellement important, il est en réalité indirect, résultant de la réduction des barrières à l'entrée. Dans ce contexte, l'existence de Fintech exploitant la technologie Bitcoin, parfois

212. Mauro F. Romaldini, « How is the international money transfer market evolving? » , mars 2017. Lien : https://www.toptal.com/finance/market-research-analysts/international-money-transfer
213. « Does Bitcoin/Blockchain make sense for international money transfers? », mars 2018. Lien : https://www.saveonsend.com/blog/bitcoin-Blockchain-money-transfer/
214. Auteur média sous le profil {cryptonight}, juillet 2015. Lien : https://medium.com/cryptonight/bitcoin-doesn-t-make-remittances-cheaper-eb5f437849fe.
215. La *remittance* est le terme désignant les transferts d'argent internationaux entre les travailleurs d'un pays ou d'une région vers les familles d'un autre pays ou d'une autre région.

adossée à des réseaux existants apparaît nécessaire (exemple de Bit Pesa/M-Pesa déjà évoqué). Le modèle de coopération entre Blockchain, Fintech, acteurs centralisés et décentralisés semble être une réponse efficace, du moins sur ce marché.

Enfin, cette création monétaire adossée à la validation de blocs permet de répondre à la problématique de la rémunération des nœuds du réseau : la création d'une incitation à la validation de nouveaux blocs permet au réseau d'avoir une bonne densité de nœuds, lui assurant ainsi la robustesse promise. Néanmoins, la croissance logarithmique des bitcoins reçus par bloc validé interroge la rentabilité à terme du minage. Ce dernier nécessite la mise à disposition du réseau d'une puissance de calcul assez élevée pour pouvoir résoudre l'algorithme de consensus. Cette mise à disposition est nécessairement consommatrice d'énergie et doit donc être rémunérée. Le moyen de compenser le nombre décroissant de bitcoins reçus par bloc validé est l'inclusion des frais de transaction qui permettent de rémunérer, sans création monétaire, les nœuds du réseau.

In fine, la vitesse d'adoption de la Blockchain dépendra de trois facteurs majeurs : le besoin des consommateurs, l'adéquation de la solution technologique à ces besoins et l'impact de la réglementation. Le cas des données personnelles en est un bon exemple. En effet, l'économie d'Internet possède des logiques qui lui sont propres et qui représentent une rupture vis-à-vis de l'économie industrielle *brick and mortar*. Les principaux usages du Web sont, de fait, gratuits : moteur de recherche, réseaux sociaux, consultation de vidéos ou de sites d'actualité. Les applications embarquées sur nos téléphones mobiles le sont également. Pour rentabiliser un service gratuit, les entreprises du Web demandent aux utilisateurs de leur céder un nombre important de données personnelles, parfois à leur insu. Or, à l'instar du pétrole durant les Trente Glorieuses, les données représentent une matière première dont le contrôle est stratégique pour l'économie du début XXIe siècle.

Dans l'économie d'Internet, la donnée est l'essence des algorithmes de types Big Data. Elle contient en effet les informations de ce que peut constituer la vie privée d'une personne. En utilisant les services des géants du Web, les utilisateurs acceptent, de manière plus ou moins consciente, que des sociétés privées possèdent des informations sur eux qu'elles pourront revendre aux plus offrants, créant ainsi un marché de la donnée.

Les risques de ce marché sont bien réels comme en témoignent les récents déboires de Facebook avec Cambridge Analytica soupçonné d'avoir dérobé les données de 87 millions d'utilisateurs à des fins politiques. Permettre à l'utilisateur de redevenir maître de la gestion de sa

donnée est donc un enjeu clé pour l'avenir. À cet égard, la mise en place en 2018 du Règlement général sur la protection des données (RGPD) par l'Union Européenne, visant à mieux protéger l'utilisation des données personnelles par les entreprises du Web, est une première réponse. La Blockchain pourrait en être une seconde, en devenant un levier puissant pour mettre en œuvre la RGPD. Elle a en effet le potentiel nécessaire pour proposer un changement stratégique majeur dans la gestion et la protection des données personnelles sur le Web, notamment grâce à une réappropriation de la part des citoyens des données relatives à leur vie privée.

En synthèse, le scénario de cartes économiques rebattues apparaît très crédible, porté à la fois par l'accaparement de la technologie par les acteurs existants et l'émergence d'acteurs – eux-mêmes plus ou moins décentralisés – complémentaires ou concurrents. Les chaînes de valeur devraient être – du moins partiellement – impactées, marquées par la disparition de certaines formes d'intermédiaires au profit de la Blockchain et l'émergence de nouvelles formes d'intermédiaires.

À date, le succès des Blockchains publiques nécessite de résoudre une problématique d'incompatibilité triangulaire : décentralisation – sécurité – scalabilité. Est-elle conceptuellement inévitable ou solutionnable par le progrès technique ?

Le second enjeu est la difficulté de concilier expérience client et décentralisation.

In fine, l'arbitrage entre des solutions – notamment de paiement ou liées à la donnée – s'effectue sur deux critères : le prix et la qualité de l'usage.

Peut-être la combinaison de protocoles décentralisés et d'interfaces centralisées constitue-t-elle la meilleure synthèse ?

E

LA RUÉE VERS L'OR DIGITAL : FORCES STRATÉGIQUES ET JEUX D'ACTEURS

Comprendre la technologie Blockchain *via* une approche conceptuelle permet de saisir toutes les notions qu'elle interroge bien au-delà de la simple innovation technologique : la confiance, l'individu, la liberté, la monnaie, la souveraineté et l'État. Néanmoins elle nécessite d'être complétée par une approche topographique de l'écosystème qui s'agrège autour d'elle. Dans cette optique, nous déterminerons les éléments de la chaîne de valeur propre à la technologie Blockchain afin de repérer les problématiques économiques en jeu et les forces en présence.

Autour de la Blockchain, ses promesses, ses clivages, ses limites, s'organise une véritable course à la valeur autour d'un jeu stratégique d'acteurs et donc pas toujours facile à suivre. Quelles sont les forces en présence ? Quels sont leurs rôles ? Quelles chaînes de valeur ?

Les cas d'usage sont réels mais nous n'en sommes encore qu'aux balbutiements des possibilités de la Blockchain. Comprendre les dynamiques en cours, pour affiner sa stratégie dans cet océan de complexité, est clé. Innovation, partenariats, rachats, cessions, lobbying sont autant de réponses stratégiques possibles.

I.
La chaîne de valeur de la Blockchain, un processus d'innovation linéaire ?

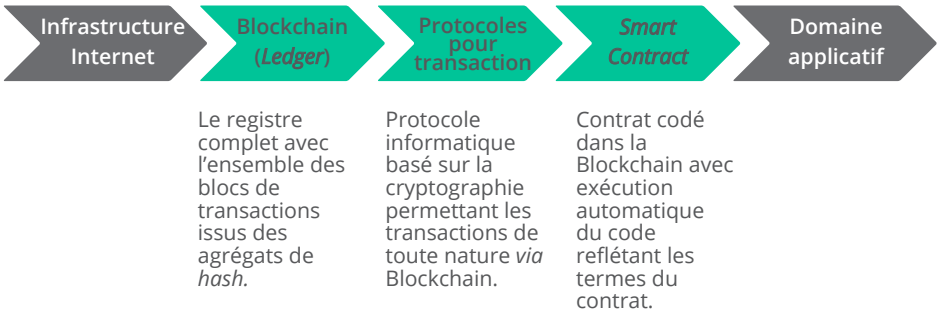
La chaîne de valeur de l'écosystème de la Blockchain s'apparente à un processus d'innovation linéaire où la complexité technologique est croissante avec le temps. Cela s'explique par la superposition de briques technologiques qui, s'accumulant, créent un écosystème dont les usages se complexifient au fur et à mesure de sa maturation. Les principales briques ou piliers technologiques composant l'écosystème de la Blockchain sont :

- la Blockchain en tant que registre complet de l'ensemble des blocs de transactions ;
- le protocole de transaction qui permet les transactions de toutes natures sur la Blockchain grâce à un réseau informatique pair-à-pair ;

- les *Smart Contracts* qui permettent l'exécution automatique de contrats dont la fiabilité et la sécurité sont assurées par la Blockchain en tant que registre et protocole de transaction.

En amont de ces trois briques technologiques, on retrouve l'infrastructure Internet sans laquelle le réseau ne pourrait pas exister et sans laquelle les utilisateurs ne pourraient pas avoir accès aux usages. En aval de cette chaîne de valeur se trouve l'ensemble des applications qui utilisent les possibilités de la technologie, sans nécessairement participer à son évolution, mais qui en démultiplient les usages possibles.

SYNTHÈSE CHAÎNE DE VALEUR DE LA BLOCKCHAIN



II.
La Blockchain impacte de nombreux secteurs de l'économie traditionnelle

La technologie Blockchain doit être comprise comme une *general purpose technology* dans le sens où son impact sur l'économie traditionnelle concerne, potentiellement, la plupart des secteurs économiques. Cet impact se décompose selon les trois piliers technologiques précédemment identifiés (registre distribué, protocole de transaction et *Smart Contract*). Cette segmentation de la technologie Blockchain en trois piliers distincts permet de cibler avec plus de précision les différents usages qu'elle peut avoir pour un secteur économique donné. Chaque pilier technologique apporte, en effet, une réponse à une ou plusieurs problématiques se décomposant de la sorte :

- Le registre distribué répond à la problématique générique de la gestion des données de toutes natures auxquelles font face toutes les entreprises. Le registre distribué ne doit pas être compris comme un moyen de stocker de grandes quantités de données, comme pourrait l'être un *Data Center*. Le registre distribué propre à la Blockchain doit être compris comme un outil permettant la collaboration, l'interopérabilité et la destruction des silos de données. Avec la Blockchain, la donnée devient traçable dans l'espace et dans le temps, consultable et auditable par les parties prenantes autorisées[216].

- Le protocole de transaction répond à la problématique du transfert de valeurs digitalisées de manière sécurisée.

- Les *Smart Contracts* peuvent être considérés comme le moyen de démultiplier les usages des deux premiers piliers en leur apportant une efficacité accrue. Cette efficacité se décline autour de l'automaticité des tâches et des transferts effectués, de la réduction de la complexité liée à la coordination des systèmes, de la sécurité liée aux clauses inscrites dans ces contrats. Enfin, tout comme le registre distribué, les données contenues dans ces *Smart Contracts* sont consultables et auditables par tous.

Dans la matrice ci-contre, nous proposons, en synthèse, de décliner les usages de ces trois piliers technologiques en fonction des problématiques adressées et des secteurs économiques. Pour chaque usage et pour chaque secteur, a été mesuré l'impact de ces usages en fonction de la criticité qu'ils représentent.

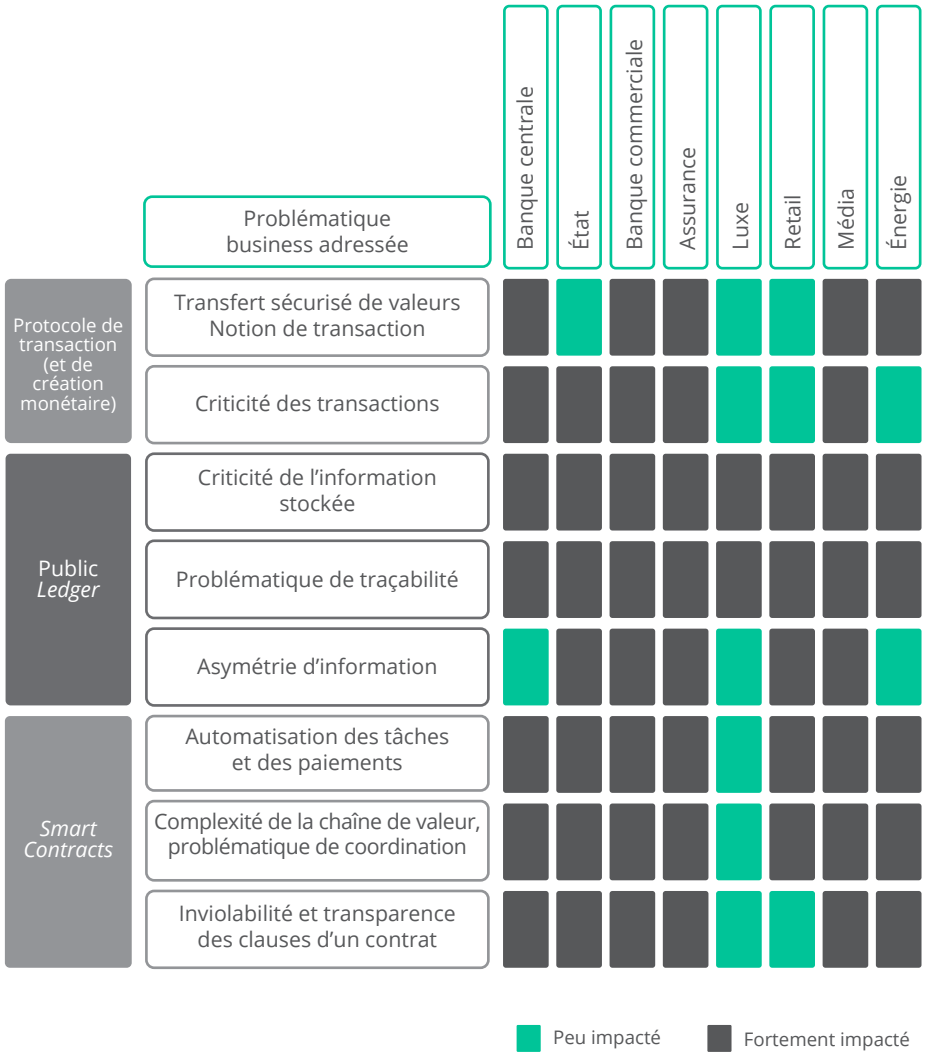
Parmi les secteurs présentés ci-contre, les services financiers (banque et assurance), les médias et l'énergie font l'objet d'une analyse détaillée dans le chapitre dédié aux cas d'usage sectoriels.

Banques centrales et commerciales

La technologie Blockchain a été pensée initialement comme le moyen d'effectuer des transactions indépendantes d'un organe central de contrôle grâce à l'utilisation de crypto-monnaie. Ces deux caractéristiques initiales expliquent que les banques, qu'elles soient centrales ou commerciales, soient aussi directement concernées : la gestion de la création monétaire et la garantie de transactions sécurisées sont les deux composantes de leur cœur de métier. Les banques se sont néanmoins beaucoup diversifiées autour d'une chaîne de valeur complexe.

216. Pour rappel : dans une Blockchain publique, l'information est consultable par tous sans contrainte, dans une Blockchain privée et permissive, l'information est consultable seulement par ceux dont l'accès a été autorisé par une autorité centrale.

MATRICE DES IMPACTS DE LA BLOCKCHAIN PAR SECTEUR ÉCONOMIQUE



Assurance

Dans un contexte de chaîne de valeur complexe, le métier de l'assurance repose sur la confiance, la gestion des asymétries d'information et l'exécution de transactions sous conditions. Le remboursement d'un sinistre en est le bon exemple : la transaction s'effectue après le déclenchement d'un événement (le sinistre). Le pilier technologique des *Smart Contracts* est donc un cas d'usage aux impacts importants pour ce secteur. D'autres usages de la technologie Blockchain ciblent des points précis de la chaîne de valeur du secteur de l'assurance.

État

Un des cas d'application de la technologie Blockchain et du registre distribué est la gestion des données personnelles sensibles et officielles (l'identité) de manière décentralisée et sécurisée. En proposant d'apporter de la fluidité et de la traçabilité dans la gestion des données, la technologie Blockchain pourrait devenir un outil étatique performant. À cet égard, l'Estonie fait figure de pionnier puisque ce pays envisage d'utiliser la technologie Blockchain comme moyen de partage et de standardisation numérique des données personnelles des citoyens (santé, justice et sécurité[217]).

Média

La technologie Blockchain permet d'assurer la traçabilité dans la gestion des transactions. C'est, notamment en ce qui concerne les droits d'auteur, un des points critiques de la chaîne de valeur. D'autres éléments concernant l'impact de la technologie Blockchain sur la chaîne de valeur du secteur des médias sont détaillés ci-après (cf. « Les cas d'usage des médias »).

Retail et luxe

Les secteurs du retail et du luxe sont également confrontés à des problématiques de traçabilité (qualité des produits, certification d'authenticité…). La technologie Blockchain pourrait donc offrir des solutions à ces problématiques spécifiques. À cet égard, la start-up Provenance cherche ainsi à développer des solutions pour certifier l'origine de produits alimentaires.

Énergie

La Blockchain peut servir des cas d'usage dans le domaine de l'énergie, soit pour des acteurs existants souhaitant améliorer l'efficacité de leurs

217. Lien : https://e-estonia.com/wp-content/uploads/faq-a4-v02-Blockchain.pdf

services, soit pour de nouveaux acteurs. Ces derniers proposent essentiellement une gestion désintermédiée de l'énergie.

La technologie Blockchain a vu les cas d'usage se multiplier dans de nombreux secteurs économiques, la transformant en une *general purpose technology,* au gré des évolutions technologiques qui lui sont liées. La criticité de son impact dépend de la chaîne de valeur de chaque secteur économique et des solutions concrètes qu'elle peut apporter face à une problématique précise.

Le cas d'usage le plus communément évoqué, testé et implémenté est celui de la traçabilité, dans la plupart des industries, bien que les enjeux ne soient pas toujours identiques en fonction des industries. Plusieurs cas récents ont été fortement relayés : la traçabilité de l'énergie verte tokenisée par le fournisseur d'électricité Engie, la traçabilité des diamants utilisant la technologie Everledger par le diamantaire De Beers ou encore la traçabilité des poulets mis en œuvre par le *retailer* Carrefour. D'autres projets dans l'industrie sont également à l'étude.

Ces projets comportent néanmoins des différences et font l'objet de critiques, notamment des communautés Bitcoin, Ethereum ou plus largement des défenseurs des Blockchains publiques et de la philosophie open source et de décentralisation sous-jacente.

En effet, la Blockchain Carrefour est par exemple une Blockchain privée, c'est-à-dire que le registre n'est pas accessible à tous et que la validation des transactions et leur ancrage dans la chaîne n'est pas validée par un mécanisme de consensus décentralisé et donc neutre et résilient. Ces projets ne sont pas totalement dénués de valeur puisqu'ils comportent une dimension forte d'engagement des acteurs en faveur de la transparence des produits et de leurs modes de production. Ils comportent également, il est vrai, une composante communication et marketing importante. À titre d'exemple, le consommateur peut accéder, dans le point de vente, à une photo du poulet acheté lors de son élevage.

De notre point de vue, la principale difficulté est la problématique d'interopérabilité entre la Blockchain et le monde physique. Le point clé de ces cas de traçabilité dans le monde physique est d'être capable de vérifier l'information ancrée dans la Blockchain, qu'elle soit d'ailleurs publique ou non. Ce vérificateur d'informations est communément appelé « oracle » dans le jargon. À l'origine, avec Bitcoin, la Blockchain fonctionnait comme un système homogène : les valeurs digitales associées aux informations ancrées dans le registre n'ont pas d'existence physique. La véracité de l'information ne tient donc qu'au caractère correct et reconnu de tous, des entrées saisies dans le registre. En synthèse, le système est autosuffisant.

Dans le cas par exemple de la transaction et de la traçabilité d'un (vrai) sac à main, la problématique est autre. Il faut associer à ce sac une valeur digitale (*token*) correspondant à ce sac ; c'est ce *token* qui est échangé aux yeux de la Blockchain, pas le sac à main lui-même. Si le sac à main est une contrefaçon, mais que l'information « sac authentique » est ancrée dans la Blockchain, alors il sera noté comme authentique dans le registre. Autre situation : si le sac était authentique mais qu'il a été échangé avec un faux, la Blockchain ne reconnaîtra pas ce changement d'état puisque l'information initiale était « sac authentique », induisant de fait un écart entre ce qui est écrit dans la base et la réalité. Il faut donc être en mesure de sécuriser l'entrée et le suivi d'une information réelle dans la Blockchain ; en d'autres termes : synchroniser le monde physique et le monde de la Blockchain. Une des solutions explorées est la combinaison entre l'Internet des objets et la Blockchain, pour limiter les risques d'erreur, de fraude ou de mauvaise information, liés entre autres à l'aléa moral. En reprenant l'exemple du sac à main, on peut par exemple accrocher une puce RFID à l'objet correspondant de façon unique à une série de caractères ancrée dans la Blockchain. Bien sûr, cette puce ne doit pas pouvoir être retirée sans détruire l'objet.

III.
La Blockchain implique une restructuration de la vie économique

La technologie Blockchain a des impacts multiples sur la structuration et l'organisation de la vie économique. Sur ce point également, l'analogie avec Internet permet de mieux les appréhender. En effet, l'apparition d'Internet a permis à un certain nombre d'acteurs nouveaux d'émerger, comme les GAFA [218], dont le modèle économique repose sur une utilisation pleine et entière d'Internet, faisant d'eux des *pure players*. Néanmoins, on ne peut résumer l'impact d'Internet à leur apparition : chaque entreprise de l'économie traditionnelle a pu s'appuyer sur Internet pour créer de nouveaux usages (commandes en ligne par exemple) ou améliorer les processus internes (réduction du coût de la communication grâce aux vidéoconférences par exemple).

218. Google, Amazon, Facebook et Apple.

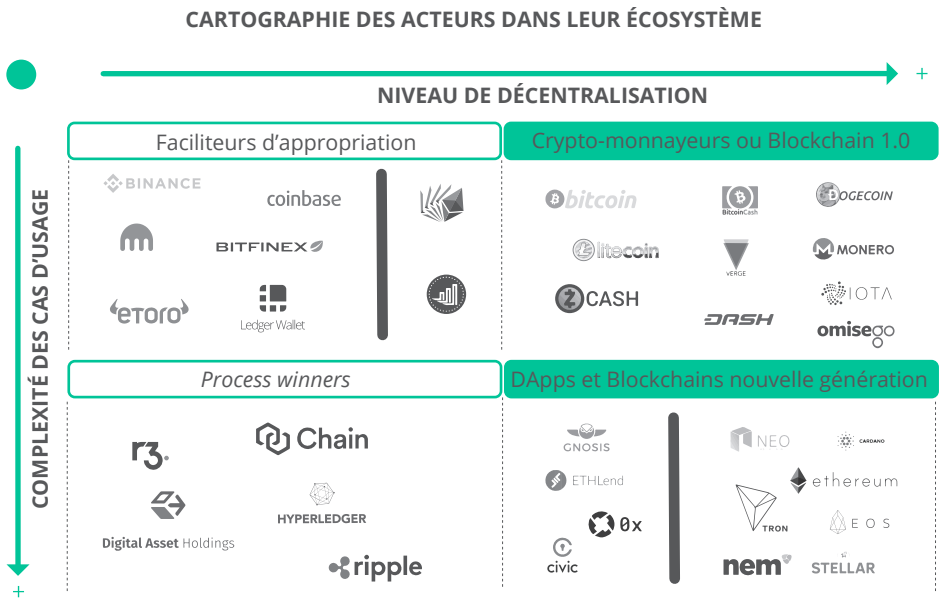
La technologie Blockchain peut donc avoir un impact sur la vie économique avec la même ampleur qu'Internet : d'une part, des *pure players*, dont le modèle économique s'appuie sur une utilisation pleine et entière de la technologie vont émerger. D'autre part, les entreprises traditionnelles vont pouvoir développer de nouveaux usages et améliorer les processus internes.

a. L'écosystème se structure autour deux axes : le niveau de décentralisation et la complexité des cas d'usage. L'axe horizontal mesure le niveau de décentralisation de l'organisation qui permet globalement de distinguer les acteurs centralisés de ceux plutôt décentralisés. Les acteurs les plus centralisés utilisent des Blockchains permissives ou privées ou gravitent autour de l'écosystème Blockchain sans en utiliser la technologie. Les acteurs les plus décentralisés utilisent des Blockchains publiques. En réalité, tous les acteurs utilisant des Blockchains publiques n'ont pas le même niveau de décentralisation. En effet, le niveau de décentralisation d'une entreprise dans l'écosystème Blockchain se définit essentiellement par le rôle que joue le *token* dans son modèle économique. Un niveau de décentralisation élevé implique un *token* garantissant un alignement d'intérêts maximisé au sein de l'écosystème créé, en l'absence d'intervention directe de tiers centralisé. *A contrario*, un niveau de décentralisation plus faible s'explique par l'intervention d'un acteur centralisé dans la circulation des crypto-actifs. Contrairement aux idées reçues, le lien direct entre nouveaux acteurs Blockchain et décentralisation est loin d'être automatique.

b. L'axe vertical mesure la complexité du cas d'usage du produit proposé, qui permet de distinguer les acteurs en amont de la chaîne de valeur de l'écosystème de ceux en aval. Le point de rupture entre l'amont et l'aval de l'écosystème étant l'usage ou non de *Smart Contract*.

Le croisement de ces deux axes nous permet de cartographier quatre familles d'acteurs :

- les facilitateurs d'appropriations ;
- les *process winners* ;
- les crypto-monnayeurs ou Blockchain 1.0 ;
- les DApps et Blockchains nouvelle génération.



IV.
Les facilitateurs d'appropriation

De façon générale, ces acteurs peuvent être comparés aux vendeurs de pelles lors de la ruée vers l'or. La catégorie des facilitateurs d'appropriation rassemble les acteurs qui proposent un service ou un produit en lien avec l'écosystème de la Blockchain. Ces acteurs sont donc peu décentralisés, puisque reposant sur une organisation traditionnelle, et situés en amont de la chaîne de valeur selon le critère de différenciation défini précédemment. Ils sont considérés comme des facilitateurs d'appropriation et de pénétration de la technologie puisqu'ils participent directement au développement et à la sécurisation de l'écosystème. Dans cette catégorie, nous distinguons quatre sous-catégories d'acteurs : les accompagnateurs, les échangeurs, les régulateurs et les coffres-forts.

IV.1 Les accompagnateurs

Les accompagnateurs sont les acteurs qui favorisent le développement de l'écosystème en proposant un service, l'activité de miner, qui permet de faire vivre les réseaux Blockchain. Les accompagnateurs rassemblent aussi bien le mineur ayant mis l'ordinateur familial à contribution que les fermes de minage. Ces dernières sont des sociétés qui se sont spécialisées dans l'installation de parcs informatiques (l'idée étant de relier plusieurs ordinateurs entre eux afin d'augmenter la puissance de calcul disponible et donc avoir plus de *chances* de remporter la mise). Les noms les plus connus sont par exemple Bitmain en Chine, Bitfury ou Bitfarms.

Là encore, ces fermes de mineurs créent une sorte de paradoxe dans l'écosystème de la technologie Blockchain. En effet, les mineurs sont censés assurer au réseau sa sécurité et en même temps sa décentralisation : l'existence d'un tissu de nœuds plus ou moins de même taille permettrait, en théorie, un maillage planétaire et donc une décentralisation du réseau quasi parfaite. Cependant, les rentabilités importantes offertes par cette activité ont eu pour conséquences une centralisation des pôles de minage autour de sociétés disposant de superpuissance de calcul, dans des environnements au climat froid (limitant ainsi naturellement le coût de refroidissement) et à l'électricité bon marché (afin de réduire le coût du minage). Ainsi l'Islande et le Canada apparaissent comme des destinations privilégiées pour l'activité de minage. La chute du cours du Bitcoin a très fortement diminué les niveaux de rentabilité de cette industrie et a entraîné un potentiel rebattage des cartes, sur le plan stratégique.

L'activité de minage entraîne une « course à l'armement » qui pousse les acteurs à s'équiper de matériel toujours plus performant, ce qui est par conséquent une opportunité stratégique pour certains. Il est à ce titre très intéressant de noter les retombées commerciales pour des fabricants et revendeurs existants, qui ne sont pas spécialisés dans le minage. La carte graphique Radeon RX 580 8GD5 PULSE (Sapphire) a vu son prix augmenter de plus de 20 % en 2017, sous la pression de la demande et des ruptures de stock en cascade[219]. Dans ce contexte, Sapphire, Asus et MSI auraient annoncé vouloir commencer une activité de production de cartes graphiques parfaitement adaptées au minage de cryptoactifs. Non moins impressionnante, la société Nvidia (spécialisée dans les cartes graphiques) a vu le prix de son action exploser entre 2014 et 2017 (170 dollars en septembre 2017 contre 20 dollars fin 2014). Cette hausse est liée à la progression spectaculaire des ventes de 52 % en 2017, portée notamment par la carte Asus Mining P106, spécialement conçue

219. Jean-Baptiste Giraud, 30 juillet 2017. Lien : www.clubic.com/technologies-d-avenir/actualite-834188-cryptomonnaie-prix-graphique.html?_sm_au_=iVVPS5rQFvj0QZ7P

pour optimiser le minage[220]. À l'inverse, la baisse brutale du cours du Bitcoin a eu un impact très négatif sur les activités et les cours de Bourse sur l'année 2018. La société chinoise Bitmain s'est quant à elle spécialisée dans la fourniture du fameux ANTMINER Asic qui permet de miner du bitcoin ou du litecoin de manière très optimisée[221]. Des sites Web proposent même des comparatifs de rentabilité du minage en fonction de l'équipement utilisé[222].

IV.2 Les échangeurs

Les échangeurs (ou les *exchanges*) sont les acteurs qui favorisent le développement de l'écosystème en proposant des solutions qui permettent aux utilisateurs d'acquérir des crypto-monnaies. Dans l'économie traditionnelle, si un acteur économique change de zone monétaire, mettons de l'Europe vers les États-Unis, et qu'il souhaite échanger sa devise papier contre une autre, il doit pour cela se rendre dans un bureau de change. À ce titre, le bureau de change est le pont permettant de relier les zones monétaires entre elles. Les échangeurs ont le même rôle que les bureaux de change. La différence réside dans la nature des zones monétaires qu'ils relient : les échanges ne sont plus effectués entre deux zones monétaires attachées à des territoires (Europe et États-Unis par exemple) mais entre la zone monétaire de l'économie traditionnelle, donc territorialisée, et la zone crypto-monétaire, qui s'affranchit des territoires physiques pour occuper le cyberespace.

L'existence des échangeurs, qui se matérialise en plates-formes Internet, insère un paradoxe dans la technologie Blockchain : pourquoi avoir besoin d'une plate-forme Internet centralisée pour acquérir des *tokens* apportant une promesse de décentralisation ?

Pour répondre à ces questions, raisonnons par l'absurde et plaçons-nous dans un cas où ces plates-formes n'existeraient pas. Dans ce cas-là, si Bob souhaite acquérir un bitcoin, il doit se créer un *wallet* sur la Blockchain Bitcoin puis demander à Alice de lui en envoyer (ou directement miner du bitcoin). Une fois le bitcoin reçu, Bob envoie à Alice le montant équivalent en euros sur le circuit bancaire de l'économie traditionnelle. Dans cet exemple, l'absence de plate-forme d'échange implique que Bob et Alice se connaissent et se fassent confiance. Cette

220. Julio Gil-Pulgar, 05/09/2017. Lien : https://news.bitcoin.com/bitcoin-nvidia-price-soar-sync/
221. Lien : https://www.bitmain.com/
222. Lien : https://www.cryptocompare.com/mining/calculator/btc?HashingPower=14000&HashingUnit=GH%2Fs&PowerConsumption=1293&CostPerkWh=0.12&MiningPoolFee=1

contrainte limite l'usage des crypto-monnaies puisqu'elle rend peu pratique l'accès aux agents économiques à la zone crypto-monétaire.

La problématique ne s'arrête pas là puisque l'échange de crypto-monnaie dans la zone crypto-monétaire n'est également pas fluide du fait du manque d'interopérabilité des crypto-monnaies entre elles. En effet, plaçons-nous désormais dans le cas où Bob a pu acquérir un bitcoin et souhaite l'échanger contre un ether. Comme les deux Blockchains sont distinctes et ne communiquent pas directement, il doit envoyer un bitcoin à Alice qui le reçoit sur son *wallet* Bitcoin. Ensuite, elle peut changer de *wallet* et envoyer le montant en ethers équivalent à Bob sur son *wallet* Ethereum. Là encore, l'absence de plate-forme d'échange implique que Bob et Alice se connaissent et se fassent confiance.

En synthèse, les échangeurs apportent du liant entre la zone monétaire traditionnelle et la zone crypto-monétaire mais également dans la zone crypto-monétaire. Par quel mécanisme arrivent-ils à dépasser les contraintes d'interopérabilité ? Il faut, pour répondre à cette question, garder en tête l'analogie avec les bureaux de change. Pour pouvoir échanger les devises entre elles, ils détiennent des stocks physiques importants de chacune des monnaies et piochent dans ces stocks dès lors que l'on souhaite une monnaie contre une autre. Les échangeurs fonctionnent de la même manière mais de façon dématérialisée : pour chaque crypto-monnaie qu'ils cotent, ils détiennent un *wallet* dans lesquels sont stockés un montant important de crypto-monnaies (bitcoins, ethers...) ainsi qu'un compte bancaire traditionnel. Le montant de crypto-monnaie stocké par les échangeurs est consultable sur les Blockchain afférentes, à des adresses Internet .io (commeetherscan.io). On y identifie des séries d'adresses publiques et une quantité de crypto-actifs de l'unité de compte de la Blockchain considérée, ainsi que l'historique des transactions. C'est le principe de transparence de la Blockchain qui impose cela : le montant de crypto-monnaie détenu par un *wallet* est consultable par tous comme dans un grand livre de compte ouvert. L'anonymat est garanti par le fait que l'on ne peut pas publiquement déduire un nom de personne physique à partir d'un numéro de *wallet*. On peut néanmoins associer un nom de personne morale, comme c'est le cas pour les échangeurs dans notre exemple.

Kraken possède un *wallet* de plus de 800 000 ethers et Bittrex en détient un peu plus de 700 000. Comme les plates-formes d'échange possèdent de nombreux *wallets* de diverses crypto-monnaies, les échanges se font sur la plate-forme et non pas entre les Blockchains. Par exemple, Bob décide d'acquérir des crypto-monnaies et se rend pour ce faire sur une de ces plates-formes. Il s'y inscrit et y dépose un montant de 1 000 euros. Cette première transaction est une transaction de l'économie traditionnelle vers l'économie traditionnelle : du compte bancaire de

Bob vers le compte bancaire de la plate-forme qui, rappelons-le, est une entreprise commerciale. Une fois ce montant de 1 000 euros déposé, la plate-forme crédite Bob d'un solde virtuel de 1 000 euros lui permettant d'acquérir les crypto-monnaies disponibles. Le prix d'une crypto-monnaie dans une plate-forme est fixé par agrégation de l'offre et de la demande, et les échanges entre les acteurs économiques de cette plate-forme se font en circuit fermé en son sein. Aucune des crypto-monnaies échangées sur une plate-forme ne transite sur la Blockchain, si bien que les volumes de transaction sont sans commune mesure avec les capacités actuelles des Blockchain. Ainsi, en 2018, le volume de transactions effectuées par jour est de l'ordre de 500 millions, toutes plates-formes et monnaies confondues. En synthèse, ce qu'il faut bien comprendre sur les transactions chez les échangeurs, c'est qu'elles sont *fictives,* dans le sens où elles n'interagissent pas directement avec les Blockchains afférentes. Néanmoins, un utilisateur peut décider de retirer un montant détenu dans une crypto-monnaie de la plate-forme pour le stocker sur un *wallet* en dehors de la plate-forme. Dans ce cas-là, la transaction se fait dans la zone crypto-monétaire entre le *wallet* de l'échangeur et le *wallet* de l'utilisateur et transite sur la Blockchain associée.

Le prix relevé sur une plate-forme provient de l'équilibre entre l'offre et la demande au sein de celle-ci. Il peut par conséquent varier significativement d'une plate-forme à l'autre puisqu'elles fonctionnent de manière indépendante les unes des autres. À titre d'illustration, il est possible d'observer pour le bitcoin au 1er mai 2018, un prix de 8 980 dollars sur Poloniex contre 9 013 dollars sur Hitbtc, soit une différence de 0,4 %[223].

Cette différence de prix entre les plates-formes pour une même crypto-monnaie pourrait ouvrir la voie à des stratégies d'arbitrage entre les plates-formes. La stratégie optimale serait d'acheter un bitcoin sur Bitfinex (9 046,50 dollars) et de le vendre sur TrustDex (9 977 dollars). Le gain théorique, immédiat et sans risque, serait de 930,50 dollars. Dans les faits, les importants frais de transaction appliqués par cette plate-forme, ainsi que la longueur d'une telle opération rendent celle-ci, si ce n'est impossible, au moins très difficile. La différence de prix entre les plates-formes traduit leurs différences de liquidité. Le succès d'une plate-forme auprès des utilisateurs impacte directement la liquidité des titres : plus le nombre d'utilisateurs actifs est élevé, plus les volumes échangés le sont et plus la liquidité des titres est forte.

En jouant le rôle de places de cotation, de fournisseurs de liquidité, de ponts entre les zones monétaires, les échangeurs occupent une place prépondérante dans l'écosystème de la Blockchain alors même qu'ils n'en utilisent pas la technologie. Cela est également renforcé par le fait

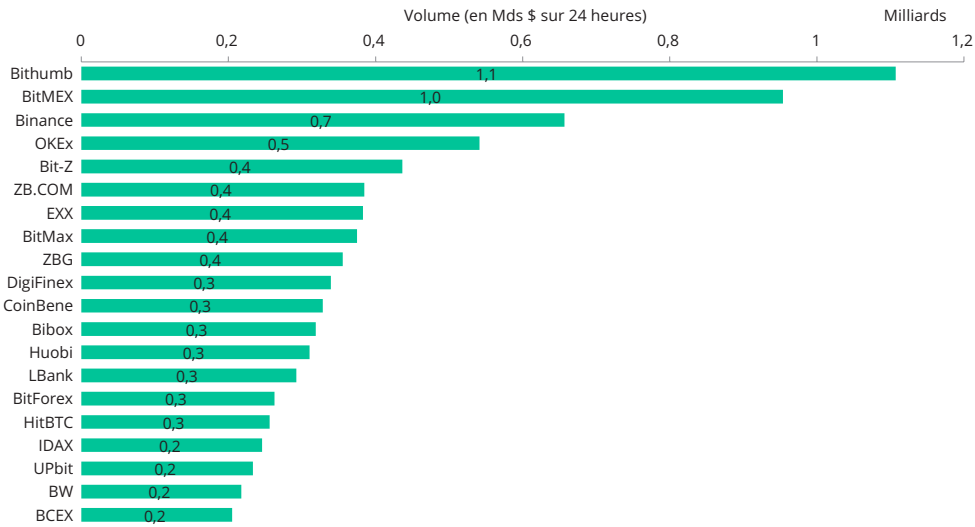
223. Source : https://www.cryptocompare.com/coins/btc/markets/USD

qu'ils sélectionnent les crypto-monnaies qui peuvent être acceptées sur la plate-forme. En effet, la technologie Blockchain étant encore non mature et le marché non régulé, de nombreux risques existent quant aux crypto-monnaies : risque d'arnaque pur et simple où un projet fantoche est associé à une crypto-monnaie[224], risque technologique, risque économique, risque financier… Pour lutter contre tous ces risques et pour éviter de coter une crypto-monnaie sans valeur, ce qui nuirait à sa réputation[225], les échangeurs effectuent de nombreuses vérifications :

- générale *via* un audit du projet et de son équipe ;
- technique *via* des audits du code informatique du projet ;
- financière *via* un droit de cotation important qui est payé par le projet.

Ces audits sont essentiels pour les plates-formes d'échange puisque la confiance qu'ont les utilisateurs dans leur capacité à filtrer les projets de crypto-monnaies sans valeur est un des facteurs clés de leur succès. Le marché des échangeurs est aujourd'hui très compétitif puisqu'on compte plus de 30 initiatives, dont les principales, en termes de volume, sont les suivantes :

VOLUMES OBSERVÉS EN MILLIARDS DE DOLLARS PAR 24 HEURES SUR LES PRINCIPALES PLATES-FORMES D'ÉCHANGE EN JANVIER 2019[226]



224. Dans la communauté Blockchain, une arnaque est appelée un *scam*.
225. Si une plate-forme a la réputation de coter des crypto-monnaies qui supportent des projets sans véritable valeur économique ou des *scams*, les utilisateurs vont la fuir. Dès lors, la capacité pour une plate-forme de dégager une réputation de sérieux est primordiale.
226. Lien : https://coinmarketcap.com/exchanges/volume/24-hour/. *Nota* : GDAX correspond à Coinbase.

Si toutes les plates-formes proposent d'échanger les principales crypto-monnaies (bitcoin, ether, litecoin...) il n'en demeure pas moins que des stratégies différenciées existent parmi ces échangeurs pour attirer de nouveaux utilisateurs :

- Binance propose sa propre monnaie (BNB) pour réduire les frais de transaction ;

- BitMex propose des produits dérivés pour les crypto-monnaies pour un volume de transactions qui avoisine les 17 milliards de dollars début 2018[227].

Leur place prépondérante dans l'écosystème, à laquelle s'ajoute la volonté toujours croissante d'acteurs économiques d'acquérir des crypto-monnaies, explique leur succès : le chiffre d'affaires de Coinbase (et de sa plateforme de trading GDAX) a atteint plus de 1 milliard de dollars en 2017[228] et les principales plates-formes enregistrent plus de 100 000 nouvelles inscriptions quotidiennes, les forçant parfois à fermer les inscriptions momentanément ou à ne les ouvrir qu'à certaines périodes de la journée[229]. Ces inscriptions permettent notamment de vérifier l'identité des usagers, *via* un processus dit de *Know Your Costumer* (KYC) strict. Les usagers doivent prouver leur identité avec des photos, des noms et un passeport, ce qui permet de limiter les échanges douteux. Plus récemment, les réseaux sociaux et médias spécialisés ont relayé l'information de bénéfices records pour Binance au premier trimestre 2018 : 200 millions de dollars avec seulement 200 collaborateurs[230].

Néanmoins, comme nous le soulignions précédemment, ces plates-formes d'échange reposent sur la technologie Internet et créent une forme de paradoxe quant au développement de la technologie Blockchain : elles fournissent un accès au marché des crypto-monnaies décentralisées tout en étant elles-mêmes centralisées puisqu'elles ne se distinguent pas d'autres acteurs marchands d'Internet. Cette centralisation implique de nombreux risques de piratage. Funestement célèbre est celui de la plate-forme japonaise Mt Gox. Créée en 2010, elle gérait, en 2014, 70 % des transactions Bitcoin. Le 28 février 2014, une attaque informatique a mis fin à ses activités. Elle a permis aux *hackers* de dérober 750 000 bitcoins, soit environ 345 millions d'euros si l'on prend le cours du jour de l'attaque. De même, plus récemment,

---

227. Lien : https://coinmarketcap.com/exchanges/volume/24-hour/
228. Lien : https://www.ccn.com/cryptocurrency-hits-1-billion-revenues-rejects-investors-report/
229. Lien : https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day
230. Pour l'anecdote, la comparaison avec les bénéfices de Deutsche Bank sur la même période (146 milliards de dollars) a été fortement relayée par les réseaux sociaux.

la plate-forme Coincheck s'est fait dérober l'équivalent de 426 millions d'euros. Elle a indiqué qu'elle rembourserait ses utilisateurs à hauteur de 322 millions d'euros.

Le marché des échangeurs est cela dit encore loin d'être arrivé à maturité, puisque, pour dépasser le paradoxe de leur centralisation, de nombreuses initiatives sont en train d'émerger afin de proposer des plates-formes fonctionnant directement sur la technologie Blockchain, comme IDEX ou EtherDelta, mais font face à des problèmes de scalabilité[231]. Citons également d'autres initiatives, comme la maison du Bitcoin à Paris qui propose d'échanger directement des euros en espèce contre des crypto-monnaies et réciproquement[232], ou LocalBitcoins et BitQuick, qui sont des plates-formes d'échange de gré à gré de crypto-monnaies contre de la monnaie fiduciaire.

IV.3 Les régulateurs

Les régulateurs sont les acteurs qui favorisent la sécurisation de l'écosystème en proposant des services visant à encadrer *via* la mise en place d'un cadre juridique de cet écosystème encore en phase de croissance. Ils vont continuer à être un *driver* important des tendances stratégiques du marché. Le risque réglementaire reste un sujet de préoccupation et de risque majeur. Le rôle des régulateurs dans le développement de l'écosystème est primordial et en même temps paradoxal : une régulation est nécessaire afin de créer un cadre et un système de règles permettant au consommateur d'être protégé face aux risques qu'implique un investissement dans les crypto-monnaies (manipulation de cours, délit d'initié, entreprise écran…).

En même temps, une régulation trop forte et trop hâtive risque de freiner le développement de la technologie sur les territoires trop réglementés aux profits de ceux qui le sont moins. En France, ce sont l'ACPR (Autorité de contrôle prudentiel et de résolution), l'AMF (Autorité des marchés financiers) et le législateur qui jouent le rôle de régulateurs du marché.

À ce titre, notons que le régulateur français s'inscrit dans une démarche de dialogue et de progrès avec les acteurs de l'écosystème afin de trouver le bon équilibre réglementaire. La loi Pacte (plan

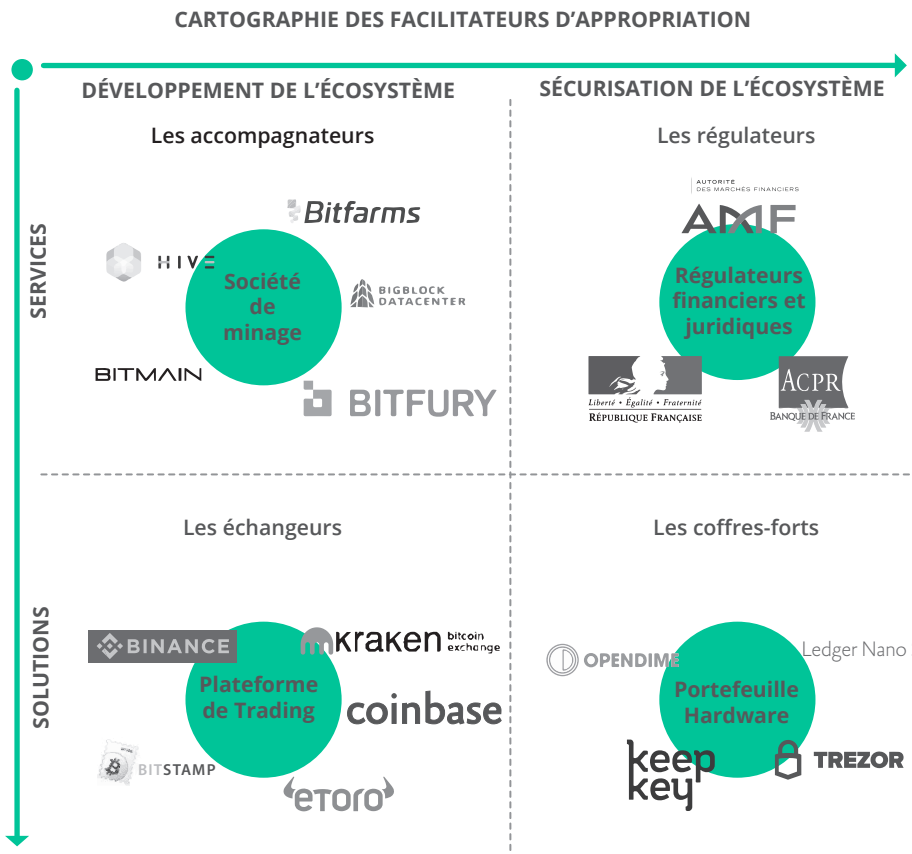
231. Lien : https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79

232. En ce sens, elle s'approche des bureaux de change traditionnels.

d'action pour la croissance et la transformation des entreprises) et la publication du décret d'application de l'ordonnance Blockchain en décembre 2018 en sont deux bons exemples.

IV.4 Les coffres-forts

Les coffres-forts sont les acteurs qui favorisent la sécurisation de l'écosystème en proposant des solutions visant à protéger les porte-monnaie *(wallets)* en crypto-monnaies. En effet, comme nous l'avons vu précédemment, détenir des crypto-monnaies sur des plates-formes Internet comporte un risque non négligeable, puisque le piratage d'une de ces plates-formes implique la perte pure et simple des crypto-monnaies stockées dans les comptes des consommateurs.



Dès lors, pour apporter une couche de sécurité supplémentaire, des acteurs ont développé des solutions *hardware* qui permettent de stocker les clés privées permettant d'avoir accès à ses *wallets* électroniques. Ce mode de stockage *via* le *hardware* permet aux consommateurs de sortir leurs comptes en crypto-monnaies du réseau Internet et donc de se protéger des risques de piratage. Parmi les coffres-forts, nous trouvons par exemple les sociétés Ledger, Opendime ou KeepKey, qui proposent toutes ce type de *wallet* électronique.

En conclusion, les facilitateurs d'appropriation rassemblent ainsi les acteurs de l'écosystème de la technologie Blockchain qui permettent à cette dernière de se développer, de se structurer, et rendent son usage plus simple et plus sécurisé.

V.
Les *process winners*

Les *process winners* sont les acteurs qui considèrent la technologie Blockchain comme un moyen d'améliorer un certain nombre de processus internes des entreprises de l'économie traditionnelle en y apportant de l'automaticité, de la transparence et de la sécurité. Cela permet d'actionner deux leviers de croissance : celui de l'augmentation des revenus et celui de la réduction des coûts. Parmi ces initiatives, certaines sont menées par des acteurs de l'économie traditionnelle qui veulent s'approprier la technologie Blockchain *via* de l'investissement en recherche et développement, des partenariats ou des acquisitions ; d'autres le sont par des start-up appartenant à l'écosystème Blockchain. La collaboration, que ce soit entre acteurs traditionnels, avec des start-up ou avec des projets *open source,* joue un rôle essentiel dans le développement d'usages technologiques propres à l'économie traditionnelle. L'essence de la technologie Blockchain, à savoir un registre distribué entre plusieurs acteurs, explique ce choix de la collaboration. Néanmoins, nous considérons que les *process winners* n'entrent pas dans la *token economy* puisque les acteurs de cette catégorie ne proposent pas de *tokens* en échange de leurs services. En ce sens, le mode de fonctionnement de ces acteurs reste ancré dans le fonctionnement de l'économie traditionnelle.

V.1 Une coopération économique au service de l'innovation

Les entreprises de l'économie traditionnelle cherchent à exploiter la Blockchain pour diversifier leur offre, améliorer l'usage de produits existants ou optimiser leurs *process*. Ces initiatives sont menées la plupart du temps sous forme de consortium ou de partenariats avec des start-up et/ou des projets *open source* :

- Dans le secteur de l'assurance, l'initiative la plus connue à ce jour est celle menée par Axa *via* sa plate-forme Fizzy, qui propose des contrats visant à assurer le consommateur contre les retards d'avion. Le contrat est enregistré sous forme de *Smart Contract* dans la Blockchain Ethereum. L'avantage du *Smart Contract*, comme nous l'expliquions précédemment, est l'automaticité de l'exécution des clauses du contrat : le consommateur, en cas de retard d'un avion, sera remboursé automatiquement selon les termes du contrat, sans démarche[233]. Le site FlighStats joue le rôle d'oracle pour la bonne exécution du contrat : il sera le juge de paix pour déterminer l'heure d'arrivée d'un avion et son éventuel retard, permettant ainsi au consommateur de s'exonérer de la charge de la preuve[234]. La technologie Blockchain apporte automaticité et fiabilité.

- Dans le secteur de la grande distribution, Walmart et JD.com se sont associés à IBM, qui fait figure de leader dans le développement de Blockchains pour l'entreprise, notamment grâce à sa participation active au projet *open source* Hyperledger. Ce projet, hébergé par *The Linux Foundation,* a pour objectif de promouvoir les technologies Blockchain grâce à un travail collaboratif. IBM, en participant à ce projet, a pu s'approprier la technologie Blockchain et participe à de nombreuses collaborations avec d'autres entreprises afin de tester les nouveaux cas d'usage qui pourraient améliorer à terme l'expérience client offerte par des entreprises traditionnelles. Ainsi, IBM s'est associé avec Walmart et JD.com afin d'expérimenter des solutions pour améliorer la traçabilité des produits alimentaires que distribue la société JD.com en Chine. Offrir aux consommateurs l'assurance d'une traçabilité améliorée des produits proposés dans leurs rayons pourrait constituer à terme un avantage concurrentiel non négligeable pour les entreprises de la grande distribution[235]. La technologie Blockchain apporte transparence et fiabilité.

---

233. Lien : https://www.axa.com/fr/newsroom/actualites/axa-se-lance-sur-la-Blockchain-avec-fizzy
234. Lien : https://www.flightstats.com/v2/
235. Roger Aitken, décembre 2017. Lien : https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-Blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#13fb58347d9c

V.2 Collaboration et optimisation

La catégorie « collaboration et optimisation » rassemble les initiatives menées par les entreprises de l'économie traditionnelle qui cherchent à déterminer quels sont les usages de la technologie Blockchain qui pourraient leur permettre d'optimiser des processus internes grâce à une amélioration de la gestion des données. Les entreprises insérées dans l'économie mondiale font face à une complexité croissante de flux de données qu'il est de plus en plus difficile de traiter efficacement. La multiplication des filiales, des réglementations, des sources de revenus, des bases clients, des bases informatiques, demande aux entreprises des outils capables d'apporter à la fois fiabilité, rapidité et transparence dans le traitement des données. Ce dernier point, celui de la transparence, est de plus en plus prégnant puisque c'est une demande à la fois du régulateur et du consommateur. La technologie Blockchain, puisqu'elle apporte une promesse de transformation de ces processus internes, intéresse de nombreux acteurs. À cet égard, des initiatives sont en cours d'expérimentation :

- Dans le secteur bancaire, Australian Securities Exchange (ASX), la place boursière australienne, a annoncé avoir développé, avec l'aide de la start-up Digital Asset[236], une Blockchain permissive permettant d'enregistrer les transactions sans dévoiler le nom du vendeur ou de l'acheteur ni même le montant de la transaction. Tous les détails de ces transactions sont contenus dans des contrats détenus par des banques ou des brokers qui travaillent avec l'ASX. Ces contrats sont ensuite enregistrés et exécutés par une technologie Blockchain jouant le rôle de registre distribué et d'organe de contrôle de la bonne exécution de la transaction, rôle usuellement tenu par les chambres de compensation. La technologie Blockchain apporte ainsi automaticité et vitesse de transaction.

- La start-up Ripple propose également des solutions ciblant le secteur bancaire et, plus particulièrement, les transactions internationales. En effet, *via* sa solution *XCurrent*, Ripple propose un logiciel permettant aux banques de réaliser des transferts internationaux de manière quasi instantanée (contre 3 à 5 jours avec le système actuel). Il est important de souligner que la solution *XCurrent* est une forme de Blockchain privée, complètement dissociée du *token* XRP (ou ripple). En effet, le *token* XRP est le sous-jacent d'une autre offre de la société Ripple (le produit *XRapid*). L'avantage de la solution *XCurrent* de Ripple

236. Lien : www.digitalasset.com/. Digital Asset est une start-up qui a pour ambition de développer des Blockchains permissives dont les applications sont financières. Elle a trouvé 110 millions d'euros de financement et s'est associée avec les plus grandes institutions financières (JPMorgan, Goldman Sachs, BNP Paribas).

est d'apporter, là encore, de la vitesse dans les transactions. Dernière nouvelle en date, JP Morgan vient d'annoncer le lancement (en test) de sa crypto-monnaie privée, indexée sur le dollar, permettant des échanges instantanés entre clients institutionnels et la banque[237].

- Dans le secteur de l'assurance, AIG et Standard Chartered se sont associés à IBM et son savoir-faire développé dans le projet *open source* Hyperledger afin de développer un *Smart Contract* qui permet de mettre en commun des données relatives à des polices d'assurance de quatre pays : Angleterre, États-Unis, Singapour et Kenya. Cette mise en commun permet à des tierces parties (auditeurs ou brokers) d'avoir accès une qualité supérieure de l'information[238]. La technologie Blockchain permet ici une meilleure interopérabilité de l'information partagée par des assureurs couvrant plusieurs pays.

- Dans le secteur de l'énergie, l'EWF (*Energy Web Foundation*) est une initiative de plusieurs grands groupes[239]. Cette collaboration, avec des acteurs comme Blockchain Capital, a mené au développement de la plate-forme Tobalaba. Elle permet de tester les avantages que pourrait apporter une Blockchain permissive au secteur de l'énergie, à savoir : partage de l'information, amélioration du réseau de distribution ou transparence des transactions.

En conclusion, les *process winners* rassemblent donc l'ensemble des acteurs, qu'ils soient de l'économie traditionnelle ou des start-up de l'écosystème de la Blockchain, qui ont pensé et développé des applications de la technologie Blockchain pour les entreprises de l'économie traditionnelle. Comme nous l'avons vu, ces applications permettent d'actionner des leviers de croissance liés soit à une augmentation des revenus soit à une baisse des coûts. L'entreprise IBM, *via* son implication dans le projet Hyperledger, est un acteur important du lien entre l'économie traditionnelle (dont il fait historiquement partie) et le nouvel écosystème en train de naître.

---

237. Lien : https://www.latribune.fr/entreprises-finance/banques-finance/blockchain-pourquoi-jp-morgan-cree-sa-propre-crypto-monnaie-jpm-coin-807577.html
238. Lien : www-03.ibm.com/press/us/en/pressrelease/52607.wss
239. TWL, Tepco, SwissPower, Stedin, Statoil, SPgroup, Shell, Sempra Energy, PTTGroup, Innogy, Engie, Eneco, Elia, Centrica, AGL Energy.

VI.
Les crypto-monnayeurs ou les Blockchains 1.0

Les crypto-monnayeurs ou les Blockchains 1.0 sont les acteurs qui ont développé des protocoles décentralisés et s'appuyant sur les couches technologiques les plus en amont de la chaîne de valeur et d'innovation de la technologie Blockchain, à savoir les couches *ledger* (registres) et de transaction. Elles permettent de proposer un usage de la technologie Blockchain uniquement centré autour de la monnaie. Les crypto-monnayeurs regroupent l'ensemble des acteurs ayant développé des crypto-monnaies concurrençant plus ou moins directement le bitcoin, chef de file de cette catégorie. Notons que les projets appartenant aux crypto-monnayeurs sont ceux qui, chronologiquement, sont apparus les premiers[240].

Pour cartographier la catégorie des crypto-monnayeurs, deux axes d'analyse sont proposés. Le premier axe, celui des horizontaux, est la vitesse de transaction : plus une monnaie propose une vitesse de transaction élevée, plus elle peut se substituer aux monnaies fiduciaires qui, en pratique, ont une vitesse de transaction nulle. En effet, il est difficile d'imaginer une adoption massive des crypto-monnaies comme moyen de paiement pour les microtransactions, s'il est nécessaire d'attendre 10 minutes pour que la validation soit effective, comme c'est le cas actuellement pour le bitcoin. Pour améliorer la vitesse de transaction d'une crypto-monnaie, plusieurs leviers sont possibles :

- réduire le temps de validation des blocs ;
- augmenter la taille des blocs et donc le nombre de transactions pouvant y être enregistrées ;
- alléger/modifier le protocole de validation.

Dans ce qui suit, le volume de transactions – ou scalabilité – fera référence à un nombre de transactions par seconde[241] que l'on pourra comparer aux moyens de paiement actuels (comme Visa qui peut supporter plusieurs milliers de transactions par seconde). Avant de détailler les solutions permettant d'améliorer la rapidité des transactions, rappelons qu'avec la manière dont ont été construites les crypto-monnaies, il existe

240. Le projet IOTA est apparu plus tardivement que les autres, mais propose un cas d'usage particulier de sa crypto-monnaie puisque uniquement centré sur les objets connectés.
241. La notion du nombre de transactions par seconde ne doit pas être confondue avec celle d'immédiateté des transactions.

un compromis presque inextinguible entre vitesse et sécurité. Si l'on prend le cas du Bitcoin, sa sécurité provient du fait que son algorithme de consensus, le *proof-of-work*, permet, comme nous l'expliquions précédemment, d'avoir une sécurité qui tend vers l'infini avec une altération des données historiques impossible. Cette sécurité est garantie par le temps de validation choisi par son créateur, de l'ordre de 10 minutes. Si l'on réduit ce temps de validation, la sécurité en pâtit puisqu'il serait plus facile de modifier l'historique des transactions. Pour dépasser ce compromis, des projets tentent d'imaginer de nouveaux moyens de validation.

Le second axe, celui des verticaux, est le niveau de confidentialité : une monnaie dont le niveau de confidentialité est total n'aura pas nécessairement le même usage qu'une monnaie avec un niveau de confidentialité moindre. Les monnaies ayant un niveau de confidentialité moindre, ou pseudo-anonyme, sont des monnaies où, à chaque *wallet,* est associé un montant connu de tous sans qu'on connaisse l'identité de celui qui le détient. C'est le cas, par exemple, du bitcoin. Ce type de monnaie propose un usage similaire à celui de la gestion d'un compte en banque où on échange des sommes d'argent *via* des virements[242]. Les monnaies ayant un niveau de confidentialité important, ou parfaitement anonyme, sont des monnaies où l'on ne connaît ni le montant associé à chaque *wallet* ni l'identité de celui qui détient le *wallet*. Ce type de monnaie propose un usage similaire à celui qu'on peut avoir de l'argent liquide et s'applique ainsi plutôt au micropaiement. Comme le cas d'usage de ces monnaies est centré autour de la notion d'argent liquide et d'anonymat, il n'est pas à exclure qu'elles puissent favoriser certaines transactions illégales comme l'achat d'armes ou de drogues.

Ces deux axes font apparaître trois catégories que nous détaillerons dans ce qui suit :

- *Bitcoin and its fellows* (le bitcoin et ses dérivés) ;
- *Secret money* (les solutions confidentielles) ;
- *High Tech' money* (les solutions de dernière génération).

VI.1 Bitcoin *and its fellows*

Le bitcoin étant la première crypto-monnaie, sa technologie présente des limites que certains projets ont cherché à dépasser. Le code source

242. Cet usage pourrait être utilisé par des entreprises commerciales effectuant des virements réguliers de montants importants nécessitant donc une sécurité maximale.

du Bitcoin est *open source*, c'est-à-dire complètement libre d'accès en ligne. Les projets de cette catégorie se sont contentés de repartir du code source et de modifier des paramètres, à la marge. À cet égard, on peut parler de *code is business* puisque le code est adapté pour répondre à un besoin du marché. Les principales modifications concernent le temps de validation et la taille des blocs. Parmi les plus connus, citons le Litecoin, le Bitcoin Cash, et le Dogecoin.

Le temps de validation d'un bloc pour le protocole Bitcoin est de 10 minutes environ. Si l'on rapporte ce temps de validation par bloc en équivalent transactions, on estime que le protocole Bitcoin permet d'en valider 3 par seconde environ, contre 2 500 pour Visa. Pour obtenir une validation plus rapide des transactions, le protocole Litecoin, qui s'appuie sur le protocole Bitcoin, propose une validation de bloc toutes les 2 minutes 30 environ[243].

Le protocole Dogecoin propose de son côté une validation de blocs toutes les minutes environ. L'objectif du dogecoin est ainsi de devenir la monnaie de pourboires d'Internet : un utilisateur ayant bien aimé une vidéo ou un tweet pourrait laisser quelques dogecoins, dont la valeur est avant tout symbolique[244]. Le projet Dogecoin est à l'origine une plaisanterie dont le but est de montrer la facilité avec laquelle on peut créer une crypto-monnaie à partir du code source Bitcoin. Néanmoins, cette plaisanterie a reçu un accueil favorable de la communauté Blockchain.

La taille maximale d'un bloc pouvant être validé par le protocole Bitcoin a été fixée par ses créateurs à 1 Mo. Cette limite peut avoir comme conséquence de saturer le réseau, ce qui entraîne un allongement du temps de transaction. L'augmentation de la taille maximale d'un bloc a longtemps fait l'objet de discussions entre les mineurs du réseau. Aucune position ne permettant de concilier les deux clans, un *fork* définitif a eu lieu au début du mois d'août 2017. Il a donné lieu à la création du protocole Bitcoin Cash qui permet de porter la taille maximale d'un bloc pouvant être validé à 8 Mo. Il est intéressant de noter que, jusqu'à la date de leur séparation (1er août 2017), les deux protocoles possédaient le même historique de transactions[245].

---

243. Lien : https://litecoin.org/fr/
244. Lien : dogecoin.com/. Le Dogecoin est représenté par une tête de Shiba, très populaire dans les communautés Internet.
245. Lien : https://www.bitcoincash.org/

VI.2 *Secret money*

Les monnaies complètement anonymes répondent à un besoin imparfaitement adressé jusqu'à présent par les crypto-monnaies : le *cash* digital. Elles s'inspirent également du code source du Bitcoin, mais changent plus radicalement sa philosophie en incluant cette notion de pur anonymat. Parmi les plus connues, citons le dash, le ZCash, le monero, et le verge. Si les niveaux de confidentialité proposés sont très adaptés aux transactions illégales, et notamment du *dark web*, en réalité, ce besoin dépasse largement ce cadre. Nous avons mentionné les cas de restriction des sorties de devises dans des états au contrôle strict des changes. ZCash a également récemment développé des solutions pour le compte de Quorum (Blockchain de JPMorgan[246]).

Le protocole Bitcoin assure un certain niveau de confidentialité à ses utilisateurs grâce à l'existence des clés privées et publiques. Il a néanmoins été pensé pour que l'on puisse accéder au registre des transactions et connaître, *via* la clé publique, l'origine des fonds transférés, le montant et le destinataire. C'est le principe même du protocole Bitcoin : être un registre distribué dont l'ensemble des transactions passées est consultable à n'importe quel moment et par n'importe qui.

Le protocole Dash a pour ambition d'être une monnaie équivalente au *cash* mais digitalisée[247]. Pour cela, son créateur, Evan Duffield, a imaginé deux technologies venant se superposer au protocole Bictoin : l'*InstantSend* qui propose une transaction de manière immédiate et *PrivateSend* qui propose aux utilisateurs qui le souhaitent une confidentialité totale quant aux transactions.

Le protocole ZCash propose, grâce au concept de la preuve sans connaissance *(zero knowledge proof)*, une monnaie où l'anonymat des transactions est total. Ainsi, en utilisant le ZCash, un utilisateur peut choisir de cacher l'origine, le montant et le destinataire de la transaction. Néanmoins, grâce au concept de preuve sans connaissance, le protocole ZCash permet de garantir que l'événement (la transaction) a bien eu lieu sans fournir d'informations à son sujet (origine, destination, montant[248]).

Le protocole ByteCoin repose sur la technologie *CryptoNote*. Il n'est donc pas un *fork* du Bitcoin mais crée une Blockchain nouvelle. L'intérêt de la technologie *CrytpoNote* est de proposer un niveau de confidentialité

246. Victor Abraham, « JP Morgan ajoute la technologie de ZCash à sa Blockchain Quorum », 17 octobre 2017. Lien : https://cryptoactu.com/blockchain/jpmorgan-ajoute-technologie-de-zcash-a-blockchain-quorum/
247. Lien : https://github.com/dashpay/dash/wiki/Whitepaper
248. Lien : https://www.google.fr/search?q=Zcash&oq=Zcash&aqs=chrome..69i57j0l5.1493j0j7&sourceid=chrome&ie=UTF-8

élevé ainsi qu'un temps de transaction d'environ 2 minutes. Notons que de nombreuses autres monnaies sont nées d'un *fork* du byteCoin, comme le monero (qui modifie des caractéristiques de l'augmentation de la vitesse du minage, et utilise une technique dite *one time* pour les adresses publiques ce qui rend impossible de tracer le solde d'un compte[249]).

Le Verge propose « une protection de notre intimité digitale » grâce à l'utilisation de réseaux multiples axés sur l'anonymat, comme Tor et i2p où les adresses IP des utilisateurs sont complètement cachées et par, conséquent, les transactions sont intraçables.

VI.3 *High Tech' money*

Les monnaies *High Tech'* visent à dépasser assez largement le protocole du Bitcoin ; elles proposent des usages nouveaux des crypto-monnaies tout en apportant des réponses technologiques aux principales critiques et/ou limites du bitcoin, à savoir :

- son manque de scalabilité ;
- ses frais de transaction qui peuvent s'avérer élevés ;
- le problème de la consommation d'énergie liée au *proof-of-work*.

Parmi ces initiatives, citons les plus connues : le Iota, le Nano et le OmiseGO.

Le Iota est une monnaie qui diffère totalement, sur un plan technologique, du protocole Bitcoin. En effet, il a pour objectif de se passer du principe de bloc, pourtant fondamental pour une Blockchain, au profit d'une dislocation des nœuds de validation. C'est une monnaie qui s'applique aux objets connectés. L'idée est de mettre à disposition la petite puissance de calcul, embarquée dans chaque objet connecté, pour valider les transactions, confondant ainsi la notion de mineur et d'utilisateur du réseau. Dès lors, il n'est plus nécessaire de concaténer l'ensemble des transactions dans un bloc pour les valider. Le nom de ce mécanisme est le *Tangle* qui s'appuie sur un *Directed Acyclic Graph* (graphe orienté acyclique) pour enregistrer les transactions[250].

---

249. Lien : whitepaperdatabase.com/monero-xmr-whitepaper/

250. Ce concept est très technique et demande un niveau de maîtrise en mathématiques important pour pouvoir être appréhendé pleinement. Il a été formalisé par Sergei Popov, un mathématicien de renom de l'université Unicamp, au Brésil, membre actif de la communauté des crypto-monnaies. La formalisation est accessible *via* le lien suivant : https://iota.org/IOTA_Whitepaper.pdf

Le Nano, anciennement connu sous le nom de Railblock, est assimilable au Iota dans le sens où le concept de mineur et d'utilisateur est plus ou moins confondu[251], mais il ne s'applique pas aux objets connectés. Son cas d'usage est concentré sur une efficacité maximale autour des transactions : elles se valident en 2 secondes, sans frais de transaction et avec une scalabilité présentée comme infinie[252].

Le omiseGO est une monnaie particulière qui s'appuie, elle, sur la Blockchain Ethereum pour être déployée et pourrait être, à ce titre, assimilée à une c*rypto-aps'* (cf. ci-dessous). Nous faisons cependant le choix de la classer dans la catégorie des crypto-monnaies, puisque son cas d'usage est essentiellement centré sur les paiements à partir des applications ou sites Internet. OmiseGO propose une technologie de stockage et de transfert d'argent en temps réel qui est agnostique aux juridictions, aux organisations et au type de monnaie traitée – monnaie traditionnelle et crypto-monnaie confondues. Le *token* OmiseGO n'est pas, à la différence des monnaies citées précédemment, un moyen d'échange, mais il est utilisé pour valider des transactions et permet d'obtenir des remises et/ou des récompenses lorsqu'on passe par lui pour effectuer un règlement.

En conclusion, la catégorie des crypto-monnayeurs rassemble les acteurs ayant développé des crypto-monnaies à usage purement monétaire. Ils ont souvent créé des initiatives dérivant légèrement du code source du protocole Bitcoin en y incorporant de légères modifications sans changer fondamentalement le produit proposé même si certaines crypto-monnaies ont été créées avec des changements plus importants dans les protocoles comme le ZCash ou le Bytecoin. Résultat : on compte aujourd'hui plus d'une trentaine de crypto-monnaies à usage purement monétaire. Nous avons donc fait le choix de limiter les exemples à celles ayant les capitalisations boursières les plus importantes (en fin d'année 2017). Comme nous l'expliquions précédemment, il n'est pas à exclure que l'émergence des crypto-monnaies ait fait naître, presque *ex nihilo*, un grand nombre de monnaies concurrentes dont la viabilité à long terme est faible. Elles fournissent néanmoins un exemple de la théorie des monnaies concurrentes de Hayek : la sélection des bonnes et de mauvaises monnaies sera faite, sur le long terme, par les choix des consommateurs.

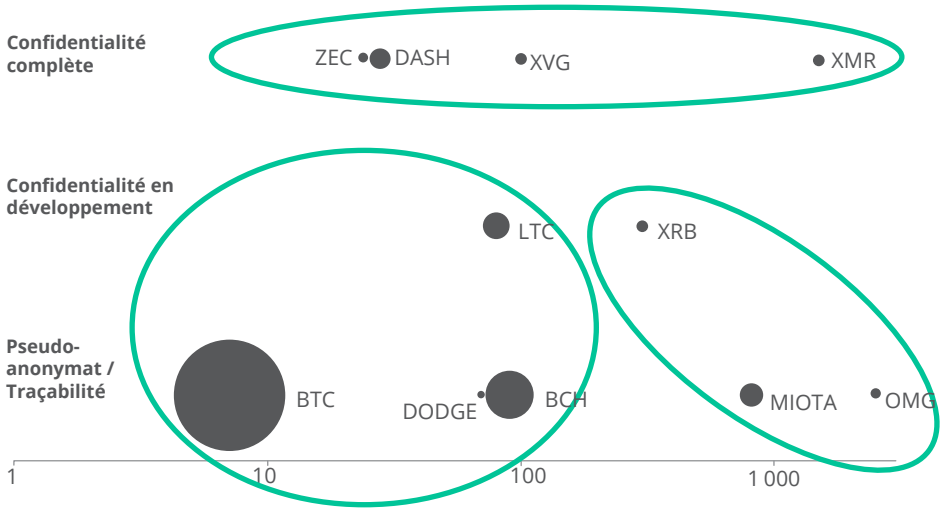
Les crypto-monnaies évoquées précédemment se répartissent donc de la manière indiquée sur le graphique suivant. Notons que la taille des points noirs représente la capitalisation boursière, calculée en fonction

251. Le Iota repose sur le *Tangle* pour ce mécanisme alors que le Nano repose sur le mécanisme dit *block lattice* ou « bloc tressé », qui reprend néanmoins le principe d'une implémentation d'un graphe orienté acyclique.
252. Lien : https://nano.org/en/whitepaper

du nombre de monnaies en circulation multiplié par le prix unitaire. Nous avons retenu les données au 31 décembre 2018. Les transactions sont exprimées en transactions par seconde avec une échelle logarithmique.

Notons dans les nouvelles cryptomonnaies l'apparition de Grin, fonctionnant sur le protocole MimbleWimble. Ce protocole permet des transactions anonymes tout en réduisant le nombre d'informations stockées, et donc le poids informatique de la Blockchain. Les blocs de Grin sont validés toutes les minutes sans limite de création monétaire.

RÉPARTITION DES MONNAIES PAR NIVEAU DE CONFIDENTIALITÉ ET VITESSE DE TRANSACTION (NOMBRE DE TRANSACTIONS PAR SECONDE)[253]



VII.
Les DApps et les Blockchains nouvelle génération

La catégorie des *crypto-aps'* est un ensemble plus vaste et plus complexe que celle des crypto-monnayeurs. En effet, elle rassemble les acteurs en aval de la chaîne de valeur, dont les usages dépassent

253. Sources : CoinMarketCap pour les capitalisations et *whitepapers* des projets pour les vitesses de transactions.

largement le purement monétaire, et porte en germe un changement radical de paradigme économique. Comme nous l'expliquions précédemment, la technologie Blockchain a ouvert la voie à la *token economy* où une entreprise propose un service et une crypto-monnaie permettant d'acheter ce service. Elle devient, par conséquent, à la fois une entreprise de l'économie traditionnelle dont le modèle économique repose sur le bien ou service vendu et en même temps une banque centrale qui émet sa propre monnaie. Cette dislocation de l'espace monétaire crée ainsi un écosystème s'apparentant à un système parallèle, où chaque usage ou service est adossé à une valeur propre dont la valeur fluctue en fonction d'autres crypto-monnaies de référence. Dans cet écosystème en formation, les crypto-monnayeurs pourront avoir un rôle double : unité de compte par rapport à tous ces *tokens* d'usage et moyen d'échange dans l'écosystème.

Pour autant, la catégorie des *crypto-aps'* n'est pas homogène : une nouvelle topographie est nécessaire afin de comprendre les rôles et les spécificités de chacun de ses acteurs.

Cette topographie distinguera donc d'une part les acteurs fournissant une infrastructure aux *crypto-aps'* (les *Chain Producers*) et ceux utilisant cette infrastructure pour développer des applications et des usages (les *Chain Users*).

VII.1 Les *Chain Producers*

La catégorie des *Chain Producers* rassemble l'ensemble des acteurs ayant développé leur Blockchain et dont l'usage par les *Chain Users* est monnayé dans la crypto-monnaie créée. D'une certaine manière, les *Chain Producers* pourraient être assimilés aux constructeurs d'autoroute qui fournissent l'accès au réseau routier d'un pays en contrepartie de quoi ils sont rémunérés à l'usage *via* les péages. À la différence près que chaque autoroute créée disposerait de sa propre monnaie.

Le pionnier des *Chain Producers* est Ethereum qui, comme nous l'expliquions précédemment, fut la première entreprise à créer des *Smart Contracts* venant s'agréger à la Blockchain Ethereum. En ce sens, elle est souvent dénommée « Blockchain 2.0 » en comparaison de la Blockchain Bitcoin et ses équivalentes (Blockchains de première génération ou « 1.0 »).

Ainsi la Blockchain Ethereum comporte une sorte de plate-forme, sur laquelle il est possible pour un développeur (langage Solidity) de bâtir un

écosystème auquel est adossé un *token*. Les transactions seront effectuées et tracées dans la Blockchain Ethereum. De nombreuses autres compagnies proposent une Blockchain dont l'usage est équivalent à celle d'Ethereum à quelques caractéristiques près. Parmi ces compagnies, les plus importantes en capitalisation sont :

- Ethereum Classic, née d'un *hardfork* avec Ethereum, c'est-à-dire une séparation de la Blockchain en deux lignées distinctes. Les différences techniques avec Ethereum sont relativement faibles[254] ;
- Cardano, développée par une équipe de chercheurs et d'ingénieurs japonais ;
- Neo, une initiative soutenue par le gouvernement chinois[255] ;
- EOS. Le protocole EOS est aujourd'hui le concurrent le plus sérieux d'Ethereum. Après une levée de fonds via ICO de plus de 3 milliards d'euros, EOS offre une infrastructure plus rapide et moins chère qu'Ethereum, bien que naissante.

Ces nouvelles initiatives cherchent à dépasser les limites d'Ethereum, notamment en ce qui concerne la capacité de la Blockchain à soutenir de grandes quantités de transactions et à proposer un système de minage ayant une consommation d'électricité moindre. Elles sont souvent appelées « Blockchain 3.0 », ou Blockchains de 3e génération.

Bien qu'Ethereum soit une révolution par rapport au protocole Bitcoin, il n'en demeure pas moins que sa capacité à gérer de grandes quantités de transactions pose encore question. À titre d'exemple, le déploiement d'un des premiers jeux sur la Blockchain, les *cryptokitties*, a eu pour effet de la saturer du fait du trop grand nombre de transactions que le jeu engendrait[256].

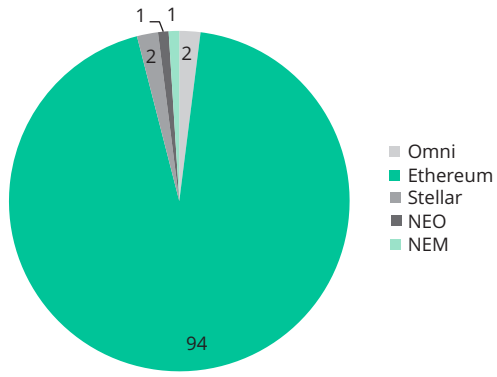
Quant à la consommation d'énergie, les Blockchains 3.0 utilisent des algorithmes de consensus pour valider les blocs moins énergivores, comme le *proof-of-stake* pour Cardano ou le *Delegated Byzantine Fault Tolerance* pour NEO.

Notons tout de même qu'à l'heure actuelle, Ethereum reste la Blockchain la plus utilisée et la plus adaptée pour construire des applications. En effet, sur les 100 plus grosses applications (en

254. Article publié sous le pseudonyme « Hindou », juin 2017. Lien : https://Blockchainmag.fr/comprendre-la-difference-entre-ethereum-et-ethereum-classic/coni
255. Initiative non exempte de critiques par les experts. Lien : https://blockchainpartner.fr/blockchain-neo-imposture/, 20 mars 2018.
256. Juliette Raynal, décembre 2017. Lien : https://www.usine-digitale.fr/article/cryptokitties-l-improbable-jeu-de-chatons-virtuels-qui-embouteille-la-Blockchain-ethereum.N623383

« capitalisation de marché », nous reviendrons sur cette notion plus en détail dans l'analyse financière), 94 sont construites sur Ethereum.

RÉPARTITION DES 100 PLUS GROSSES APPLICATIONS PAR *CHAIN PRODUCERS*



VII.2 Les *Chain Users*

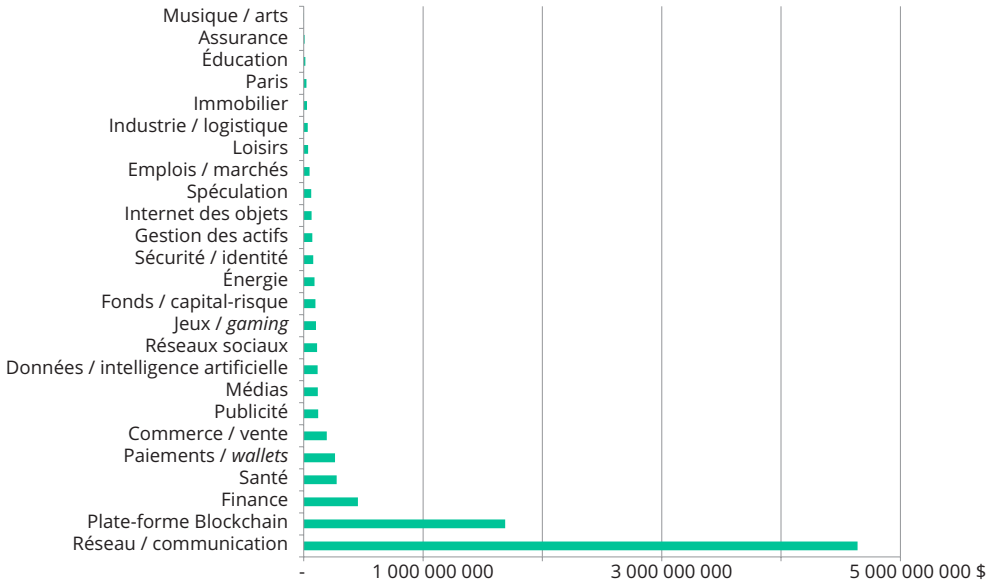
La catégorie des *Chain Users* rassemble l'ensemble des acteurs qui proposent un usage ou un service dont le mode de commercialisation se fait *via* un *token* et se trouvent par conséquent tout en aval de la chaîne de valeur de l'écosystème de la Blockchain. Ces *Chain Users* viennent s'agréger aux Blockchains développées par les *Chain Producers*. Les *Chain Users* constituent l'essentiel des initiatives de l'écosystème puisque l'on compte plus de 2 000 projets pour seulement 70 Blockchains. À noter toutefois que certaines applications reposent sur leurs propres Blockchains, par exemple si les caractéristiques nécessaires ne figurent pas sur les Blockchains existantes.

Pour des raisons pratiques, ces acteurs utilisent la Blockchain Ethereum pour créer leur *token*, selon la norme ERC20 (voir partie C). En effet, cette norme étant la première, elle a été adoptée par l'ensemble des acteurs de l'écosystème, des plates-formes d'échange aux outils de *custody*, améliorant ainsi la manipulation et la liquidité du *token*.

La diversité des projets de cette catégorie en rend impossible une liste exhaustive. La finance constitue un axe d'analyse intéressant que nous étudierons dans une partie dédiée. Ici, l'objectif est de comprendre la nature de ces projets, leur équation économique et le cadre stratégique

dans lequel ils s'inscrivent. L'axe sectoriel est pertinent pour catégoriser ces initiatives et définir les segments de marché auxquels elles s'adressent : banque, assurance, énergie, transport, luxe, grande distribution. La grande majorité de ces projets étant financés par ICO, nous avons utilisé la répartition des montants levés en 2017 par industrie. Ils incluent les *Chain Producers*, dans la mesure où ils se financent également *via* ICO.

RÉPARTITION DES MONTANTS LEVÉS PAR ICO EN 2018 PAR SECTEUR[257]



Les projets ayant levé les sommes les plus importantes *via* ICO sont les plates-formes Blockchain, c'est-à-dire les C*hain Producers*. On peut citer notamment Tezos, start-up française, qui a levé plus de 200 millions de dollars. Cela peut s'expliquer par deux raisons :

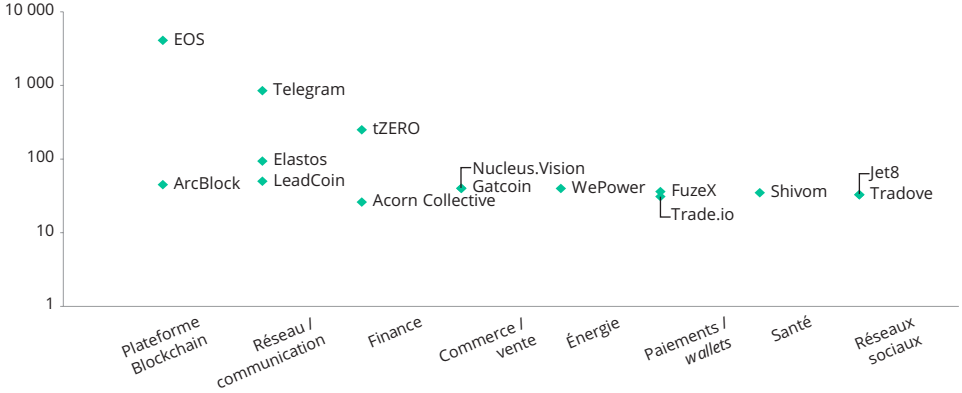
- l'écosystème Blockchain s'est avant tout construit autour de profils experts en informatique et réseaux ;
- les *Chain Producers* représentent, dans la majorité des cas, un potentiel de création de valeur supérieur aux applications (ou *Chain Users*) dans la mesure où ils permettent l'existence de ces applications.

On retrouve ensuite le secteur de la finance et des paiements, domaine d'application premier de la technologie Blockchain. Cela fait écho à

257. Source : https://icowatchlist.com/statistics/categories.

la matrice précédente calibrant l'impact de cette technologie sur les différents secteurs d'activité. Cependant, on peut remarquer que le secteur de l'assurance, pourtant également fortement concerné, concentre moins de projets de type ICO. On retrouve ces secteurs d'activité si l'on considère les quinze plus importantes ICO en 2017.

RÉPARTITION PAR SECTEUR EN VOLUMES DES PRINCIPALES ICO EN 2018[258]



Notons qu'en 2018, Telegram, l'application de messagerie, a réalisé à ce jour la plus grande ICO, levant autour de 1,7 milliard d'USD[259]. Au 11 février 2019, Telegram revendique un taux de complétude de 90 % de son projet blockchain Ton[260].

Comme nous l'évoquions dans la partie dédiée à la technique, de nombreuses applications peinent à trouver leur marché. Certains analystes considèrent que le développement de ces applications était prématuré du fait que les infrastructures ne sont pas encore pleinement stabilisées. Une autre explication est que les expériences client restent imparfaites sur les différentes interfaces. En réalité, de nouveaux projets se sont également contentés de proclamer les bénéfices de la décentralisation, sans forcément les démontrer ou analyser l'existence et les caractéristiques d'une demande en la matière.

Néanmoins, des applications sont utilisées de façon croissante et ont trouvé leur marché. Elles fonctionnent par exemple sur les chaînes Ethereum, Tron ou EOS. Fait intéressant : les industries du jeu et du pari concentrent la plupart des applications (paiements et fidélisation),

258. Lien : https://icowatchlist.com/statistics/year
259. Lien : https://www.coindesk.com/telegram-doubles-amount-raised-in-ico-to-1-7-billion/
260. Lien : https://cryptonaute.fr/crypto-monnaie-telegram-bientot-voir-le-jour/

preuve que la technologie reste encore plus proche de la culture « *geek* » et « *tech* » que du grand public. Historiquement, et ce fut le cas avec Internet notamment, les disruptions ont d'abord été adoptées par les industries dites « à la marge », comme le jeu, les paris ou la pornographie.

Pour les curieux, le site dappradar.com recense les différentes Dapps, les volumes d'échange et les protocoles sous-jacents.

VIII. *Decision Making* : quels leviers d'action pour les acteurs économiques ?

L'approche topographique de l'écosystème de la Blockchain pourrait laisser croire que celui-ci est statique, alors que, comme tout écosystème, il est en perpétuelle mutation : des acteurs naissent, d'autres meurent, certains se font phagocyter dans le cadre d'opérations de fusions-acquisitions *(Mergers & Acquisitions)*. La ruée vers l'or digital se traduit par un jeu d'acteurs multiples, anciens et nouveaux, à la recherche des voies de succès.

VIII.1 Des choix stratégiques

La Blockchain est source de risques et d'opportunités pour l'ensemble de ses acteurs. Des options stratégiques structurantes se dessinent.

Pour les acteurs traditionnels, les possibilités sont diverses. La Blockchain peut être vue comme un moyen d'optimiser les *process* et de réduire les coûts (Blockchains privées, permissives notamment), mais également comme une opportunité de s'adresser à de nouveaux marchés créés par la Blockchain.

D'autres acteurs font le choix de capitaliser sur la vague médiatique en annonçant une ICO. À titre d'exemple, dans le secteur de l'industrie graphique, la société Kodak a annoncé émettre des *tokens*, les KodakCoins, s'échangeant sur une plate-forme dédiée, KodakOne. Cette plate-forme,

nouveau service proposé par Kodak, permettra de gérer les droits liés aux images. Cette application s'adresse aux photographes professionnels ainsi qu'aux agences de photo, pour leur permettre d'enregistrer et de tracer les photos, et de garantir les licences de propriété intellectuelle[261]. La version bêta de cette plateforme a permis à Kodak de générer 1 million de dollars de droits photographiques en octobre 2018.

Certains acteurs adoptent une attitude plus défensive en observant le marché et/ou en contribuant passivement *via* une prise de participation dans un consortium. Dans le cas des *retailers*, la question de l'acceptation des crypto-monnaies comme moyen de paiement, voire de la création de monnaies propres, est un enjeu. Cela dynamiserait-il les ventes ? Comment gérer opérationnellement un tel choix, notamment compte tenu de la volatilité des cours ?

Pour les nouveaux acteurs, il faut distinguer les créations de projet (ICO ou non) des initiatives plus matures. Dans le cas des nouvelles initiatives, l'entrepreneur choisit de réaliser une ICO ou non. Cette dernière n'est pertinente que dans le cas où le *token* émis a réellement un rôle dans l'équation économique. Il est également clé de définir la nature de Blockchain pertinente (publique ou permissive) et de choisir la chaîne appropriée au projet en fonction des besoins *business*. Dans le cas des projets les plus matures, les décideurs peuvent envisager la signature de partenariats à la recherche de complémentarité de modèles (exemple : partenariat entre Changelly et Binance) et d'économies d'échelle (notamment dans le cas des activités de minage ou des plateformes d'échange).

VIII.2 Les dynamiques de fusions-acquisitions

Si le secteur des fusions-acquisitions (hors ICO) n'affiche pas encore des volumes considérables à l'échelle du marché, plusieurs opérations sont enregistrées et témoignent de tendances stratégiques sur le secteur. Le nouveau géant des échanges Coinbase avait acheté et investi dans 27 sociétés en 2018, spécialisées dans l'information, les *security tokens*, l'infrastructure, le *gambling*, les échanges (dont la plateforme décentralisée Paradex). Ces opérations permettent d'offrir des choix stratégiques aux acteurs de l'écosystème, soit par des acquisitions horizontales qui leur permettent de consolider leur position sur leur niveau de la chaîne de valeur, soit par des acquisitions verticales qui leur permettent de diversifier cette position.

261. Lien : https://www.kodak.com/FR/fr//corp/press_center/kodak_and_wenn_digital_partner_to_launch_major_Blockchain_initiative_and_cryptocurrency/default.htm

Pour les acteurs de l'écosystème Blockchain, les acquisitions horizontales se focalisent sur les secteurs où les économies d'échelle et la concentration sont des facteurs clés de succès. Cela concerne en particulier les catégories des :

- *échangeurs,* puisqu'une des composantes principales du succès économique des plates-formes d'échange est leur capacité à traiter un volume d'échanges important et donc à attirer le maximum d'utilisateurs. À ce titre, la plate-forme Kraken est très active puisqu'elle a acheté en 2016 la plate-forme new-yorkaise Coinsetter[262] afin de renforcer sa position sur le marché américain et, plus largement, sur le marché en dollars. Coinsetter avait, quelques mois avant son rachat, elle-même acheté la plate-forme canadienne CAVirtex. Kraken continue cette stratégie de consolidation avec l'achat de la plate-forme néerlandaise CleverCoin, moins de 6 mois après l'achat de Coinsetter[263]. Le partenariat annoncé entre Changelly et Binance s'inscrit dans cette même dynamique de consolidation et de complémentarité, bien qu'il n'y ait à ce stade aucune opération capitalistique en cours[264] ;

- activités de minage (appartenant à la catégorie « facilitateurs d'appropriation ») puisqu'une des composantes du succès d'une ferme de minage est sa capacité à agréger une puissance de calcul importante afin de maximiser ses chances de décrypter l'équation mathématique, et donc d'en toucher la récompense. À ce titre, la société HIVE a racheté de nombreux *data centers* en Islande afin de créer un pôle de minage aux coûts compétitifs (électricité peu chère et refroidissement naturel des ordinateurs lié au climat).

Quant aux acteurs de l'économie traditionnelle, les acquisitions horizontales constituent des options stratégiques pour accéder rapidement à la technologie Blockchain. La plate-forme de logement de particulier à particulier Airbnb a ainsi racheté en avril 2016 la start-up Changecoin pour 16 millions de dollars. L'intérêt de cette acquisition portait moins sur le produit initialement développé par Changecoin – une crypto-monnaie facilitant les micropaiements sur Internet – que sur le savoir-faire des équipes opérationnelles. L'intégration des équipes de Changecoin a permis à Airbnb de disposer d'une équipe d'ingénieurs avec une expérience forte dans le développement de crypto-monnaies. Airbnb pourrait tirer profit de la technologie Blockchain pour encore mieux cibler les profils des utilisateurs, grâce à une traçabilité accrue et l'indélébilité

---

262. Pete Rizzo, janvier 2016. Lien : https://www.coindesk.com/bitcoin-kraken-coinsetter-acquired/
263. Blog Kraken, juin 2016. Lien : https://blog.kraken.com/post/229/kraken-acquires-dutch-bitcoin-exchange-clevercoin/
264. Lucas E., avril 2018. Lien : https://journalducoin.com/exchange/binance-changelly-entrent-partenariat/

des profils[265]. La plate-forme de musique Spotify a racheté en avril 2017 la start-up MediaChain afin de mettre à profit le protocole Metadata, qui permet au créateur d'une œuvre de stocker son empreinte numérique dans la Blockchain Bitcoin. Grâce à l'acquisition de cette solution, Spotify se dote d'un moyen d'améliorer, à terme, la traçabilité des droits d'auteur et d'ainsi rémunérer les artistes à leur juste valeur grâce à une meilleure mise en relation entre eux et les consommateurs[266]. Toujours du côté des acteurs de la Tech, l'acquisition par Facebook de Chainspace (50 personnes environ) en février 2019 n'est pas passée inaperçue et démontre une fois encore l'intérêt des GAFA pour la technologie[267].

Plus récemment, le Nasdaq a annoncé un investissement de 20 milliards dans la start-up Symbiont spécialisée dans les « *smart securities* » (source : Forbes).

Dans le secteur de l'énergie en France, Engie a pris une participation en 2018 dans Blockchain Studio, lui permettant d'avoir un accès facilité aux équipes de développement (source : Engie).

Les acquisitions verticales de l'écosystème Blockchain se concentrent sur la catégorie des facilitateurs d'appropriation. Ces derniers cherchent à proposer une expérience utilisateur complète en ce qui concerne l'interopérabilité entre le système financier de l'économie traditionnelle et celui des crypto-monnaies. Ils sont également la seule porte d'entrée actuelle sur le monde des crypto-monnaies, et représentent donc un enjeu stratégique. Notons que ces acquisitions sont également permises par la fragmentation du marché, encore naissant. À titre d'exemple, la plate-forme Kraken a acheté en décembre 2016 la société Glidera, service d'achat et de vente de bitcoins, reliés à un compte bancaire et stockés directement dans un *wallet*. Cela constitue le premier pas vers la consolidation de l'espace de l'actif digital : l'objectif est ainsi de constituer une offre globale autour de l'accès, la gestion et le stockage des crypto-actifs. Nous pouvons également citer le rachat de Earn.com par Coinbase pour un montant de 120 millions de dollars. Earn.com est une application permettant de recevoir des micromontants versés en crypto-monnaie en échange de réponses à des mails commerciaux (sondages par exemple). La stratégie de CoinBase est de constituer une

265. Biz Carson, avril 2016. Lien : www.businessinsider.com/airbnb-buys-bitcoin-startup-changecoin-2016-4?IR=T
266. Lien : https://techcrunch.com/2017/04/26/spotify-acquires-Blockchain-startup-mediachain-to-solve-musics-attribution-problem/
267. Lien : https://www.lefigaro.fr/secteur/high-tech/2019/02/05/32001-20190205ARTFIG01096-facebook-fait-une-premiere-acquisition-dans-la-blockchain.php

plate-forme intégrant des canaux permettant de rendre plus liquides les crypto-monnaies achetées sur CoinBase[268].

Dans cette optique de créer un acteur globalisé autour des crypto-monnaies, Circle, application mobile de paiement pair-à-pair, qui avait déjà fait un premier pas dans ce monde avec son application Circle Trade app, a acquis récemment Poloniex afin de se placer au centre de l'écosystème. En effet, Poloniex est une plate-forme d'échange américaine de renom, parmi les premières à atteindre 1 milliard d'USD de volume échangé journalier, mais souffrant dernièrement de l'augmentation très forte de la concurrence des plates-formes asiatiques (Binance, Kucoin…). L'objectif est de transformer Poloniex en une place de marché pour l'ensemble des *tokens*, tout en respectant la régulation américaine.

Des regroupements ont également lieu dans le domaine de l'information. Le média Coindesk a acquis en janvier 2017 la plate-forme de suivi de portefeuille Lawnmower. L'objectif est de constituer un acteur central de l'information sur les crypto-monnaies en intégrant les données de marché en temps réel[269].

Les acquisitions verticales de l'économie traditionnelle sont liées à des prises de participation majoritaires ou minoritaires dans des activités de l'écosystème Blockchain à des fins de diversification. Nous citons notamment l'exemple des investissements réalisés par CNP, le Nasdaq, Cardif, aux côtés d'Otium Capital et de Digital Currency Group. Ces opérations s'inscrivent dans du capital investissement, mais avec une logique de complémentarité industrielle. En effet, Stratumn possède notamment des capacités technologiques fortes, très utiles aux acteurs traditionnels pour mettre en place des solutions Blockchain concrètes.

Le groupe japonais Monex Group, dont le cœur de métier est un service Internet de courtage, a acheté en avril 2018 la plate-forme d'échange de crypto-monnaie CoinCheck pour 34 millions de dollars. Cette dernière avait été victime d'un piratage où l'équivalent de 530 millions de dollars lui avait été dérobé[270]. Le groupe Monex Group, par le rachat de cette plate-forme, consolide son offre globale de services financiers en se positionnant sur le nouveau marché des crypto-monnaies.

---

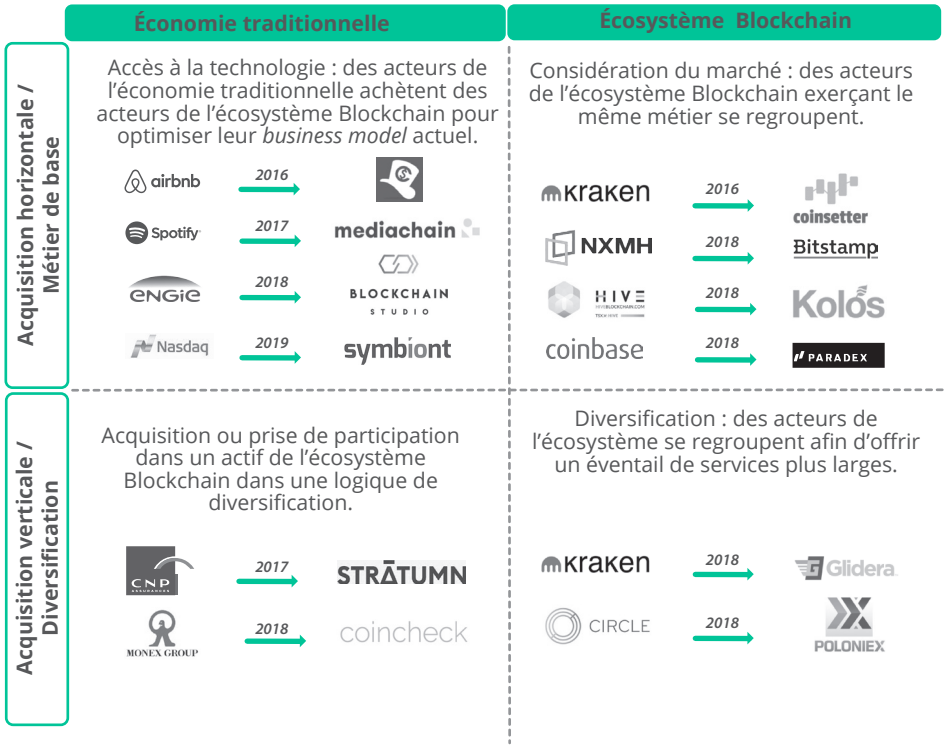
268. Jon Russell, *Coinbase buys Earn.com and makes CEO Balaji Srinivasan its first CTO*, 16 avril 2018, lien : https://techcrunch.com/2018/04/16/coinbase-buys-earn-com-and-makes-ceo-balaji-srinivasan-its-first-cto/

269. Lien **:** https://www.coindesk.com/press-releases/press-release-coindesk-acquires-lawnmower-accelerating-growth-research-offerings/

270. Thomas Wilson, avril 2018. Lien : https://www.reuters.com/article/us-crypto-currencies-coincheck-monex-gro/japans-monex-to-buy-coincheck-for-34-million-eyes-future-ipo-idUSKCN1HD0AE

Le nombre d'opérations de diversification réalisées par ces acteurs reste limité, les choix stratégiques étant principalement orientés à date sur le renforcement des activités centrales.

SYNTHÈSE DES *DEALS* FUSIONS-ACQUISITIONS



Outre les opérations de capital classiquement observées, il est probable que nous assistions à davantage d'investissements en *tokens*, y compris du côté des industriels. À titre d'exemple, la compagnie aérienne Lufthansa a souscrit en *tokens* à la prévente de la société Winding Tree qui propose des applications dans le secteur des voyages.

F

LA BLOCKCHAIN APPLIQUÉE AUX SERVICES FINANCIERS, AUX MÉDIAS ET À L'ÉNERGIE

Comme évoqué précédemment, les cas d'usage sont nombreux et concernent la quasi-totalité de la sphère économique, mais avec une magnitude différente. Nous présentons ici la situation stratégique à date et les perspectives pour les secteurs des services financiers, des médias et de l'énergie.

I.
Les services financiers en première ligne

La Blockchain impacte directement le cœur de métier de la banque, autour de ce que Don Alex Tapscott appelle les *golden eight*[271] : authentification et vérification de l'identité et de son lien avec une valeur, transfert de valeurs, stockage de valeurs (compte en banque, épargne…), prêt de valeurs, financement et investissement, assurance de valeurs et comptabilité[272]. Les services financiers devraient connaître une transformation en profondeur de leurs métiers et des chaînes de valeur. Nous traitons ici le cas de la banque, avec un focus sur la banque d'investissement, et l'assurance.

I.1 La banque : une transformation amorcée, catalysée par la Blockchain[273]

La technologie Blockchain ambitionnait à ses débuts de concurrencer le système financier dans son essence mais pourrait, paradoxalement, constituer une opportunité majeure pour le secteur bancaire. À cet égard, le CEO du consortium R3, David Rutter, qualifiait en mars 2018 la technologie Blockchain « d'opportunité qui ne se présente qu'une fois par génération pour le secteur des services financiers[274] ». Reposant sur les trois piliers technologiques précédemment analysés, elle apporte la promesse de réduire un certain nombre de coûts. C'est donc naturellement que se sont développés des projets ciblés, dans les banques, qui

271. « Les huit points-clés ».
272. Don et Alex Tapscott, *Blockchain revolution*, Portfolio Penguin, 2016.
273. D'après notre contribution au supplément n° 821, juin 2018, p. 43-46 de *Revue Banque*.
274. Lien : https://www.bloomberg.com/news/videos/2018-03-22/r3-ceo-says-Blockchain-is-a-once-in-a-generation-opportunity-for-financial-markets-video

ont rapidement délivré des résultats tangibles, mais des défis subsistent pour une industrialisation à grande échelle. L'écosystème foisonnant autour de la technologie peut également constituer un gisement d'opportunités *business*, mais comporte des risques.

Jusqu'à présent, la vague d'innovation des Fintech avait ciblé la banque de détail en se focalisant sur des innovations en aval de la chaîne de valeur bancaire, *via* notamment des applications transformant l'expérience client. Le segment de la banque de financement et d'investissement (BFI) était jusqu'alors peu impacté du fait de fortes barrières à l'entrée. La criticité des opérations, le coût des infrastructures autour de chaînes de valeur complexes constituent, en effet, des obstacles technologiques et financiers importants pour les nouveaux entrants sur ce segment d'activité. La Blockchain, elle, représente une vraie opportunité technologique pour la BFI. Par conséquent, nous concentrons l'analyse ci-dessous sur les métiers de la banque d'investissement. Bien sûr, les métiers des paiements, transferts internationaux, gestion d'actifs sont également impactés.

Pour ne pas passer à côté de cette opportunité, les BFI ont fait le choix stratégique d'investir dans des consortiums, qui présentent de nombreux avantages. Ils permettent, d'une part, la mise en commun de compétences dans un contexte de risques mutualisés.

D'autre part, ils proposent de diversifier les investissements puisque chaque consortium poursuit une stratégie propre, allant du développement d'infrastructures globales et de logiciels permettant la création d'applications (comme R3 et Digital Asset Holdings) au marché de niche centré sur des cas d'usage précis (Liquidshare pour les petites capitalisations listées et les titres non cotés, ou We.Trade et Marco Polo sur le *trade finance*).

La Blockchain permet donc de créer un univers de coopération entre les banques, au service notamment de l'efficacité, de la standardisation et de la digitalisation. Cette dernière constitue, en effet, une tendance stratégique observée dans le secteur des services financiers, et plus particulièrement dans celui du postmarché pour lequel elle est un enjeu majeur. L'émergence de ces consortiums n'est d'ailleurs pas sans rappeler la volonté d'Euroclear, dans les années 2000, de créer une plateforme unique visant à uniformiser les processus de transmission et de conservation pour les dépositaires français, belges et néerlandais.

Concrètement, ces initiatives vont se traduire par des gains de productivité à court terme, mais sur des activités ciblées, plus particulièrement dans le segment postmarché.

Plus précisément, les banques suivent une approche pragmatique guidée par les opérationnels. Par exemple, Natixis a réalisé en 2017, en partenariat avec Trafigura et IBM, la première solution Blockchain permettant de réaliser des opérations de *trade finance* sur le marché des matières premières. Cette initiative promet une transparence accrue et une efficacité opérationnelle optimisée. Dans le même domaine, Natixis et le Groupe BPCE sont également moteurs dans le consortium We.Trade dont les premiers résultats sont attendus courant 2018. La Blockchain et les *Smart Contracts* sont particulièrement adaptés aux réalités de la chaîne de valeur du *trade finance* dont la forte complexité s'explique par la nécessité de coordonner un nombre important d'acteurs autour de processus de validation lourds et coûteux.

Le segment du postmarché est supposé être le plus directement concerné par la technologie Blockchain mais des initiatives concernent d'autres segments de la chaîne de valeur, par exemple sur d'autres métiers comme la distribution de fonds. BNP Paribas Securities Services (BP2S) fait figure d'acteur majeur de la transformation en ce domaine, en étant moteur auprès de ses clients *Asset managers* et des banques d'investissement. À titre d'exemple, le groupe travaille en partenariat avec Axa IM pour simplifier la collecte de documents réglementaires *Know Your Costumer* (KYC). À plus long terme, l'ensemble de la chaîne de distribution de parts de fonds pourrait se transformer et se restructurer autour de nouveaux canaux de souscription reposant sur des infrastructures de type Blockchain. Récemment, l'entreprise a annoncé avoir réalisé la première souscription de part de fonds *via* un réseau distribué avec une autre entité du groupe BNP Paribas, BNP Paribas Asset Management. Société Générale Securities Services et OFI Asset Management ont également réalisé des ordres de souscription et rachats de parts de fonds *via* la plateforme Iznes (start-up Setl[275]).

La majorité des investissements se concentre encore sur la partie basse de la chaîne de valeur, si bien que les applications *middle* et *front office* se font rares. Le projet LenderComm, mené par Finastra en lien avec BNP Paribas, Natixis, HSBC et ING, constitue cependant un cas d'usage intéressant. Il vise à faciliter les échanges d'informations entre les participants à un crédit syndiqué, allégeant de fait les tâches incombant à l'agent.

Pour le système financier, la Blockchain est une technologie de rupture fondamentale dont l'essence vise une refonte de l'infrastructure globale. Si des premiers cas d'usages concrets sont prometteurs et fonctionnels, une industrialisation à grande échelle nécessitera le développement

275. Lien : https://www.societegenerale.com/fr/Societe-Generale-et-OFI-AM-executent-premieres-Transactions-via-blockchain

d'applications capables d'embrasser la complexité du système existant. Se pose également la question, à court terme, de l'interopérabilité entre les nouvelles infrastructures sur la Blockchain et le Legacy. Puis, à moyen terme, pourrait être articulée une migration progressive mais totale du système actuel vers une économie bancaire « blockchainisée ».

Si les projecteurs sont majoritairement tournés vers l'apport de la Blockchain en tant que pure technologie, au service de gains de productivité (difficiles à quantifier pour le moment), son potentiel est bien plus large. Il pourrait représenter des relais de croissance et des sources de diversification pour les acteurs qui sauront le valoriser.

Une séparation nette semble avoir été érigée entre ce que l'on appelle les crypto-monnaies (ou crypto-actifs) – et en premier lieu le bitcoin – et la technologie Blockchain sous-jacente. Dans les faits, on constate des espaces aux contours moins définis. La technologie Ripple, Swift nouvelle génération *via* une Blockchain permissive, est un bon exemple du mélange des genres (technologie testée par le Crédit agricole notamment[276]). Expérimentés par plus de 70 banques, controversés dans la communauté Blockchain du fait de leur centralisation, Ripple et son *token* XRP constituent la troisième capitalisation de l'univers des crypto-actifs, soit plus de 14,4 milliards de dollars fin décembre 2018.

La Blockchain dépasse de très loin les seuls cas d'usage liés aux *process* et pourrait ouvrir de nouveaux marchés, y compris pour les acteurs en place. Les ICO, les plates-formes d'échanges, le métier de conservation *(custody)* et la fusion-acquisition pourraient constituer des relais de croissance pour les institutionnels en capacité de capitaliser sur leur savoir-faire. L'ICO est une opération sur le marché primaire, à l'image des activités des banques d'affaires sur les actions (IPO, *Initial Public Offering*) et les émissions de titres de dette. Les plates-formes d'échange sont des formes de Bourse ; le Nasdaq a d'ailleurs déclaré s'y intéresser et vient de réaliser un investissement de 20 millions de dollars dans Symbiont, une start-up Blockchain (janvier 2019). L'enjeu financier est majeur, en témoignent le 1,3 milliard de dollars de chiffre d'affaires de Coinbase en 2018 malgré la baisse des cours. Sa valorisation était estimée à 8 milliards de dollars en octobre 2018 (Bloomberg.com). Il faut néanmoins être en mesure de gérer le risque de cybersécurité, dans un contexte de *hacking* récurrent des plates-formes existantes. La Blockchain joue par ailleurs un rôle de *custody* puisqu'elle est un registre public et distribué de l'ensemble des transactions. Cependant, un utilisateur, pour avoir accès à ses crypto-actifs, doit être en possession

276. Lien : https://www.credit-agricole.com/chaines-thematiques/toutes-les-chaines-d-info-du-groupe-credit-agricole/actualites-du-groupe/le-credit-agricole-experimente-la-technologie-blockchain-avec-ripple-pour-les-transferts-d-argent

d'un mot de passe cryptographique. Il est la clé d'entrée pour ses comptes et doit être par conséquent protégé. À ce stade, le *off-line storage* (autrement appelé *cold storage*) constitue la meilleure réponse possible à cette problématique. La start-up française Ledger a pris une position majeure sur ce segment, matérialisée par des tours de table impressionnants dans la sphère du *private equity* (75 millions de dollars levés). Les principales plates-formes d'échange proposent des offres d'*online storage*, à l'image de Coinbase et de son service de conservation proposé aux institutionnels. Le marché de la fusion-acquisition est également impacté par l'émergence de cet écosystème, comme nous l'évoquions précédemment, représentant potentiellement un gisement de marché pour les banquiers d'affaires.

Les acteurs bancaires traditionnels semblent avancer avec prudence pour ne pas s'exposer à un risque d'image ou s'aventurer sur des territoires trop éloignés de leur stratégie cœur. Le jeu stratégique entre nouveaux acteurs orientés B2B (comme les consortiums), acteurs traditionnels et nouveaux entrants B2C promet d'être passionnant.

Le futur des paiements

Au global, notre conviction est que l'industrie des paiements reste la plus exposée à une disruption issue de la Blockchain.

La scalabilité limitée du Bitcoin, comparé aux systèmes de paiement actuels, a fait couler beaucoup d'encre et généré de nombreuses confusions. Le Bitcoin ne peut en réalité pas être comparé à Visa sur le plan du nombre de transactions à la seconde, puisqu'il constitue un socle d'infrastructure (*layer* 1 en anglais), alors que Visa est d'avantage un *layer* 2 voire 3. Il est vraisemblable que des projets s'ajoutent à Bitcoin en *layer* 2 et lui permettent de devenir un moyen de paiement compétitif. Le Lightning Network est très prometteur en la matière. L'idée est la suivante : si Alice et Bob échangent régulièrement de l'argent, alors ils peuvent ouvrir un canal dans lequel ils placent un montant de bitcoin, correspondant au montant maximal qu'ils pourront échanger. Seule la situation « finale » sera inscrite dans la Blockchain, permettant ainsi de rendre instantanée toute transaction entre Alice et Bob en bitcoin. Notons également la transitivité des canaux : si Alice et Bob ont ouvert un canal, et Bob et Cédric également, alors Alice et Cédric pourront échanger des bitcoins via le Lightning Network. Trois équipes de développeurs travaillent sur ce projet dont les Français de la start-up ACINQ.

Le futur des paiements passera également par les GAFA et BATX, qui disposent de très larges bases utilisateurs et d'interfaces mobiles. Alipay, la solution de paiement d'Alibaba en est une bonne illustration. La question

est de savoir si les géants de la Tech pourraient être tentés d'utiliser des protocoles pair-à-pair *open source* pour opérer les transactions réalisées via leurs applications. Facebook a toutefois récemment annoncé vouloir utiliser sa propre crypto-monnaie pour réaliser des paiements à travers Whatsapp (Forbes) en Inde. À suivre…

I.2 L'assurance : la confiance comme pierre angulaire de l'activité

Le secteur de l'assurance est naturellement impacté par la Blockchain. De nombreuses initiatives émergent, chez les acteurs institutionnels, avec pour objectif de réduire les coûts ou d'activer des leviers de croissance, et dans un écosystème dynamique de start-up Insurtech/Blockchain. Selon Arup Kumar Chatterjee (spécialiste services financiers, développement et changement climatique de la Banque asiatique du développement) : « La Blockchain reconstruit la confiance entre les assureurs et les assurés grâce à une expérience client améliorée, des coûts réduits et l'innovation produits[277]. » En quoi l'assurance est-elle concernée par la Blockchain ?

Le métier d'assureur repose sur la mutualisation du risque, l'asymétrie d'information et la gestion de l'aléa moral. La réduction des asymétries par davantage de transparence et de traçabilité constituerait par conséquent un facteur majeur de transformation et de simplification du métier. À titre d'exemple, Everledger ambitionne d'utiliser la technologie Blockchain pour garantir des titres de propriété sur des objets de valeur (travaux en cours sur les diamants). Cette innovation permet, entre autres, de lutter contre la fraude. Après une indemnisation consécutive à un vol ou une perte, un éventuel retour à la surface du diamant serait identifié grâce aux informations inscrites dans la Blockchain et l'assureur pourrait agir en conséquence.

Dans la continuité de la vague « assurtech », est-il possible de mutualiser le risque dans une logique pair-à-pair ? Des start-up proposent des approches innovantes, repensant l'asymétrie d'information et l'aléa moral, largement guidées par les thèses de l'économie expérimentale. Prenons deux exemples. L'insurtech israélienne Lemonade (pas spécialisée dans la Blockchain), valorisée fin 2017 à près de 500 millions de

277. Arup Kumar Chatterjee, « How Blockchain can rebuild Consumer Trust in Insurance », 1er mai 2018. Lien : www.brinknews.com/asia/how-blockchain-can-rebuild-consumer-trust-in-insurance/Blockchain is rebuilding trust between insurers and policyholders via improved customer experience, higher scrutiny of affordability, and product innovation.

dollars de dollars, consécutivement à une levée de 120 millions de dollars, propose depuis 2016 une solution d'assurance habitation pair-à-pair. À la fin de l'année, les versements des assurés non utilisés sont redistribués à des œuvres avec l'idée sous-jacente que les acteurs frauderont moins du fait de l'existence d'une cause sociale. Point intéressant : l'économiste spécialiste de l'économie comportementale – déjà cité dans cet ouvrage – Dan Ariely est membre du projet[278].

Autre cas intéressant, la start-up slovène InsurePal (18 millions de dollars levés) qui propose une plate-forme d'assurance décentralisée fondée sur la preuve sociale. Les produits assurantiels proposés par InsurePal reposeront sur des évaluations entre particuliers. Chaque particulier sera incité financièrement à donner de l'information sur un pair et possédera une note de confiance *(Social Proof Trustcore)*. Grâce à ce système novateur, InsurePal prévoit de proposer des assurances dans de nouveaux domaines, grâce à la facilité de mise en place des contrats et leur autonomisation.

La chaîne de valeur de l'assurance est complexe et regroupe de nombreux acteurs : producteur, distributeur, *broker*. Cette multiplicité d'acteurs, couplée à des processus complexes, se traduit par un niveau de transparence insuffisant et des coûts élevés. La Blockchain permet de réintroduire des espaces de coopération entre les acteurs de place, notamment autour de la donnée et sa gouvernance. À l'image du secteur bancaire et de ses consortiums, le monde de l'assurance s'organise et s'est notamment réuni sous le projet *Blockchain Insurance Industry Initiative* (B3i). Développé par un groupement de quinze assureurs-réassureurs européens (Aegon, Allianz, Scor, Generali, Munich Re, Swiss Re et Zurich, entre autres[279]), le consortium oriente notamment ses recherches sur la création d'un registre partagé par tous les partenaires et permettant la facilitation de la mobilité interassureurs.

Les assureurs sont très dépendants de la donnée, de sa qualité et de son utilisation. L'exploitation d'une donnée intrinsèquement qualitative (parfaitement tracée et infalsifiable) de la Blockchain constitue par conséquent un point de rupture majeur.

Les processus d'indemnisation restent lourds et très manuels. Ces processus longs et récurrents pourraient être automatisés par des *Smart Contracts*, comprenant à la fois la souscription et l'indemnisation par

278. Lila Megrhoua, « Lemonade mise sur une assurance ultra-personnalisée, *peer-to-peer* et sociale », octobre 2016. Lien : https://atelier.bnpparibas/fintech/article/lemonade-mise-assurance-ultra-personnalisee-peer-to-peer-sociale

279. Article de l'Agefi, 26 mars 2018. Lien : https://www.agefi.fr/banque-assurance/actualites/quotidien/20180326/assureurs-b3i-concretisent-leurs-travaux-243529

l'exécution des clauses selon une série de conditions (par exemple : dédommager le compte X si la température dépasse strictement 5 °C à telle date). Outre une meilleure expérience client (confiance accrue dans la probabilité de recouvrement), ce point représente une opportunité de réduction de coûts majeurs, permis par l'allégement des lourdeurs et l'instantanéité des tâches. Prenons l'exemple de la plateforme Fizzy qui permet aux clients de se couvrir face aux retards lors de voyages en avion. Si un vol est retardé de plus de 2 heures, un voyageur ayant souscrit à l'assurance sera automatiquement indemnisé. Une fois l'assurance souscrite, le processus est réalisé de façon autonome, quasiment immédiate et l'assuré est indemnisé[280].

Il convient de noter que l'ensemble des sinistres ne seront pas directement gérables par un *Smart Contract* sans aucune intervention d'un tiers de confiance. Par exemple, de nombreux sinistres nécessiteront toujours la constatation par un expert mandaté.

Le marché de l'assurance va poursuivre une transformation en profondeur, portée par les stratégies des grands institutionnels et les projets, plus décentralisés, issus de l'écosystème et des start-up. Des défis subsistent, la faible maturité des technologies et la gestion problématique des oracles (nouveaux tiers de confiance ?) en constituent deux exemples.

II.
Les médias : la Blockchain donne le bit[281]

Pour l'industrie des médias, le développement de l'informatique s'est révélé à la fois une opportunité de développement sans précédent et une apparition de nouveaux défis, avec principalement celui de la gestion des droits d'auteur d'actifs digitaux, à une échelle globale, et la traçabilité de l'information. Actuellement, le fossé séparant les nouveaux types de litiges digitaux de ceux pris en charge par la législation est en croissance continue, et les institutions judiciaires peinent à s'adapter à cet environnement en mutation rapide.

---

280. Lien : https://www.axa.com/fr/newsroom/actualites/axa-se-lance-sur-la-Blockchain-avec-fizzy

281. Inspiré du mémoire de Pierre-Louis Terry, ancien élève d'HEC et collaborateur d'Accuracy, sous la direction de M. Thomasz Michaslki.

L'un des enjeux principaux de la digitalisation consiste à établir un encadrement juridique clair et complet, afin que les opportunités mises à jour par cette technologie soient de nature à soutenir la croissance économique de ce secteur, et non à accentuer son essoufflement. Or, la possibilité de dupliquer l'information digitale à l'infini, quel qu'en soit le support (textuel, musical, vidéo, photographique…) soulève le problème de la gestion des droits d'auteur. Dans un premier temps, l'apparition du piratage en ligne a opposé les artistes souhaitant utiliser Internet pour promouvoir leurs travaux à une échelle plus globale, au public simplement désireux de réduire les coûts associés à la consommation de ces médias. Depuis, ce contexte s'est généralisé à l'ensemble des supports, avec l'apparition du *streaming* (pour la musique et la vidéo), des sites d'information et de désinformation, ainsi qu'avec le développement des réseaux sociaux comme plates-formes privilégiées de relais de l'information. En conséquence, ce sont autant d'infractions juridiques, nées en contrepartie des innovations technologiques (duplication de fichiers, *streaming*, piratage…), qui font chuter les revenus des producteurs de contenu, au profit d'intermédiaires.

La technologie Blockchain permet déjà aux acteurs de l'industrie d'imaginer deux catégories de solutions pour répondre à ces nouveaux enjeux. La Blockchain se caractérise par l'établissement d'une information à la fois transparente, fiable et immuable : des concepts fondamentaux qui, appliqués à l'industrie des médias, participeraient à son développement[282].

D'une part, la technologie Blockchain constitue une fondation prometteuse pour structurer une base de données de droits d'auteur décentralisée et accessible au plus grand nombre, afin de permettre et de faciliter les processus transactionnels liés à l'utilisation légale de contenu protégé. D'autre part, l'utilisation des *Smart Contracts* représente également un moyen d'automatiser, tout au moins partiellement, les transactions liées aux paiements de droits d'auteur, afin de fluidifier le processus.

L'établissement d'une base de données de droits d'auteur vise à rendre l'information juridique transparente et accessible au plus grand nombre, afin de faciliter et d'encourager l'utilisation de contenus protégés en échange des paiements dus. De fait, cette information reste fragmentée encore aujourd'hui entre les grands acteurs du secteur, chacun détenant sa propre base de données sans en ouvrir l'accès au public. Ainsi, consolider ces bases de données revient à se heurter aux acteurs récalcitrants à la publication de leurs données, ainsi qu'à faire face aux enjeux techniques d'intracompatibilité et d'interopérabilité entre chacune de ces bases.

---

282. Marc S. Pritchard, *Chief Brand Officer* chez P&G, décrit l'industrie des médias comme « au mieux trouble, au pire frauduleuse ».

La technologie Blockchain constitue une réponse pertinente à cette question en cela qu'une base de données décentralisée (donc sans autorité centrale), dont le contenu est fiable, transparent et mis à jour en temps réel, résout par construction les problèmes liés à la gestion de l'information à l'échelle de l'industrie. Le projet est actuellement en développement dans l'industrie de la musique, avec la création d'un format de fichier (.bc) permettant de réunir l'ensemble des informations décrivant une pièce musicale, afin que le public y ait accès. Plusieurs organisations et entreprises telles que l'Open Music Initiative, DotBC Open Source Project, ou encore DotBlockchainMusic travaillent en concurrence ou de concert, afin de répondre aux difficultés techniques inhérentes à ce type de projet, représentant un défi tout aussi technique que managérial. Les structures, présentées au cours de conférences, mettent en avant une architecture concentrique où les données enregistrées servent à la fois de référence pour l'industrie, et de base sur laquelle faire des analyses de tendances et de prévisions du marché.

L'idée derrière ces initiatives est d'organiser une base de données de tous les fichiers musicaux créés par les artistes, afin de faciliter l'accès aux informations pertinentes les caractérisant. Le format spécifique .bc évoqué doit permettre d'intégrer l'ensemble des informations (nom, taille, durée, auteurs, compositeurs, interprètes, ayants droit, informations commerciales et juridiques…) de façon cohérente. Ces fichiers sont assimilables à des blocs, en cela qu'ils ne contiennent qu'une information textuelle, et doivent répondre aux mêmes critères de fiabilité, et de sécurité qu'un bloc dans une chaîne. Cette architecture concentrique s'organise autour de la réunion de ces fichiers .bc. Elle se fonde sur quatre cercles fondamentaux, sachant que la communication d'un cercle à l'autre se fait *via* la Blockchain. Le premier cercle représente l'ensemble des fichiers .bc réunis dans le système. Ces fichiers sont rassemblés et distribués sur la Blockchain afin de donner aux informations qu'ils contiennent le caractère immuable propre à la Blockchain. Le deuxième cercle utilise un ensemble d'algorithmes, actuellement employés massivement dans les réseaux sociaux, afin de structurer les informations de la base de données en un ensemble utilisable, afin de réaliser des analyses, notamment tendancielles et prédictives à l'échelle de l'industrie. Leurs résultats constituent un support afin de faciliter les processus de collaboration et d'utilisation de contenus protégés, dans un cadre juridiquement normé. Le troisième cercle représente l'interface à partir de laquelle les acteurs de l'industrie peuvent accéder aux données, les compléter et les mettre à jour. Bien entendu, si les erreurs de saisie et les manipulations restent possibles dans une telle structure, la Blockchain permet de réduire leur temps de détection. Le dernier cercle a pour but d'organiser les relations entre cette structure et l'ensemble des systèmes de gestion de l'information actuellement en vigueur dans l'industrie, afin d'assurer une interopérabilité optimale, de sorte que

tous les agents de l'industrie (maisons de disques, agrégateurs, artistes, compositeurs, auteurs…) puissent garantir ensemble la qualité de l'information disponible.

Le but, à terme, est de lutter contre la culture des boîtes noires dans cette industrie, de dissuader l'utilisation illégale de contenus protégés, et de rééquilibrer la chaîne de valeur par une distribution plus transparente sinon plus juste des revenus générés[283]. Bien entendu, l'établissement d'une telle base de données bénéficierait au développement économique futur de l'industrie des médias dans son ensemble, par exemple en mettant à jour de nouvelles opportunités et de nouveaux marchés. Un tel projet nécessiterait des changements structurels au sein de l'industrie, conditionnés à leur acceptation par les acteurs impliqués.

L'adoption de ce projet par l'industrie de la musique représenterait un changement de paradigme profond, et serait un indice de compatibilité entre l'industrie des médias dans son ensemble et ce mode de fonctionnement décentralisé. Mais ce projet est encore en phase de développement et nécessitera plusieurs années de travail avant d'être opérationnel. Si la généralisation de cette base de données de fichiers musicaux aux médias digitaux en général, tous types confondus, constitue un défi à part entière, celui-ci ne prendrait qu'une dimension purement technique après vérification de la compatibilité du système avec l'industrie. La difficulté principale réside donc dans son acceptation par l'industrie. L'application d'une structure équivalente à l'industrie des médias ouvrirait la voie notamment vers de nouveaux standards de qualité de l'information, grâce à une technologie permettant sa traçabilité parfaite, depuis son point d'origine jusqu'à l'utilisateur final.

En complément de cet axe de développement majeur dans l'industrie des médias, l'utilisation de la technologie des *Smart Contracts* est également prometteuse, car elle permet à la fois de fluidifier le processus transactionnel en l'automatisant partiellement et de limiter les intermédiaires. L'application de cette technologie à l'industrie des médias représente une simplification importante du processus, complexe par nature, qu'est le rachat de droits. Cependant, cette complexité tient davantage des rigidités structurelles de l'industrie actuelle que d'une difficulté inhérente à la procédure elle-même. Ainsi, les *Smart Contracts* forment une solution complémentaire avec l'établissement de bases de données décentralisées ; le premier système fluidifie le processus transactionnel entre les acteurs de l'industrie en supprimant les intermédiaires, tandis que le second fournit l'ensemble des informations pertinentes requises

283. La notion de justesse ici employée fait écho à la distribution de la valeur ajoutée créée par chaque acteur de la chaîne de valeur traditionnelle dans l'industrie musicale. La disruption de la chaîne de valeur traditionnelle grâce à la digitalisation tend néanmoins à long terme à ajuster cette distribution.

pour réaliser ces transactions, tout en garantissant leur fiabilité et leur traçabilité d'un bout à l'autre de la chaîne de valeur.

L'industrie du cinéma mériterait également à elle seule un long développement. Dans un contexte de chaîne de valeur complexe, elle souffre de problèmes de faible transparence de la répartition de valeur.

III.
L'atomisation du marché de l'énergie[284]

III.1 Les évolutions du secteur

Le secteur de l'énergie est en pleine mutation, sous l'effet conjugué d'une dérégulation impulsée par le législateur et d'une évolution profonde des technologies et des usages. Les ambitions sont élevées pour transformer cette industrie mature en laboratoire d'expérimentations scientifiques et *business*, avec des modèles construits autour de solutions digitales innovantes au service du consommateur. Les thèmes récurrents concernent, entre autres, le déploiement des réseaux intelligents (ou *smartgrids*), le développement de la mobilité électrique, l'essor du photovoltaïque et d'autres moyens de production décentralisés et intermittents.

Aussi, les frontières traditionnelles entre les acteurs de la chaîne de valeur structurelle deviennent de plus en plus poreuses : producteurs, gestionnaires de réseaux, fournisseurs, consommateurs et nouveaux entrants (équipementiers, gestionnaires de données…) évoluent sur de nouveaux marchés (production locale, technologies intégrées) et multiplient les échanges d'informations (dans la mouvance *open data* qui s'applique donc encore à un nouveau domaine).

Une série d'évolutions précipite la transformation de la chaîne de valeur. Des moyens de production intermittents sont intégrés en masse sur le réseau de distribution (on parle de *Distributed Energy Resources*) et sont souvent gérés par des agents multiples. L'un des effets est la création

284. Partie issue des travaux de recherche d'Alexandre Simon, ancien élève de l'École centrale et collaborateur d'Accuracy.

de consomm'acteurs qui remontent la chaîne de valeur de l'énergie en devenant producteurs et détiennent un surplus d'énergie à vendre. Des échanges directs sont ainsi envisageables grâce au développement de l'autoconsommation collective, qui nécessite d'importantes adaptations du cadre réglementaire, et pourrait notamment remettre en cause le principe du timbre-poste pour les tarifs d'utilisation du réseau. Ces évolutions ont des effets couplés de décentralisation des réseaux et de désintermédiation des échanges. Une option de gestion est la mise en place de micromarchés comme véritable lieu de rencontre de l'offre et de la demande en local, nécessitant des systèmes d'information pour gérer la plate-forme. De nombreuses structures organisationnelles sont possibles pour opérer ces marchés virtuels et la livraison physique subséquente (notamment des consortiums entre des entreprises *tech*, les fournisseurs et le gestionnaire du réseau de distribution).

En soutien de ces initiatives, les opportunités de modernisation du contrôle du réseau passent par une collecte de données individualisées, un contrôle de la demande et une utilisation intelligente du stockage.

La transformation profonde de la chaîne de valeur, la maîtrise des flux, des moyens de financement et des transactions entre ces acteurs deviennent donc des enjeux majeurs. La Blockchain pourrait dès lors devenir un véritable moyen de développement du digital dans l'énergie, à travers des *use cases* bien déterminés.

III.2 Le potentiel de la Blockchain face aux évolutions du marché

À l'heure actuelle, différentes entreprises développent des applications Blockchain pour le secteur de l'énergie. Toutes ces initiatives, sans exception, se trouvent encore au stade de la conception ou sont des projets pilotes. Ainsi, pour la première fois, en 2016, à Brooklyn, une électricité produite de façon décentralisée a été directement vendue entre voisins par le biais d'un système de Blockchain, grâce à une expérimentation simple de cette technologie de certification de l'échange[285]. Depuis, les start-up et les projets internes se sont multipliés, et les investissements se sont accrus.

285. « À New York, la Blockchain partage l'énergie verte », *Les Échos*, 3 novembre 2016, lien : https://www.lesechos.fr/industrie-services/energie-environnement/0211459206747-a-new-york-la-blockchain-partage-lenergie-verte-2040175.php

Des cas d'usages divers apparaissent pour répondre à des problèmes partagés avec d'autres industries (certification de données, gestion des transactions, *crowdfunding*), mais aussi plus spécifiquement pour apporter des solutions nouvelles aux évolutions du marché de l'énergie.

Les utilisations de la Blockchain dans le secteur de l'énergie peuvent se regrouper en plusieurs catégories, et s'effectuent à travers des associations entre start-up *tech* développant une solution disruptive et les entreprises du secteur (fournisseurs, distributeurs) qui accompagnent les tests sur les réseaux, et, de manière plus marginale, un développement en interne en lab pour des applications sur pilotes :

- archivage décentralisé des données de consommation et de production (pour la production électrique, les transactions…) et gestion de la facturation : on notera par exemple les cas de la facturation d'électromobilité par Sodetrel, filiale EDF sur les bornes de recharge Corri-Door[286], ou le consortium RWE & Slock.it[287] ;

- certification de données : comme dans d'autres industries, la Blockchain agit comme service sécurisant, par exemple pour certifier un registre des régimes de propriété et de l'état des installations comme service d'authentification. Un exemple très appliqué concerne la transmission des clés de répartition : des spécialistes de l'analyse de données de clients génèrent, *via* des algorithmes prédictifs, des clés représentant la consommation personnelle d'un consommateur afin de la prédire ;

- financement de projet communautaire par *tokens* contre contreparties futures en énergie garantie (on notera les projets récents d'émission de *tokens*, comme Sun Exchange, WePower, MyBit, ImpactPPA ou encore Lumo)[288] ;

- transactions sur microréseaux : il s'agit de systèmes de transactions entre producteurs permettant les échanges d'énergie *peer-to-peer*.

Ce dernier cas d'usage est l'application la plus disruptive et qui pourrait avoir le plus d'impact sur les modèles d'affaires de l'énergie, car c'est la seule qui bouleverse vraiment la chaîne de valeur, les autres étant des améliorations de fonctionnalités indirectement liées au domaine de l'énergie. À cela s'ajoutent de nombreux gains d'efficacité propres aux bénéfices issus des *Smart Contracts* : automatisation des *process* à travers des stratégies de trading, stockage d'énergie commandables…

286. Lien : https://www.sodetrel.fr/experimentation-olso2rome
287. Stephan Tual, 11 février 2016, lien : https://blog.slock.it/partnering-with-rwe-to-explore-the-future-of-the-energy-sector-1cc89b9993e6
288. Voir leurs *whitepapers* respectifs pour les spécificités de chacun.

Le projet récent le plus retentissant est celui du fournisseur d'électricité Engie. Il illustre parfaitement le potentiel de la tokenisation. Un objet connecté (fabriqué par la start-up française Ledger) est placé sur des éoliennes. La sortie d'électricité de l'éolienne est captée par cet objet et l'information relative à cette quantité d'électricité verte est inscrite dans un registre. À cette information est associée une valeur, matérialisée par un *token* et correspondant à une quantité de kWh certifiée produite de façon écologique. La capacité de démontrer que l'énergie est effectivement issue de dispositifs éoliens représente une grande valeur et permet *in fine* de rendre économiquement non fongible un bien parfaitement fongible physiquement.

En somme, la Blockchain pourrait devenir la clé de voûte des solutions d'avenir dans l'énergie. La gestion désintermédiée de l'énergie peut devenir un moyen fiable de gestion. Elle s'inscrit dans la lignée de la libéralisation du marché de l'électricité et offre un support idéal pour le développement des micromarchés. Plusieurs contraintes technologiques subsistent au niveau structurel du réseau électrique, et les résultats des différentes *proofs-of-work* sont attendus de manière à qualifier la faisabilité technique de chacun des cas d'usage envisagés.

G

DYNAMIQUE FINANCIÈRE : *WORK IN PROGRESS*

Le foisonnement de projets et l'engouement important observés se sont traduits par des mouvements de capitaux massifs à destination d'un espace financier nouveau et parallèle, autour des crypto-actifs. Les ICO *(Initial Coin Offering)* en sont l'exemple le plus populaire. Historiquement, les mouvements de destruction créatrice schumpéteriens ont rarement été des périodes propices à l'appréciation rationnelle des actifs. L'éclatement de la bulle Internet, certes décorrélé du succès de la technologie elle-même, en est une illustration.

Notre objectif est de poser les contours de ce nouveau marché, en définissant et catégorisant les cryptos-actifs d'un point de vue financier. Cette catégorisation nécessite de comprendre le lien entre les différents types de technologies et la finalité des *tokens* leur étant rattachés. Nous établissons également la carte d'identité de ce marché financier, étayée par des chiffres, pour en identifier les caractéristiques, les opportunités et les risques. Enfin, nous adresserons la problématique de la rationalisation des cours par une ébauche d'approche fondamentale. Cet exercice est rendu difficile par la jeunesse de la technologie, l'absence de cadre défini et stable, et les caractéristiques particulières de ces nouveaux actifs. Ces derniers compliquent l'application des théories financières actuelles associées aux classes d'actifs que nous connaissons. Nous en présenterons néanmoins les enjeux de façon simplifiée, en prenant de nombreuses hypothèses contraignantes.

I.
Les contours financiers d'un nouveau monde

Dans les lignes qui précèdent, nous nommons indifféremment *tokens*, crypto-monnaies et crypto-actifs, pour éviter les répétitions de style, dans la mesure où ces termes font référence, dans les grandes lignes, au même objet. Comment faudrait-il les définir en réalité, quelles en sont les différences au sens économique et financier ?

Nous choisirons ici d'utiliser le terme « crypto-actif » pour nommer de manière générale et non exclusive l'ensemble de ces nouveaux objets-même s'ils ne constituent pas un ensemble homogène. Si l'appellation

crypto-monnaie appliquée au bitcoin est déjà controversée sur les plans économique et politique, elle paraît d'autant plus inappropriée dans le cadre des *utility tokens*. Ils correspondent en effet généralement à un droit d'usage bien précis (comme pourrait l'être un jeton de lavomatique), s'éloignant de la définition monétaire.

D'un point de vue général, un crypto-actif peut se définir comme le droit d'entrée et l'unité de compte exclusive d'un écosystème créé (un crypto-actif par projet).

Il est à noter que les analyses qui suivent sont purement économiques et financières et ne tiennent pas compte du cadre comptable (en construction) traitant des *tokens* et des ICO. On relèvera néanmoins la progression intéressante des travaux en la matière, marquée notamment par la publication du règlement ANC (autorités des normes comptables) n°2018-07 du 10 décembre. De façon synthétique, si l'ICO est analysée comme une dette remboursable, le jeton est comptabilisé en « emprunts et dettes assimilées ». Si elle induit une obligation de fournir des services ou des biens non encore livrés, les jetons seront comptabilisés en produits constatés d'avance.

Pour rappel, la multitude d'initiatives Blockchain peut être segmentée en plusieurs catégories de projets aux objectifs propres. Nous excluons de cette partie les projets facilitateurs d'appropriation et les Blockchains privées et permissives, puisque, dans la majorité des cas, ils ne sont pas associés à un crypto-actif[289]. L'analyse se concentre donc sur les crypto-monnayeurs, les *Chain Producers* et les *Chain Users*. Des crypto-actifs sont associés à la totalité de ces projets, dont les caractéristiques sont différentes :

a. Les crypto-monnayeurs ont une ambition quasiment uniquement monétaire (valeur transactionnelle et réserve de valeur) et reposent sur des crypto-monnaies (bitcoin, dash, litecoin…).

b. Les *Chain Producers* sont également des Blockchains auxquelles est associée une crypto-monnaie (Ethereum par exemple). De plus, elles constituent une infrastructure permettant à des utilisateurs *(Chain Users)* de développer une application et son *token* associé. Les transactions de ce dernier sont effectuées et tracées *via* la Blockchain mise en place par le Blockchain *producer*. Les crypto-actifs associés à ces acteurs ont donc un usage hybride, à la fois monétaire et utilitaire (développement d'applications).

---

289. Il existe des exceptions : par exemple la plateforme Binance possède un *token*, tout comme la Blockchain permissive Ripple.

c. Les *Chain Users* correspondent à des projets d'application construits sur des Blockchain existantes (à titre d'exemple, application décentralisée de rencontres basée sur la blockchain Ethereum). Sur le plan financier, il convient de considérer d'une part les *utility tokens,* qui composent la majorité des *tokens*. Les projets associés proposent un service ou un usage qui n'est accessible que par ces derniers. Ils n'ont pas pour objectif initial de constituer une monnaie à proprement parler (réserve de valeur ou moyen d'échange généralisé). Cependant, ils peuvent être un moyen d'aligner les intérêts dans un réseau et/ou la seule grandeur permettant d'accéder au service proposé. Les *security tokens* sont, quant à eux, très proches du fonctionnement des actions et ne changent rien aux mécanismes financiers classiques. L'objectif général de ce type de mécanisme est d'associer un actif à un *token*, et donc d'introduire cet actif dans la blockchain *via* ce même *token*. Cette opération lui permet de bénéficier de tous les avantages de la technologie (traçabilité, sécurité…) : on parle alors de « tokenisation des actifs ».

En synthèse et de façon très simplifiée, on pourrait comparer les crypto-actifs soit à une pièce de monnaie digitale d'un système monétaire parallèle (crypto-monnaies), soit à un jeton d'une forme particulière permettant d'accéder à un droit d'usage, comme actionner une station de lavage automobile *(token)* ou financier (dividendes).

Parmi ces catégories, les crypto-actifs revêtent des réalités multiples, par la combinaison de différents paramètres. Selon Richard Olsen, fondateur de la plate-forme d'échange Lykke, « il n'y aura pas des millions de *tokens,* mais des millions de types de *tokens* différents[290] ».

Dans ce contexte, un canevas de classification et d'analyse unique apparaît essentiel sur les plans réglementaire, stratégique et financier. Nous proposons une grille de lecture, destinée à capter l'ensemble des projets et s'articulant autour des critères d'usage, d'origine, d'offre, d'existence du crypto-actif, de la technologie, des droits associés et du degré de centralisation.

I.1 Usage

Nous distinguons ici les crypto-actifs par l'objectif qu'ils poursuivent :

a. usage monétaire : le *token* est l'usage en lui-même du réseau (réserve de valeur et transactions) ;

290. David Siegel, *The Token Handbook,* 2017.

b. usage hybride entre l'usage monétaire et la plate-forme de développement (généralement associé aux *Chain Producers*) ;

c. usage utilitaire : le *token* est le moyen d'accéder à un service ou un produit bien spécifique *(utility)* ou de rémunérer des incitations ;

d. usage financier : les *tokens* représentent un actif financier. Il s'agit des *security tokens*.

I.2 Origine

Il s'agit de l'identification des acteurs ayant le droit d'émettre le crypto-actif dans l'écosystème :

a. émetteur unique : c'est le cas pour la grande majorité des *tokens utility*. Les *tokens* sont créés une unique fois par l'entreprise, puis mis en vente lors de la phase d'ICO ;

b. groupes d'émetteurs : le cas d'un comité de nœuds émetteurs, dans le cas d'une Blockchain permissive, par exemple ;

c. émetteur décentralisé : n'importe quelle personne du réseau participe au processus de création monétaire. C'est le cas pour le bitcoin, notamment avec le processus de minage, rémunérant le mineur pour son « travail ».

I.3 Offre

L'offre de crypto-actifs correspond au nombre d'unités qui seront créées par le ou les participants agréés. On distingue :

a. offre fixe : le cas dans la majorité des ICO, le *total supply* est inscrit dans le *whitepaper* et auditable dans la Blockchain ;

b. offre en continu mais limitée : c'est le cas du bitcoin. Le nombre total de bitcoins est connu (21 millions) mais la création monétaire est progressive, grâce au mécanisme de minage précédemment expliqué ;

c. offre illimitée : ce serait le cas pour la tokenisation d'un bien de consommation. Par exemple, si une salle de spectacle émettait des

tokens représentant des places de concert, elle pourrait en émettre sans limite.

I.4 Existence

La notion d'existence couvre la durée de vie d'un crypto-actif, et se décompose selon les axes suivants :

a. utilisation unique : le crypto-actif, une fois utilisé, est détruit (« brûlé » dans le jargon de la Blockchain). Cela peut être le cas d'un actif digital représentant un ticket de spectacle par exemple ;

b. multi-usage : il est brûlé après un certain nombre d'utilisations. Nous classons dans cette catégorie les projets qui envisagent de détruire leurs actifs progressivement (par exemple, on détruit 25 % des valeurs utilisées à la première utilisation, puis 10 % à la deuxième…) ;

c. permanent : le crypto-actif, une fois émis, n'a pas vocation à disparaître. C'est le cas des principales crypto-monnaies. Notons cependant que certains experts considèrent que des bitcoins « disparaissent » lorsque son détendeur perd sa clé privée, et donc son accès à ses crypto-monnaies.

I.5 Technologie

Il ne s'agit pas ici de décrire la capacité technique du projet ou de la Blockchain sous-jacente, mais de comprendre sur quelle « couche » technologique le crypto-actif est construit. On distingue :

a. les *DApps tokens* : il s'agit d'un crypto-actif permettant d'accéder à une application, c'est la grande majorité des C*hain Users* et des *security tokens*. Il est implémenté sur le niveau applicatif reposant sur l'infrastructure d'une Blockchain ;

b. les *tokens* de protocole non natifs : ce type de *token* est implémenté dans un protocole économique, lui-même reposant sur une infrastructure Blockchain. Ce *token* est un composant intégral du protocole économique, et lui permet de fonctionner. Nous avons classé ces projets dans la catégorie des *Chain Users* ;

c. les *tokens* natifs : *tokens* implémentés au niveau du protocole même de la Blockchain ; ils sont critiques pour le fonctionnement de la

Blockchain et font partie du mécanisme de consensus. Il s'agit principalement des crypto-monnaies et des *Chain Producers*.

I.6 Droits associés

Les droits associés au *token* diffèrent en fonction des utilisations. Il est nécessaire de distinguer :

a. le vote/la propriété : droits souvent associés au *token* de type *security* ;

b. l'usage : droit lié à l'utilisation d'un service ou du réseau ;

c. le travail : droit de contribuer au réseau (il faut posséder cet actif pour contribuer), qui rémunère alors les participants en crypto-actifs. L'exemple le plus simple est l'utilisation du *proof-of-stake* : ce mécanisme de validation fonctionne sur le principe des comptes séquestres. Un utilisateur voulant participer au réseau place dans un compte séquestre un montant de crypto-monnaie, qu'il ne pourra pas utiliser, mais qui servira à calculer son poids dans l'algorithme de la validation ;

d. l'hybride : lorsque les droits associés au crypto-actif sont multiples. Par exemple, dans le cas du protocole Dash, la détention de Dash par le mineur est requise pour procéder à la validation de la transaction, ce même Dash constituant également l'utilité principale et le droit d'utilisation du réseau. De même, Cardano et Ethereum, une fois sous Casper[291], seront dans cette catégorie.

I.7 Décentralisation du modèle

La Blockchain est souvent associée au concept de décentralisation, fidèle à la philosophie des pionniers et à la promesse d'horizontalité de la technologie. En réalité, les jeux d'acteurs à l'œuvre et la transformation économique en cours sont plus complexes qu'un simple basculement de la centralisation vers la décentralisation. Les degrés de centralisation sont donc divers, y compris dans les initiatives dites de la « nouvelle économie ». On distingue les projets :

291. Casper est le nom de la mise à jour du mécanisme de validation d'Ethereum. Le mécanisme ne nécessitera plus d'avoir de la puissance de calcul *(proof-of-work)*, mais uniquement des ethers *(proof-of-stake)*.

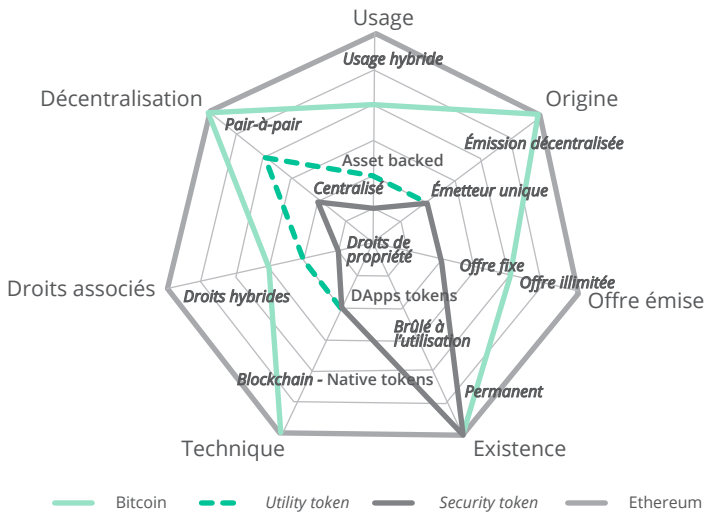
a. centralisés : pour utiliser le service d'une entreprise, le consommateur règle en *tokens*. Ainsi le fonctionnement est similaire à celui d'une entreprise traditionnelle, sauf qu'elle collecte son chiffre d'affaires en *tokens* et non en monnaie traditionnelle ;

b. semi-centralisés : l'utilisation est soumise à quelques nœuds du réseau ; on peut penser notamment aux Blockchains permissives ;

c. décentralisés : une fois le crypto-actif émis, il circule librement de pair-à-pair, sans intervention d'une entité centrale.

En intégrant ces paramètres sur une échelle de 0 à 3, on obtient la représentation ci-dessous, permettant notamment de comparer les crypto-actifs entre eux. Cela permet à l'entrepreneur de faire les choix financiers liés à la *token economy* en ligne et correspondant à ses objectifs stratégiques, et aux investisseurs, de caractériser leurs investissements. Cette classification est également clé pour envisager de rationaliser la valeur et le prix de ces nouveaux actifs. Nous avons représenté les quatre types de crypto-actifs identifiés dans la première partie : le bitcoin, représentant les crypto-monnaies pures, l'Ethereum représentant les *Chain Producers*, un *token utility* standard, et un *token security*.

CANEVAS DE CLASSIFICATION DES CRYPTO-ACTIFS



II.
Les *Initial Coin Offerings* (ICO)

II.1 Le concept

L'*Initial Coin Offering* (ICO) fait couler beaucoup d'encre et alimente la controverse. Ce phénomène est assez récent et ne date pas des débuts de la Blockchain, puisque la première opération a eu lieu en juillet 2013 avec le projet Omni, suivi du fameux Ethereum en 2014 (avec 18 millions de dollars levés à l'époque).

Cette innovation financière et stratégique est une nouvelle étape dans le processus de transformation engagé par la Blockchain et s'inscrit dans la continuité de l'esprit des pionniers. Elle bouleverse le rapport à la propriété et aux usages et accompagne la transformation des comportements.

L'ICO correspond à la mise en marché d'un *token*, sur le marché primaire ; à l'image de l'IPO *(Initial Public Offering)* dans le cadre d'actions cotées. Le droit d'usage est donc vendu en avance de phase, quasiment dès le départ du projet[292], bien avant la mise en place effective du service promis. Les investisseurs/consommateurs (cette double catégorisation est importante) achètent donc une utilité future. Les contributeurs aux projets[293] sont rémunérés par cette grandeur, tout comme les fondateurs qui conservent une partie des valeurs émises.

Pour reprendre un exemple très parlant livré par Pierre Davoust, CEO de SETL France lors de la conférence « Fintech & Blockchain – Exemples et Enjeux », organisée par l'AFGAP[294], une ICO revient à mettre en vente des jetons de laverie dans le but de financer sa création. Pour récolter les fonds nécessaires, je cède par anticipation un droit d'usage futur ; celui d'accéder à mes machines à laver. À ce titre, cela ressemblerait à une forme de chiffre d'affaires anticipé. L'acheteur *early-adopter* peut être intéressé soit par de futures lessives, soit par le gain financier potentiel, si la valeur du jeton croît à mesure que la demande de lessive augmente. En effet, les lessives ne seront accessibles qu'avec ce jeton, produit en

292. En réalité, il y a un temps de latence entre la date de l'ICO et la mise en marché du *token* (pour l'acheteur : délais de vérification d'identité notamment – sur le marché : date de cotation sur une plateforme).
293. Pour rappel, presque aucun contributeur n'est salarié pour la plupart des initiatives.
294. Association française des gestionnaires actif-passifs.

quantité limitée. Si j'ai davantage de jetons de laverie que je ne souhaite faire de lessives, je peux les échanger contre d'autres jetons, de casino par exemple. Créateurs, *early adopters*, (futurs) consommateurs et investisseurs ne se partagent plus une fraction de propriété mais une fraction d'usage. Ce mode de fonctionnement s'applique intuitivement davantage à l'économie de service, mais on pourrait imaginer la création d'un *token* associé à une valeur marchande physique (un mobile, par exemple) inscrite dans une Blockchain.

Notons que l'ICO n'est pas une condition *sine qua non* de la réussite d'un projet Blockchain, en particulier pour les acteurs facilitateurs d'appropriation. Sans ICO, des dizaines de start-up et entreprises opèrent et innovent sur des sujets Blockchain en exploitant la technologie (très puissante en soi) et/ou en occupant des nouveaux segments de marché. C'est le cas notamment de la start-up française Ledger, spécialisée dans la sécurisation des clés sur *hardware*, qui a levé au total 75 millions de dollars [295] par les canaux traditionnels. Son *business model* repose sur un modèle économique standard avec un chiffre d'affaires classiquement composé d'unités vendues à un prix donné, libellé en euros.

II.2 Quels montants en jeu ?

Les montants concernés sont très importants. L'augmentation du nombre d'ICO et des volumes levés a été très rapide, en partant de 64 millions de dollars en avril 2017 répartis sur 10 projets pour atteindre 1,5 milliard de dollars en décembre 2017, montant réparti entre 197 projets finalisés, apogée du phénomène.

Avec la chute brutale des cours observés en début d'année, les montants levés ont drastiquement baissé (1,2 milliard de dollars en janvier) avant de remonter en mars (1,7 milliard levé pour 227 projets). Selon un article de *Techcrunch* reprenant des chiffres de Crunchbase, près de 80 % des financements des initiatives liées à la Blockchain sont réalisés *via* ICO[296]. Au deuxième trimestre 2017, le montant levé par ICO dans le monde dépassait les montants levés par le biais du capital-risque pour les projets Blockchain (797 millions de dollars *vs* 235 millions de dollars selon *Coindesk*, repris par *Techcrunch*).

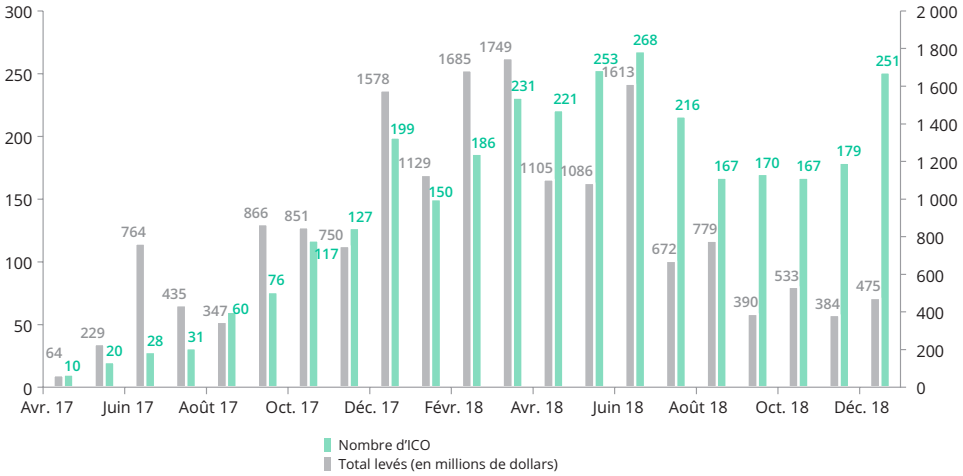
---

295. Delphine Cuny, janvier 2018. Lien : https://www.latribune.fr/entreprises-finance/banques-finance/ledger-etoile-montante-francaise-des-cryptomonnaies-leve-61-millions-d-euros-765164.html

296. Jason Rowley, 4 mars 2018. Lien : https://techcrunch.com/2018/03/04/icos-delivered-at-least-3-5x-more-capital-to-blockchain-startups-than-vc-since-2017/

Depuis la forte baisse du cours observée au 2e semestre de 2018, le montant moyen levé par ICO a fortement baissé et s'élève, sur la période, à 3,3 millions de dollars. Néanmoins, le nombre d'ICO reste relativement stable.

ÉVOLUTION DU NOMBRE D'ICO ET DU VOLUME LEVÉS PAR MOIS



II.3 L'innovation et les opportunités

Le concept d'ICO revêt six caractéristiques majeures le distinguant des modes de financement classiques :

a. La libre circulation des *tokens* permet au marché de valoriser directement l'usage afférent, de manière directe et ce pour toute initiative (à date, ce sont les actions qui sont cotées, pas le service directement ; sans parler des sociétés non cotées).

b. L'ICO démocratise le capital-risque. Tout le monde peut choisir de son plein gré d'investir ou non dans le projet de son choix, en espérant, soit un retour sur investissement en cas de revente du *token*, soit la capacité de consommer le service futur de l'entreprise à moindre coût (le service est en règle générale facturé en *tokens*). À condition d'en maîtriser les risques, l'ICO et l'investissement en *tokens* donnent leur chance à tous, avec une prime pour les *early adopters*. Ce type de fonctionnement doit en théorie sélectionner les meilleurs projets dès le départ et attirer, de façon horizontale, les profils les plus performants ayant tout intérêt à contribuer en l'échange de *tokens*. L'ICO

est également une forme de capital-investissement, capital-risque pair-à-pair, offrant également une formidable opportunité aux professionnels du secteur. Dans un article publié sur *Medium* le 27 mai 2017, Balaji S. Srinivasan (CEO de Earn.com, devenu CTO de la plate-forme Coinbase[297]) estime que les *tokens* vont détruire la barrière entre investisseurs professionnels et acheteurs de *tokens* dans les mêmes proportions qu'Internet a réduit la barrière entre journalistes et bloggers/twitters. Comme il est possible de devenir journaliste amateur grâce au Web, il est désormais possible d'être un investisseur amateur[298]. Néanmoins, l'activité de capital-risque est complexe et sophistiquée. Seuls des profils experts et initiés sont en capacité de maîtriser les risques. Rendre possible l'accès à ce type d'investissement au grand public pose la question de la protection des investisseurs particuliers.

c. Les levées par ICO permettent un élan de créativité sans précédent au service d'une offre et proposition de valeur nouvelles. Elles financent, par la formation *bottom-up* de communautés soudées, des projets qui n'auraient peut-être jamais vu le jour par le biais du financement traditionnel. En effet, pour des raisons évidentes, le crédit bancaire n'est pas toujours adapté au financement des très jeunes pousses. L'ICO est une forme de *crowdfunding* poussé à l'extrême, presque sans aucun filtre. En effet, tel qu'il existe aujourd'hui, le *crowdfunding* repose sur des agrégateurs en ligne type Kickstarter ou Angelist qui réalisent des analyses de projets[299]. Côté ICO, chaque projet réalise sa propre levée *crowdfunding* avec sa propre plate-forme, sans aucun filtre centralisé[300].

d. L'accès à des montants importants en pair-à-pair permet de réduire les barrières à l'entrée sur certains marchés et de réintroduire de la concurrence sur des segments de rente. L'accès à moindres frais à des infrastructures existantes *(open source)* est également un facteur de compétitivité.

e. Le *token* assure l'alignement des intérêts dans le système nouvellement créé. Ce constat n'est pas valable pour tous les projets mais uniquement dans les cas d'application les plus puissants, selon les

---

297. Jon Russell, « Earn.com a été racheté par Coinbase », *Techcrunch*, 16 avril 2018. Lien : https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2018/04/16/coinbase-buys-earn-com-and-makes-ceo-balaji-srinivasan-its-first-cto/amp/

298. Balaji Srinivasan, 27 mai 2017. Lien : https://news.earn.com/thoughts-on-tokens-436109aabcbe

299. Agrawal, Catalini, Goldfarb, *Some simple economics of crowdfunding, innovation policy and the Economy*, University of Chicago Press, 2014. Cité par C. Catalini (MIT, S. Gans (university of Toronto), *Some simple economics of the Blockchain.*

300. *Ibid.*, 23 novembre 2016. Lien : ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf

phénomènes que nous décrivons dans le chapitre dédié à l'économie. Plus le rôle du *token* dans l'écosystème créé est clé, plus sa valeur est mécaniquement importante. Pour rappel, dans le cas du protocole Bitcoin, les mineurs sont incités à mettre à disposition leur puissance de calcul pour valider les transactions en échange de bitcoins.

En constituant une alternative à la fois au financement par dette et par action, l'ICO pourrait d'une certaine manière résoudre plusieurs conflits d'intérêts inhérents aux entreprises capitalistes. En effet, les actionnaires et créanciers sont les bailleurs des entreprises et constituent leur passif comptable, mais poursuivent rationnellement des intérêts différents. En 1981, les économistes Stiglitz et Weiss ont démontré, dans leur modèle de rationnement du crédit bancaire, l'opposition nette des deux groupes quant à la prise de risque, du fait d'une structure de risque/rendements et d'un accès à l'information très distincts[301]. Les actionnaires ont tendance à maximiser le risque et les créanciers à le limiter puisque, contrairement aux porteurs de capital, ils toucheront une rémunération fixe tant que l'entreprise reste en vie. Selon ces économistes, cette situation peut conduire les créanciers à ne pas financer de nouveaux projets, dans un contexte d'asymétrie d'information.

En revanche, elles ont opérationnellement créé des nouvelles problématiques de conflit d'intérêt, notamment entre les fondateurs (pas toujours clairement incités à réussir en l'absence de mécanisme clair) et les clients. Intrinsèquement, on observe également un risque de désalignement d'intérêt entre un investisseur, qui souhaite voir la valeur de son *token* croître, et un consommateur futur souhaitant accéder à un service « au prix ». Trop souvent, les clients B2C non initiés ont apporté la liquidité de sortie aux *airdropers* et investisseurs des débuts…

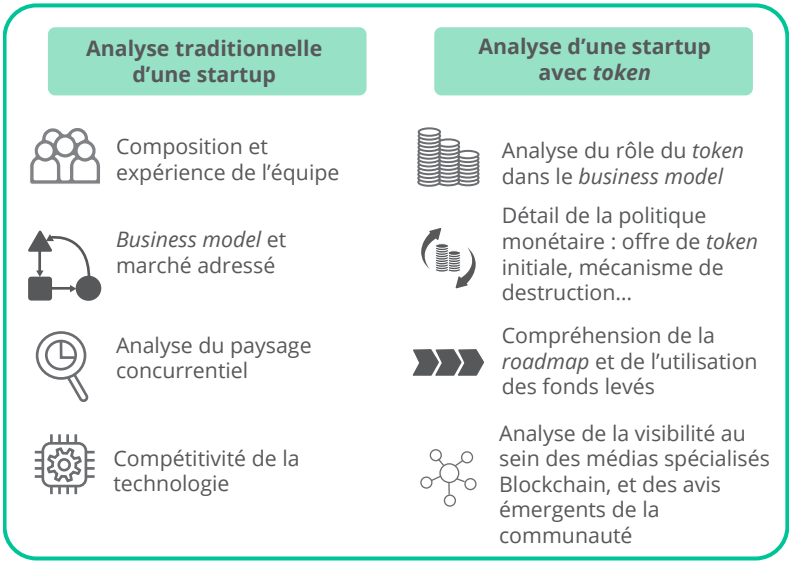
II.4 Les risques : comment distinguer le bon grain de l'ivraie ?

La fin 2017 et le début de 2018 ont été la période de toutes les exubérances : multitude de projets, absence de réglementation, flambée des capitalisations sur des projets trop « *early stage* », surestimation du matériel de certains projets bulle et fraudes à répétition. Les périodes d'innovations intenses, réelles ici, ne sont jamais propices à la rationalité financière. La baisse des cours et la sélection naturelle opérée sont salvatrices et permettent de professionnaliser l'écosystème.

301. J. Stiglitz, A. Weiss, « Credit rationing in markets with imperfect information », *The American Economic Review*, 1981.

Tout investissement dans une ICO, ou acquisition d'un crypto-actif, doit être réfléchi et mesuré en reposant sur des fondamentaux solides et une démarche rationnelle, financière et stratégique. La technologie de la transparence est aujourd'hui souvent bien obscure et peu transparente lorsqu'il s'agit de son financement. De nombreux projets mal intentionnés, *scams* (fraudes) dans le milieu, ont sali la réputation de la Blockchain dans son ensemble et nuisent à son émergence dans un climat de sécurité et de confiance. Face à cela, la communauté d'usagers se ligue contre de tels projets et des initiatives de type agences de notation, collaboratives ou non, voient le jour dans cette logique.

COMMENT IDENTIFIER UNE BONNE ICO ?



Alors sur quels points faut-il s'attarder ? Une ICO et une initiative Blockchain demeurent un projet, dont les points de vérification classiques restent d'usage que ce soit sur le plan stratégique, financier ou humain. Quelles sont la qualité de l'équipe et son expérience ? Quel marché est adressé, quelle est sa taille, quelle part de marché le projet peut-il espérer capter ? Rappelons que, sans demande et sans marché, n'importe quel projet a une valeur zéro (même avec la meilleure des technologies).

Que permet la technologie utilisée et quel avantage comparatif offre-t-elle, quelles sont les barrières à l'entrée ?

En complément de ces attendus, un projet Blockchain ou une ICO méritent d'être analysés sur plusieurs points spécifiques. Le plus important est le rôle du *token* dans l'écosystème créé : à quoi sert-il ? Que changerait le business considéré sans *token* ? Plus le rôle est fort, plus la valeur du projet est potentiellement grande. En ligne avec cette remarque, la politique monétaire, dit autrement la trajectoire d'offre, doit également être analysée puisqu'elle détermine le degré de rareté de l'unité créée. Pour finir, cet écosystème obéit à des règles particulières de communication, dans des communautés soudées auxquelles il faut être capable de s'adresser. À terme, le déplacement pair-à-pair et en temps réel de la propriété des actifs financiers pourrait avoir un impact structurant sur les équilibres économiques et financiers. En effet, cela reviendrait à supprimer le risque de contrepartie dans les échanges financiers, pris en compte dans de nombreux calculs et *pricing*.

Dans les moments difficiles, la communauté porte le projet ; le travail de construction de l'identité communautaire autour de l'initiative est donc un point fondamental.

II.5 Des ICO aux STO ?

Du fait des déconvenues sur les ICO (baisse des cours, fiasco et fraudes pour certains projets) et de l'épée de Damoclès réglementaire toujours existante sur le sujet de la caractérisation juridique des *tokens*, le marché pourrait connaitre l'émergence du phénomène de *Security Token Offering* (STO). Dit de façon très simple, un *security token* est une action digitalisée, échangeable sur une Blockchain. Cette innovation pourrait constituer la première étape de la tokenisation institutionnelle des actifs financiers à grande échelle. L'annonce de l'investissement (20m$) en janvier 2019, par le Nasdaq dans la start-up Symbiont, spécialisée dans les *smart security*, est une bonne illustration de cette tendance de fond.

L'avantage du *security token* est que son arrimage au droit positif est beaucoup plus aisé que dans le cas d'un *utility token* ou d'autres natures de crypto-actifs ; le risque réglementaire associé est donc plus faible. En effet, la nature des droits associés à un « *security* » hors Blockchain est très bien jalonnée par le droit. La loi française a d'ailleurs déjà autorisé la transmission de titres financiers (existants) non cotés via Blockchain. Par ailleurs, les *security token* peuvent avoir pour vertu d'accroître la liquidité de certains actifs, en permettant les échanges pair-à-pair ou en fractionnant des actifs existants. Ils pourraient également, dans cette même logique, avoir un impact majeur sur l'efficacité opérationnelle du système financier en réduisant drastiquement les coûts de traitements

administratifs, techniques et juridiques associés aux échanges de titres financiers.

La vague d'innovation financière associée aux ICO et aux *utility tokens* a connu en emballement trop important et le phénomène était probablement prématuré, pas toujours bien compris dans son essence et très éloigné du droit positif existant. Les *security tokens* présentent de nombreux points forts, apparaissent comme moins risqués et devraient constituer une étape importante de la tokenisation. En revanche, nous considérons qu'ils ne peuvent pas, à eux seuls, incarner l'ensemble du potentiel d'innovation financière ouvert par la Blockchain et la tokenisation (ou *token-economics*). L'intérêt des modèles de *token* est notamment de permettre de créer facilement des nouveaux droits, modulables et échangeables pair-à-pair grâce au mécanisme de monnaie programmable. Ces modèles doivent permettre l'avènement de nouvelles formes de valeur, au service de nouveaux modèles d'affaire.

III.
Un marché financier immature présentant des opportunités risquées

III.1 Un marché financier parallèle coté

Les *tokens* émis lors de l'ICO sont cotés sur un marché financier parallèle, à l'image d'ailleurs de l'ensemble des crypto-actifs acceptés sur les plates-formes. Ce marché est très embryonnaire par ses volumes, sa liquidité, sa régulation, son fonctionnement et ses modes de trading, pas du tout en ligne avec les standards actuels du marché traditionnel.

Il se structure progressivement, de manière similaire au marché financier. Les parallèles existent sur l'ensemble des segments et de la vie du marché ; la classique IPO *(Initial Public Offering)* est remplacée par l'ICO sur le marché primaire, les titres sous-jacents traditionnels (actions, obligations…) par les crypto-actifs, les Bourses (Euronext, Nasdaq) par les *exchanges* sur le marché secondaire. Plusieurs acteurs saisissent cette opportunité sur ces segments porteurs, plus ou moins matures.

PARALLÈLE ENTRE LE MARCHÉ FINANCIER TRADITIONNEL ET CELUI DES CRYPTO-ACTIFS[302]

	Introduction (si applicable)	*Actifs sous-jacents*	*Cotation*	*Stockage*	*Informations de marché*	Asset Management
Marché financier traditionnel	• IPO • Émission d'obligations	• Actions • Obligations	• Euronext • NASDAQ • Hong Kong Stock Exchange	• Banques	• Bloomberg / Sites Internet publics	• *Asset Managers* • *Hedge Funds*
Marché des crypto-actifs	• ICO	• Crypto-actifs	• Plates-formes décentralisées	• *Cold Storage* • Plates-formes	• Sites Internet publics	• *Crypto Hedge Funds*

III.2 Les caractéristiques du marché

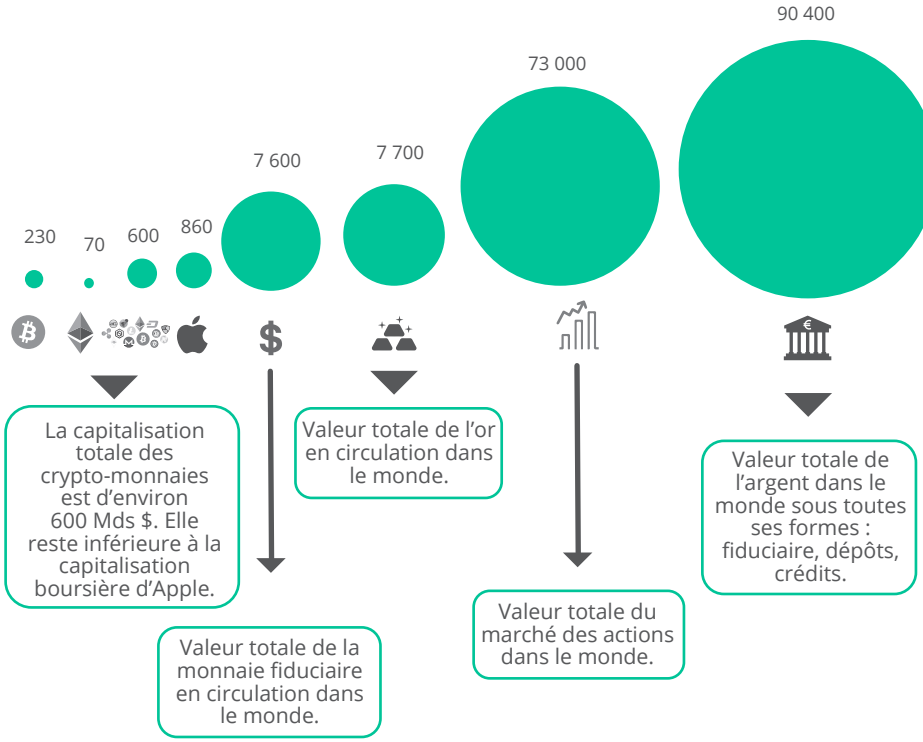
III.2.a Une taille importante à relativiser

Au 31 décembre 2018, la capitalisation totale des crypto-actifs s'élevait à 127 milliards de dollars environ. Elle s'établissait à près de 800 milliards de dollars au tout début 2018, soit le point le plus haut jamais enregistré.

En stock, ce montant est vertigineux dans l'absolu mais peut être relativisé, comparé aux métriques des autres actifs. La totalité de la capitalisation des crypto-actifs est par exemple plus de cinq fois plus faible que la seule capitalisation boursière d'Apple au 31 décembre 2018. Elle ne représente que moins de 2 % de la monnaie fiduciaire en circulation et du stock d'or mondial, et moins de 0,2 % de la valeur totale des actions mondiales.

302. Schéma réalisé par Accuracy pour le compte de la start-up Peculium et également présente dans le cadre de notre contribution au dossier de *Revue Banque* sur la technologie appliquée à la banque d'investissement, supplément au n° 821, juin 2018, p. 45.

COMPARAISON DE LA CAPITALISATION DES CRYPTO-ACTIFS COMPARÉE AUX AUTRES ACTIFS ET AGRÉGATS AU 31 DÉCEMBRE 2018 EN MILLIARDS DE DOLLARS[303]



III.2.b Une croissance fulgurante des volumes, une progression du nombre d'utilisateurs plus linéaire

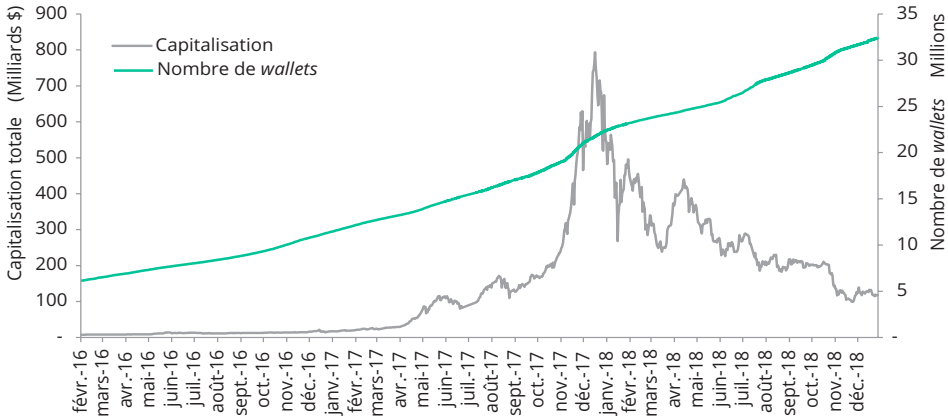
Cette masse de valeur a néanmoins été accumulée avec une rapidité fulgurante. En quelques mois, de début 2016 à tout début janvier 2018, le marché est passé de moins de 8 milliards de dollars à près de 800 milliards (le 6 janvier), soit un rapport de 1 à 100 en deux ans.

Fait intéressant, le nombre de *wallets* (portefeuilles de détention de crypto-actifs) poursuit une évolution quasi linéaire et plutôt « saine » ; sur la même période, il a été multiplié par 2,5, passant de 6,5 millions à un peu plus de 31 millions fin décembre 2018. Cette progression mesurée et soutenue semble décorrélée de l'évolution du cours (x 100 sur la

303. Liens : https://coinmarketcap.com et money.visualcapitalist.com/

même période). L'intérêt pour la technologie et les crypto-actifs apparaît donc suivre une évolution positive et régulière.

ÉVOLUTION DU NOMBRE DE *WALLETS* CRYPTO-ACTIFS PAR RAPPORT À L'ÉVOLUTION DE LA CAPITALISATION TOTALE[304]



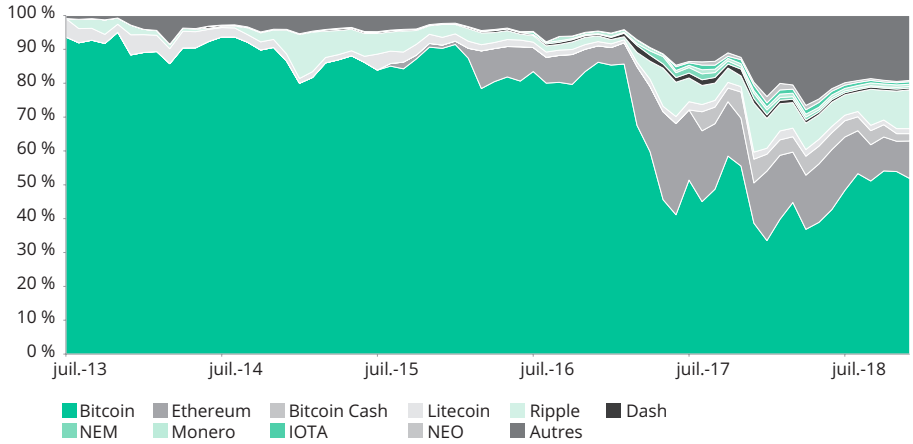
III.2.c Une diversification à l'œuvre sur un marché encore dominé par quelques acteurs

L'écosystème Blockchain apparaît de plus en plus diversifié, marqué par un foisonnement de projets. Le Bitcoin, créé en 2008, est désormais loin d'être le seul crypto-actif, bien qu'il constitue toujours la première capitalisation mondiale. D'autres crypto-monnayeurs ont vu le jour avec des modèles assez proches (Dash, Litecoin), puis d'autres natures de projets (comme Ethereum) ont ouvert la voie aux *Smart Contracts* et applications.

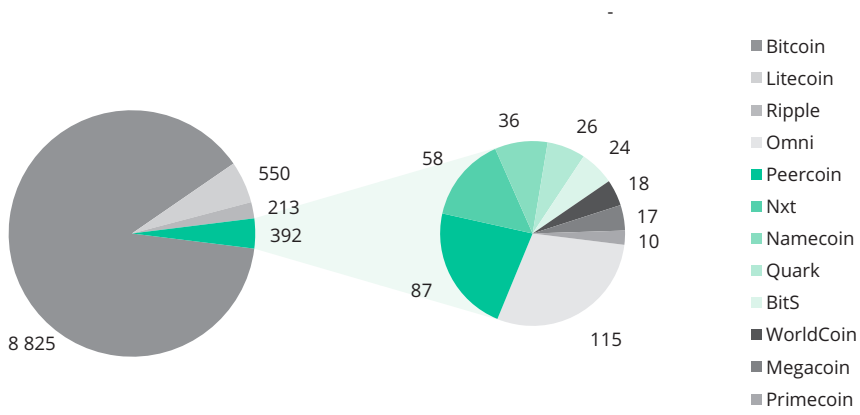
Cette diversification s'est traduite dans les chiffres par une diminution de la part relative du bitcoin dans la capitalisation totale des crypto-actifs, au profit d'ether mais aussi de bitcoin cash, litecoin ou encore ripple. Résultat : fin 2017, le bitcoin ne représentait que 40 % de la capitalisation totale fin 2017, contre 94 % en juillet 2013.

304. Nombre de *wallets* : https://api.blockchain.info/charts/my-wallet-n-users?timespan=all&format=json. Capitalisation : https://coinmarketcap.com/charts/

ÉVOLUTION RELATIVE DE LA PART DE MARCHÉ (CAPITALISATION TOTALE EN DOLLARS) DES CRYPTO-ACTIFS



ÉVOLUTION DE LA RÉPARTITION DE LA CAPITALISATION TOTALE ENTRE 2013 ET 2017

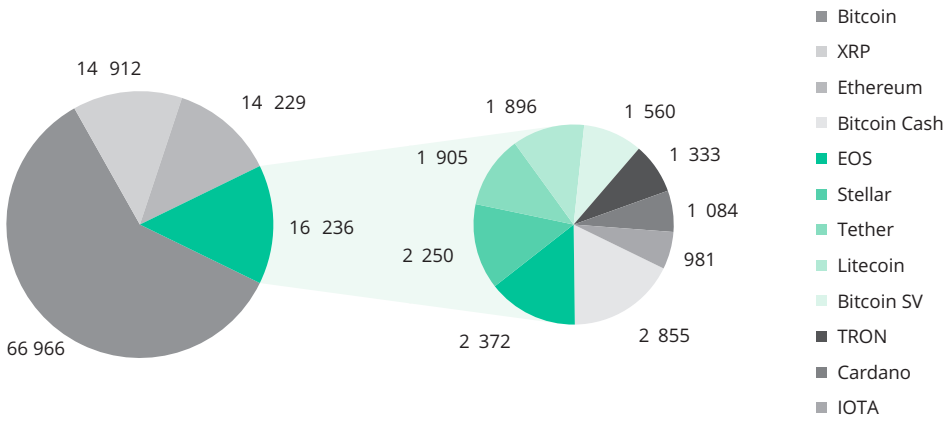


En dehors du bitcoin, la viabilité de long terme des projets n'est pas une évidence et le taux de survie sur ce marché semble relativement limité. Il est intéressant notamment de regarder si les projets qui existaient en 2013 au côté du Bitcoin sont toujours présents en 2015 par exemple. Parmi les douze principales valeurs en 2013, cinq ont disparu en 2015,

dont notamment Omni, la première ICO. D'autres projets ont émergé dans l'intervalle, comme Stellar. Entre 2015 et 2018, se sont également imposés des initiatives d'ampleur reléguant au second plan les champions de 2015 (Eos, Cardano, NEM…).

Globalement, le marché reste dominé par les *coins* et projets d'ampleur, bien implantés ; le bitcoin représentait encore fin 2018 près de 55 % du total, suivi par ripple avec un peu plus de 12 %, ether autour de 12 % et bitcoin Cash 23 %. Fin décembre 2018, ces quatre principales valeurs représentaient encore près de 80 % de la capitalisation. Le reste du marché est très atomisé, réparti sur des centaines de projets.

RÉPARTITION DE LA CAPITALISATION BOURSIÈRE ENTRE CRYPTO-ACTIFS À FIN DÉCEMBRE 2018[305]



III.2.d Un marché immature et risqué

Le marché financier des crypto-actifs est souvent décrié pour les risques qu'il comporte, sa volatilité, son manque de liquidité, sa concentration extrême et son manque de transparence. Qu'en est-il réellement ?

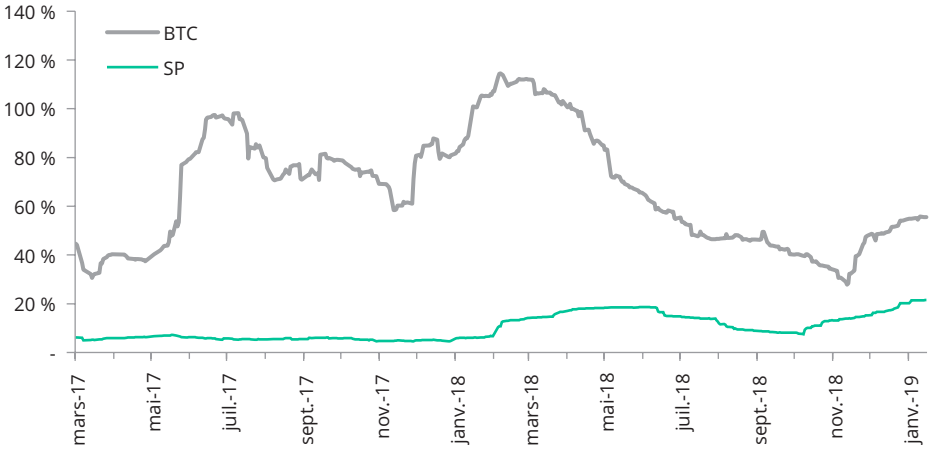
Fondamentalement, les analyses chiffrées réalisées confirment la totalité de ces affirmations, qui s'expliquent à la fois par la jeunesse du marché mais aussi par un manque de régulation bien calibrée.

305. Lien : https://coinmarketcap.com/historical/

Le marché subit une très forte volatilité, due notamment à une liquidité réduite

La comparaison de la volatilité annualisée (calculée grâce à l'estimateur de Garman-Klass sur 30 valeurs journalières) de mars à décembre 2018 entre le bitcoin et le S & P 500 suffit à étayer ce constat. La différence de volatilité moyenne est majeure puisqu'elle s'établit sur cette période à 67 % pour le bitcoin, contre 10 % pour le S & P 500. Notons toutefois une baisse de la volatilité du Bitcoin au cours du second semestre 2018 comme le montre le graphique ci-dessous :

ANALYSE COMPARATIVE DE LA VOLATILITÉ ANNUALISÉE (CALCULÉE SUR DES DONNÉES JOURNALIÈRES) ENTRE LE BITCOIN ET LE S & P 500 DE MARS 2017 À JANVIER 2019

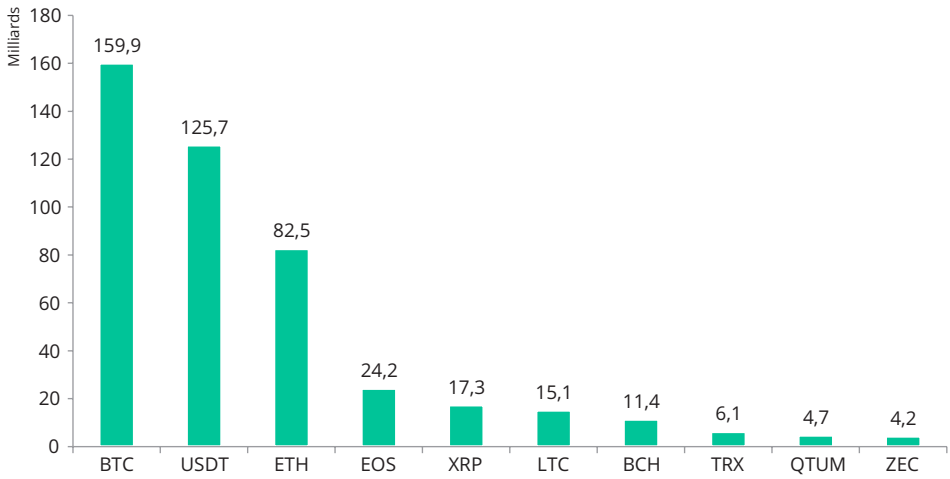


Le marché reste trop peu liquide

La liquidité du marché des crypto-actifs est encore trop limitée pour permettre le bon déroulé des transactions et limiter la volatilité.

Les discussions de place semblent s'accorder sur le fait que seulement une petite dizaine de crypto-actifs bénéficient de la liquidité suffisante pour permettre la bonne tenue du marché.

VOLUMES ÉCHANGÉS SUR LES 30 DERNIERS JOURS POUR LES PRINCIPAUX CRYPTO-ACTIFS EN JANVIER 2019[306]



Attention, certains observateurs considèrent que le montant total du volume échangé est surestimé, par l'existence du phénomène dit des *fake volumes* (faux volumes[307]). En effet, certaines plates-formes d'échange simuleraient une partie du volume échangé afin de prétendre à une liquidité en réalité inexistante.

Certains crypto-actifs, à leur lancement, n'ont parfois quasiment aucune liquidité pendant des mois, avant d'être cotés sur des plates-formes suffisamment importantes et de générer un engouement significatif. Ce point n'est cependant pas nécessairement anormal ou inquiétant dans la mesure où l'ICO peut être vue comme une forme de financement d'amorçage par le marché. Dans le cas du capital-risque, les titres achetés sont très peu liquides dans un premier temps.

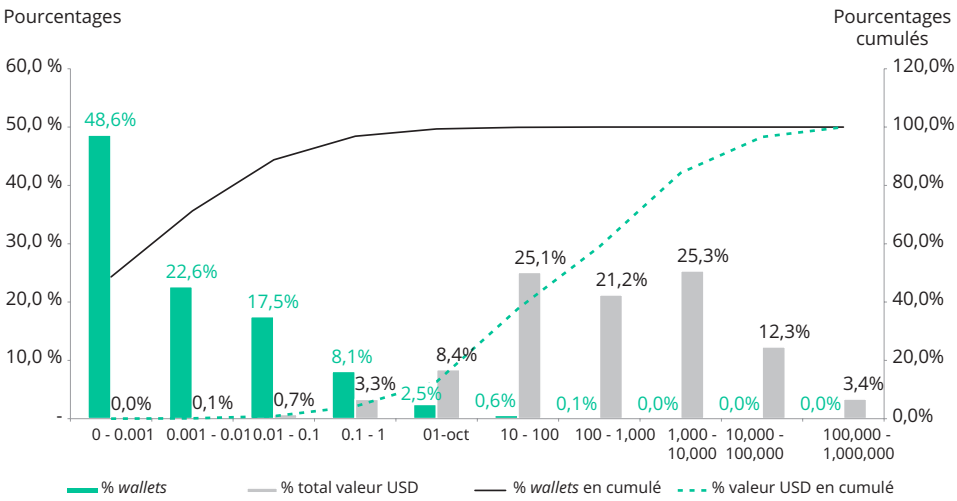
Le marché est très concentré

Les principaux actifs, le bitcoin, l'ether et le ripple, représentent à eux trois environ les trois quarts de la capitalisation totale[308]. La répartition du nombre de bitcoins par *wallet* est très déséquilibrée et extrêmement concentrée : 95 % de la valeur repose sur 3 % des *wallets*.

306. Lien : https://coinmarketcap.com/currencies/volume/monthly/
307. Lien : https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e
308. Lien : https://coinmarketcap.com/

Près de 50 % des *wallets* possèdent moins de 0,001 bitcoin. À l'inverse, les deux principaux portefeuilles représentent à eux seuls plus de 337 000 bitcoins soit plus de 2 % du total (2,5 milliards de dollars). Autre chiffre impressionnant : les 114 premiers détenteurs concentrent plus de 20 % des bitcoins. Parmi ceux-là, on retrouve par exemple régulièrement, dans la presse, les profils des « rois du bitcoin », dont font partie les frères Winklevoss, premiers milliardaires en bitcoins[309].

ANALYSE DE LA CONCENTRATION DU BITCOIN AU 31 DÉCEMBRE 2018



Pour l'ether, le constat est similaire, les 25 premières adresses cumulent environ 20 % de la capitalisation totale à la même date[310].

Cette concentration extrême se traduit mécaniquement par une liquidité limitée, y compris sur les principales capitalisations. De plus, elle induit un risque majeur de manipulation de cours en l'absence de régulation appropriée.

En synthèse, le marché reste imparfait, trop peu régulé pour permettre une information symétrique.

a. Le marché des crypto-actifs n'est pas à l'équilibre car pas totalement arbitré. La faiblesse de la liquidité et l'importance des frais de transaction appliqués par les plates-formes d'échange ne permettent pas

309. Lien : https://www.lesechos.fr/04/12/2017/lesechos.fr/030978928166_le-fabuleux-destin-des-freres-winklevoss--milliardaires-du-bitcoin.htm
310. Lien : https://etherscan.io/accounts. Ce montant comprend les *cold wallets* des *exchanges* qui réalisent du volume *offchain*.

une stratégie d'arbitrage pour afficher un prix unique quel que soit son lieu de cotation. Dans l'économie traditionnelle, une action Total cote le même cours à la Bourse de Tokyo et à celle de Paris. Ce n'est pas le cas pour les crypto-actifs pour lesquels les écarts à un instant *t* entre deux plates-formes sont importants.

b. Le marché des crypto-actifs n'est pas totalement liquide.

c. Le marché n'est pas atomisé et ne respecte pas une condition majeure de la concurrence pure et parfaite, du fait de sa très grande concentration. Plusieurs acteurs ne sont pas preneurs de prix mais ont la capacité d'influencer massivement le marché, du fait des volumes très importants déployés à l'achat ou à la vente. Dans le milieu de la Blockchain, on les appelle les *whales* (« baleines »).

d. Trop peu régulé et concentré, le marché n'est pas transparent et regorge d'asymétrie d'information. La réglementation est trop peu avancée en matière de lutte contre le blanchiment, de délit d'initié, de prévention de la fraude, de manipulation de cours et, plus largement, d'abus de marché. Ce marché regorge d'opportunités et mérite mieux que cela. La communauté doit œuvrer, au côté des pouvoirs publics, pour définir des règles adéquates permettant de révéler le potentiel de cette technologie. Les *dumps and pumps* organisés sur le marché sont de la spoliation pure et simple que nous ne pouvons collectivement pas tolérer.

e. Le marché est très loin d'obéir à des comportements d'agents rationnels. Si nous sommes convaincus des fondamentaux de la Blockchain, du Bitcoin et (de façon plus prudente) des crypto-actifs, il est difficile de nier le risque de bulle financière. L'allure de la courbe observée n'est pas sans rappeler celle de la bulle Internet (s'était ensuivi le krach du .com). L'achat de crypto-actifs doit vraisemblablement être, en partie du moins, motivé par l'appât du gain, un effet *hype* et *FOMO (fear of missing out)*. Charles P. Kindleberger écrit notamment : *« New opportunities for profit are seized, and overdone »* (« les opportunités de profit sont saisies et surexploitées »), générant la création de bulle financière. Des phénomènes rappellent également les caractéristiques d'une pyramide de Ponzi.

IV.
Tentative de rationalisation des cours et de la valeur

Dans ce contexte, notre objectif est d'apporter un point de vue rationnel sur les crypto-actifs, de les classifier, de les comparer à des actifs traditionnels et de questionner les méthodes d'évaluation – certes imparfaites à ce stade – qui pourraient permettre de rationaliser les cours existants.

Dans son article[311] et son ouvrage[312], Chris Burniske reprend les travaux de Robert J. Greer, auteur de *What is an asset class anyway?* (« Qu'est-ce qu'une classe d'actifs? »), et distingue trois catégories : les actifs financiers (basés sur l'actualisation des *cash-flows* futurs comme les actions, les obligations et l'immobilier), les actifs consommables et transformables (commodités, métaux précieux), et les *stores of value*, non consommables et ne générant pas de *cash-flow* (métaux précieux, monnaies, œuvres d'art). Dans la même logique, Damodoran distingue :

a. Les monnaies : elles constituent des moyens d'échange, de stockage et font office d'unité de compte. Elles sont utilisées pour échanger des actifs, les *cash-flows* reçus de ceux-ci, et peuvent constituer des réserves de valeur pour les investisseurs décidant de ne pas investir. Ne délivrant pas de *cash-flow*, elles ne peuvent pas être évaluées, mais peuvent être valorisées les unes par rapport aux autres. Si, à court terme, des mouvements de marché et les politiques monétaires peuvent influer sur ces prix, à long terme la valeur des monnaies avec l'acceptation la plus large et le plus grand pouvoir d'achat doit croître par rapport aux autres.

b. Les actifs financiers (actions, obligations, immobiliers, options) : ils donnent droit à des flux financiers futurs et peuvent être évalués sur cette base qu'ils soient établis contractuellement ou contingents à des paramètres (options). Les actifs financiers peuvent être classiquement évalués par l'actualisation de la séquence de *cash-flows* futurs. Ils peuvent également être évalués les uns par rapport aux autres en utilisant des métriques communes (par exemple, pour les actions : *Price Earning Ratio,*

311. Chris Burniske, Jack Tatar, « Cryptoassets: The Innovation Investor's Guide to Bitcoin and Beyond ».
312. *Ibid*.

Enterprise Value/EBITDA, Price to Book…). Une entreprise peut être considérée comme un actif et donc être évaluée en actualisant les *cash-flows* futurs. La valeur des actions est déduite par soustraction de la dette à la valeur de l'entreprise.

c. Les commodités (blé, métaux précieux comme l'or…) : elles constituent essentiellement des ressources industrielles et dérivent leur valeur d'un besoin fondamental (énergie, nourriture…). Elles peuvent théoriquement être évaluées par la rencontre de l'offre et de la demande modélisées. Selon Damodoran, elles sont globalement davantage valorisées, à travers les cycles, comparées à leur propre prix historique ou à ceux des autres commodités.

d. Les collectibles : marché de l'art et de l'émotion. La valeur est guidée par l'esthétique et l'émotion, le degré de désirabilité et la rareté. Les œuvres sont donc généralement valorisées et ne délivrent pas de flux de trésorerie.

IV.1 Les crypto-actifs peuvent-ils s'inscrire dans ces catégories ?

IV.1.a À première vue, leur catégorisation n'est pas une évidence

Aux yeux de Melamed (*chairman* émérite du Chicago Stock Exchange), le bitcoin va devenir une classe d'actifs à part entière, régulée comme telle selon des règles propres, à l'image de l'or ou des actions[313].

Dans un article du 24 octobre 2017 paru sur son blog, Aswath Damodoran[314] explique au contraire que le bitcoin ne constitue pas une nouvelle classe d'actifs de nature à remettre en cause les fondamentaux du risque, de l'investissement et de la gestion. Le professeur de finance classifie le bitcoin comme une monnaie – certes imparfaite – et non comme un actif, concluant qu'il ne peut par conséquent pas être « évalué mais seulement "pricé" ». Dans ce contexte, investir dans

313. Tomo Uetake, Hideyuki Sano, interview: « Bitcoin, a new asset class, not a crypto-currency », *CME's Melamed*, 7 novembre 2017. Lien : https://www.reuters.com/article/cme-group-bitcoin/interview-bitcoin-a-new-asset-class-not-a-crypto-currency-cmes-melamed-idINKBN1D7159

314. Aswath Damodoran, « The Bitcoin Boom : Asset, Currency, Commodity and Collectible », 24 octobre 2017. Lien : aswathdamodaran.blogspot.fr/2017/10/the-bitcoin-boom-asset-currency.html

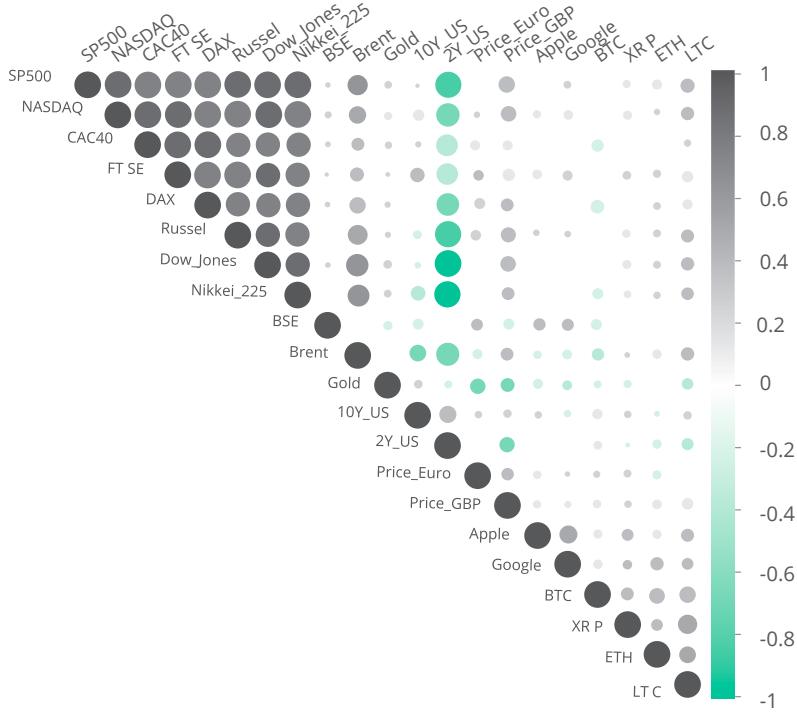
le bitcoin n'aurait pas de sens et tout agent rationnel se limiterait à réaliser des opérations de trading.

Si le bitcoin peut théoriquement répondre à la définition économique d'une monnaie (imparfaite), il n'a pas cours légal donc n'est pas réglementairement considéré comme une monnaie. Il est par ailleurs traité comme une commodité par le juge fédéral américain. Ce dernier permet en effet sa régulation par la *US commodity Futures Trading Commission* (CTFC) listant des contrats futurs[315].

Sur le plan statistique, les crypto-actifs sont-ils corrélés (séparément ou de façon uniforme) à des actifs traditionnels ? Nous avons recherché des corrélations entre les principaux crypto-actifs (bitcoin : BTC, litecoin : LTC, ripple : XRP et ether : ETH) et les actifs traditionnels (indices boursiers comme l'Eurostoxx ou le CAC 40, Brent, or, euro, dollar, niveau des taux…). Les résultats démontrent l'absence de corrélation entre les crypto-actifs et les variables « classiques » : le bitcoin semble par exemple évoluer sans aucun lien avec l'or, le pétrole, le dollar ou l'Eurostoxx. En revanche, on note une très forte corrélation entre les crypto-actifs, même de nature différente : le bitcoin, le litecoin, l'ether et le ripple sont très corrélés entre eux. Cette homogénéité statistique entre ces valeurs et l'absence de corrélation entre ce groupe et les autres actifs amènent à deux conclusions. La première est qu'ils pourraient à ce titre être considérés comme une classe d'actifs à part. La seconde est que cette absence de corrélation est un argument de poids dans la constitution de la dimension réserve de valeur de ces nouvelles grandeurs, car son absence de corrélation avec les autres variables immuniserait un investissement des variations de l'économie mondiale. En revanche, si le bitcoin ou l'ether venaient à être plus largement utilisés, ne pourrait-on pas penser que la corrélation de leurs cours aux paramètres économiques mondiaux aurait tendance à augmenter ? On peut également noter des corrélations différentes entre les crypto-actifs eux-mêmes ; le bitcoin (BTC) semble notamment davantage corréler avec le litecoin (LTC) qu'avec l'ether (ETH) ou le ripple (XRP).

315. David Mayer, « Cryptocurrencies like bitcoin are commodities, Federal Judge says. Here's why that matters », 7 mars 2018. Lien : fortune.com/2018/03/07/bitcoin-cftc-commodities-coin-drop-markets/

SYNTHÈSE DE L'ANALYSE DE CORRÉLATION RÉALISÉE[316]



IV.1.b Tentative de classification

Nous reprenons la distinction opérée préalablement entre crypto-monnaies et *tokens*.

Les crypto-monnaies

Prenons le cas du bitcoin.

a. Il présente des attributs monétaires : réserve de valeur, transactions et unité de compte. Comme nous l'avons vu, les crypto-monnaies

316. Matrice des corrélations des rendements journaliers. Les cases colorées représentent une forte corrélation (positive, c'est-à-dire évoluant dans le même sens, ou négative – évoluant dans le sens contraire). Une case non colorée représente des actifs non corrélés entre eux. À titre d'exemple, le bitcoin n'est corrélé à aucun actif du monde financier traditionnel. Les données sources utilisées pour cette analyse correspondent à une fenêtre temporelle comprise entre janvier 2014 et décembre 2017.

pourraient prétendre, sous certaines hypothèses de l'angle de l'école autrichienne, à l'appellation de monnaie imparfaite. La totalité ou presque des crypto-actifs possède une parité en bitcoin ou en ether, et la performance de nombreux *tokens* est toujours présentée au bitcoin et à l'ether. Ces derniers constitueraient en cela quasiment une forme de métrique de référence. D'un point de vue plus subjectif, il est intéressant de noter la perception en termes d'unité de compte qu'ont construit les membres de cette communauté Blockchain. Pour eux, un bitcoin représente une grandeur en soi, dont la parité en dollars semble parfois être reléguée au second rang d'importance. À titre d'exemple, nombre de projets que nous rencontrons rémunèrent leurs *stakeholders* avec un montant fixe de bitcoins, indépendamment de l'évolution du cours.

b. Il possède des caractéristiques des commodités, du fait de sa rareté programmée par le code et ne pouvant être remise en cause.

c. Cette rareté est très singulière puisque, comme le démontre Chris Burniske, la trajectoire d'offre du bitcoin, logarithmique et prédéterminée par le code, s'éloigne drastiquement de l'offre de monnaie traditionnelle (l'évolution de la création monétaire en dollars est très erratique et ne répond pratiquement plus au critère de rareté).

d. Il peut afficher également, dans une certaine mesure, des points communs avec les collectibles. Mais les crypto-actifs, et plus particulièrement le bitcoin, comportent un aspect subjectif dépassant l'effet de mode, du fait d'une forte dimension philosophique et politique. Ce phénomène fait du bitcoin une forme de totem subjectif ; idée particulièrement présente dans la communauté Bitcoin et des *Bitcoin gurus* (individus ne jurant que par le bitcoin).

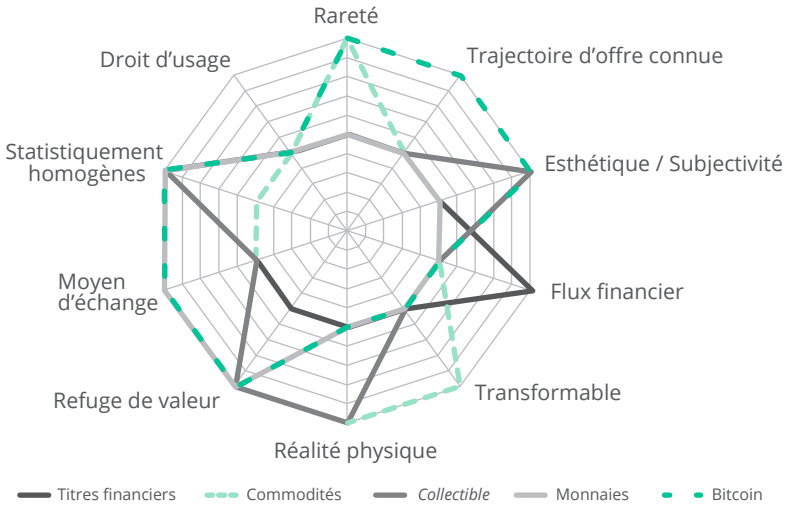
In fine, le bitcoin semble financièrement plus proche d'une monnaie, mais avec des caractéristiques singulières rencontrées dans d'autres classes d'actifs, le distinguant des monnaies traditionnelles. Ce constat peut être généralisé à l'ensemble des crypto-monnaies pures mais pas aux crypto-monnaies des *Chain Producers* (ex : ether) qui combinent une fonction monétaire et un usage.

Les *tokens* des *Chain Users*

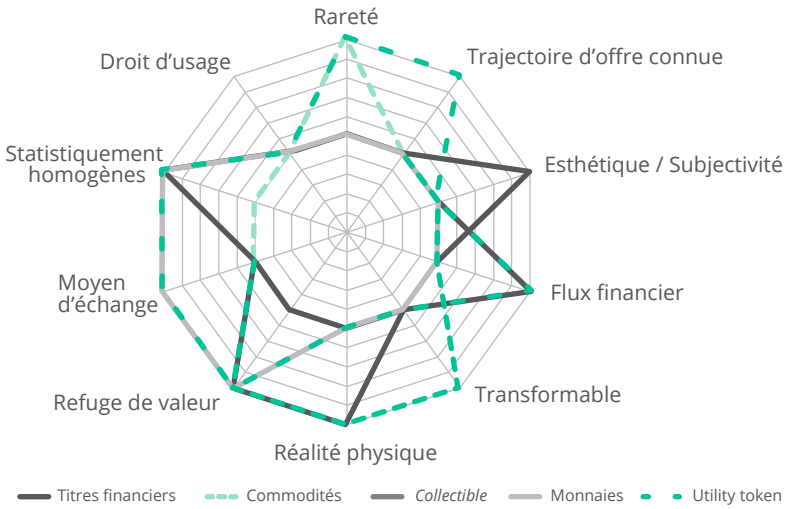
Nous ne traitons pas des *security tokens* qui s'apparentent financièrement presque parfaitement à des actions. Les *utility tokens* présentent en effet un profil très proche d'un actif financier, à l'exception de la notion de la trajectoire d'offre connue à l'avance et programmée qui leur est propre.

La caractéristique du flux financier est également différente puisque dans le cas d'un *utility token*, il s'agit de la monétisation future d'un usage donné.

ÉTAT DES LIEUX DES CLASSES D'ACTIFS ET DES CARACTÉRISTIQUES DISCRIMINANTES



ÉTAT DES LIEUX DES CLASSES D'ACTIFS ET DES CARACTÉRISTIQUES DISCRIMINANTES



IV.2 Quelles implications sur les méthodologies possibles de rationalisation de cours ?

En synthèse, nous distinguons :

a. Les crypto-monnaies pures que nous nous assimilons à une monnaie. Une monnaie ne s'évalue pas mais son cours se valorise par rapport à une autre. Pour cela, nous proposons, en ligne avec d'autres auteurs comme Chris Burniske, d'appliquer la théorie quantitative de la monnaie.

b. Les crypto-monnaies des *Chain Producers* : le caractère hybride de ces monnaies ne nous permet pas à ce stade de proposer un cadre satisfaisant de valorisation.

c. Les *security tokens* peuvent être classiquement évalués en utilisant la méthode des flux financiers actualisés. Pour rappel, un actif vaut la somme des flux financiers futurs actualisés. Cette méthode est classique et ne sera donc pas développée ici[317].

d. Les *utility tokens,* que nous traitons comme des actifs financiers mais avec certaines particularités. En effet, le flux financier futur correspond à la monétisation en monnaie traditionnelle de la valeur utilitaire future. Cette dernière est obtenue de la manière suivante :

- la demande de services future est projetée (volumes). Cette demande est traduite en monnaie traditionnelle et correspond donc à une forme de chiffre d'affaires ou de GDP du réseau ;
- celle-ci est rapportée à l'offre disponible sur le réseau (nombre de *tokens* en circulation *modulo* la vitesse de circulation des *tokens*) ;
- on en déduit une projection de la valeur utilitaire unitaire, exprimée en monnaie traditionnelle à échéance.
- on actualise cette valeur à date.

317. Pierre Vernimmen, Pascal Quiry, Yann le Fur, *Finance d'entreprise*, Dalloz, 2018.

IV.2.a Le cas des crypto-monnaies

Approche simplifiée de la valeur intrinsèque du bitcoin

Notre conviction est que la Blockchain ne remet pas en cause les fondements de l'économie. Quelle que soit la prouesse industrielle ou technologique sous-jacente, si un produit ou un service ne sert à rien ou n'est pas compétitif, il ne connaîtra aucune demande, et vaudra zéro.

Notre approche, dans le cas du bitcoin, consiste à identifier les cas d'usage, déterminer dans quelle mesure il est compétitif sur ceux-ci, pour en déduire un succès, comparé à des concurrents ou métriques similaires. Rappelons que nous nous plaçons dans le cas théorique de la valorisation d'une monnaie et qu'il s'agit par conséquent de valoriser de manière relative un cours par rapport à un autre (en l'occurrence, le cours du bitcoin par rapport au dollar).

Pour rappel, le bitcoin présente deux applications clés :

- l'aspect réserve de valeur : le bitcoin serait le nouvel or digital, moyen sécurisé de conserver ses richesses (base de données en réseau inviolable permettant une traçabilité sans faille) ;
- l'aspect transactionnel : le bitcoin pourrait être demain, dans une certaine mesure, une nouvelle unité de compte de référence, au même titre que l'euro ou le dollar.

Approche par la réserve de valeur

Comme nous l'expliquons dans les chapitres économique et stratégique, le bitcoin est encore peu utilisé sur le plan transactionnel (bien qu'il soit difficile d'estimer avec précision le volume des transactions motivé par un besoin économique). Les frais de transaction restent en moyenne élevés (*a fortiori* en période de forte demande) et le temps de validation trop long, notamment pour des transferts quotidiens à faible niveau de criticité. Nous considérons donc dans un premier temps, et pour simplifier, que l'aspect transactionnel est négligeable par rapport à l'aspect réserve de valeur[318].

Rationalisons la valeur du bitcoin à son usage de réserve de valeur en le comparant à l'or ; il représenterait un or 2.0 qui suit le processus généralisé de dématérialisation et de digitalisation. La valeur totale de

318. Voir l'analyse économique sur les frais de transaction, et stratégique sur les différences d'usage entre crypto-monnaies.

l'ensemble des bitcoins en circulation (autrement dit la capitalisation de marché) serait alors au maximum égale à la valeur placée dans l'or. La valeur du bitcoin suivrait alors l'équation suivante :

$$\text{Réserve de valeur}_{BTC} = \frac{\text{Part de marché x Valorisation de l'or}}{\text{Nombre de bitcoins en circulation}}$$

Le montant total d'or à date représenterait 7 700 milliards de dollars[319]. En considérant le nombre total de bitcoins en circulation (décembre 2018), soit environ 17 millions, on obtiendrait, pour différentes parts de marché, les chiffres suivants :

PART DE MARCHÉ PAR RAPPORT À L'OR	TAILLE DE MARCHÉ INDUITE (M$)	NOMBRE DE BITCOIN EN CIRCULATION (M#)	VALEUR UNITAIRE DU BITCOIN ($)
1 %	77 000	17	4 529
5 %	385 000	17	22 647
10 %	770 000	17	45 294
50 %	3 350 000	17	226 471
100 %	7 700 000	17	452 941

Autrement dit, en supposant que le prix actuel de marché (3 200 dollars à l'heure où nous écrivons[320]) correspond à la valeur actuelle intrinsèque du bitcoin, et que l'usage transactionnel reste négligeable pour les raisons évoquées précédemment, nous pouvons déterminer ainsi l'équivalent part de marché-or du bitcoin aujourd'hui :

$$\text{Part de marché}_{BTC\ -\ or} = \frac{\text{Valeur actuelle x bitcoins en circulation}}{\text{Valorisation de l'or}} \approx 1{,}8\ \%$$

Tom Lee, cofondateur de FundStrat Global Advisor, explique dans une interview qu'il est raisonnable de penser que le bitcoin pourrait représenter 5 % de la valeur de l'or – ce qui revient à supposer que les investisseurs n'allouent que 5 % de leur portefeuille aux monnaies dites alternatives, et en réalité constitue une hypothèse plutôt conservatrice[321]. Dans ce cas, la valeur unitaire du bitcoin s'établirait autour de 25 000 dollars.

---

319. Lien : money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/
320. Le 31 décembre 2018.
321. Lien : www.businessinsider.com/bitcoin-price-how-to-value-fundstrat-tom-lee-2017-10?IR=T

Approche par la valeur transactionnelle

Prenons l'hypothèse qu'un jour, le bitcoin sera devenu un moyen courant pour réaliser des transactions, et son usage principal résidera donc dans l'aspect transactionnel. Nous supposons qu'il pourra être alors pleinement considéré comme une monnaie, tant d'un point de vue théorique que concret.

Plusieurs approches ont été développées[322], en considérant la capitalisation de marché du bitcoin comme une part de marché des transferts d'argent internationaux ou encore de la masse monétaire. L'équation de la théorie quantitative de la monnaie est un cadre théorique plutôt pertinent dans ce contexte :

$$MV = pq$$

M : la quantité de monnaie en circulation ;
V : sans unité, la vitesse de circulation de la monnaie durant un temps, c'est-à-dire le nombre de fois qu'une monnaie « change de main » (la fréquence de transactions) sur une période donnée ;
p : le prix de la ressource ;
q : la quantité de ressource.

Cette équation n'exprime pas la valeur du bitcoin au sens de l'évaluation financière (actualisation d'un flux financier futur, nous reviendrons sur cette notion), mais permet de déterminer des parités de change entre deux masses monétaires. Par cette équation, la valeur unitaire du bitcoin peut être estimée par la prévision de la demande engendrée par la ressource sous-jacente distribuée par le réseau – le produit *pq* (ce qui pourrait se rapprocher d'un PIB de réseau), divisé par la base « monétaire » disponible. Conceptuellement, cette équation peut se résumer à l'égalité bien connue : offre = demande, l'offre étant constituée de la monnaie disponible, multipliée par la vitesse de circulation. Le membre de droite de l'équation correspond au besoin, à la richesse produite par le réseau, tandis que le membre de gauche représente l'économie monétaire associée.

Appliquer cette équation au bitcoin nécessite de poser quelques hypothèses. Nous exprimerons le PIB du réseau comme une part du PIB mondial. Cette part peut être différenciée par continent, par industrie et ou encore par segment de transactions (transactions plus ou moins volumineuses, plus ou moins critiques…).

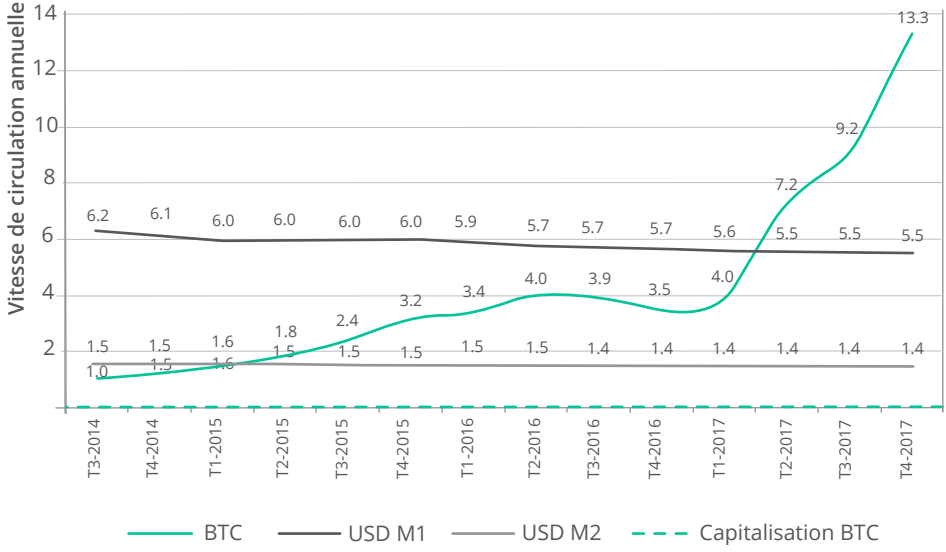
---

322. La plus connue à date reste celle de Chris Burniske, « Cryptoasset Valuation », *Medium*, 24 septembre 2017.

La vitesse de circulation de la monnaie est difficile à projeter. Une première approche consiste à calculer la vitesse de circulation historique du bitcoin. Celle-ci est calculée annuellement, en divisant le volume des transactions sur une année par la capitalisation de marché moyenne de cette même année. La limite de cette première approche est qu'historiquement, c'est la spéculation qui génère la grande majorité des transactions, et donc qui influence le plus la vitesse de circulation.

Mais quelle serait la vitesse de transaction pour un usage purement transactionnel ? Une deuxième approche est de comparer la vitesse de circulation du bitcoin à celle d'autres monnaies de référence, par exemple le dollar. En exprimant la vitesse de circulation par trimestre (calculée sur une année glissante), nous obtenons la courbe suivante :

ÉVOLUTION COMPARÉE DES VITESSES DE CIRCULATION MONÉTAIRE DU BITCOIN ET DU DOLLAR[323] (M1 ET M2)



Nous avons distingué les différentes définitions de la masse monétaire en dollar. Pour rappel, M1 désigne les billets, pièces et dépôts à vue. M2 inclut M1, mais inclut également les dépôts à terme inférieurs ou égaux à deux ans et les dépôts assortis d'un préavis de remboursement inférieur ou égal à trois mois (par exemple, pour la France, le livret jeune ou le CODEVI, les livrets A et bleu, le compte d'épargne logement, le livret d'épargne populaire…).

323. Lien : https://fred.stlouisfed.org/series/M1V

Si le bitcoin était aujourd'hui une monnaie reconnue, alors il serait utilisé pour réaliser une partie des transactions mondiales (part du PIB mondial). Une étude approfondie permettrait de prendre des hypothèses détaillées par géographie et par industrie, en fonction de l'état d'acceptation des crypto-monnaies au sens large, et de la taille du marché adressé par le bitcoin. Ce marché étant compliqué à délimiter actuellement, nous avons fait le choix d'hypothèses simples, calibrées en pourcentage du PIB mondial capté. Nous avons supposé cette part comprise entre 1 % et 10 % du PIB monde. En effet, à titre indicatif, le marché des transferts de fonds à lui seul est estimé à 4,6 % du PIB mondial[324].

Quant à la vitesse de circulation du bitcoin, il est difficile de déterminer à combien elle s'établira une fois qu'il sera stabilisé. La vitesse historique en forte croissance, est due à l'engouement récent, mais pourrait évoluer à mesure qu'un usage « réel » émergera. Nous avons donc émis l'hypothèse qu'elle serait comprise entre 1,5 (vitesse de la masse monétaire M2 des dollars américains) et 15 (approximation de la vitesse de circulation actuelle, principalement liée à la spéculation).

Nous avons construit une table de sensibilité sur la valeur induite unitaire du bitcoin, en faisant varier le pourcentage du PIB monde adressé et la vitesse de transaction. Nous obtenons le résultat suivant :

VALEUR INDUITE UNITAIRE DU BITCOIN (EN $)

	PART DU PIB DU MONDE						
Vitesse de circulation	1,0 %	2,0 %	3,0 %	4,0 %	5,0 %	7,5 %	10,0 %
1,5	31 090	62 180	93 271	124 361	155 451	233 176	310 902
3,0	15 545	31 090	46 635	62 180	77 725	116 588	155 451
4,5	10 363	20 727	**31 090**	**41 454**	**51 817**	77 725	103 634
6,0	7 773	15 545	**23 318**	**31 090**	**38 863**	58 294	77 725
7,5	6 218	12 436	**18 654**	**24 872**	**31 090**	46 635	62 180
10,0	4 664	9 327	13 991	18 654	23 318	34 976	46 635
15,0	3 109	6 218	9 327	12 436	14 545	23 318	31 090

Avec ces hypothèses, les valeurs centrales de la table[325] font ressortir une valeur transactionnelle du bitcoin comprise entre 18 654 dollars et 51 817 dollars. La valeur moyenne induite par cet encadrement placerait le bitcoin autour de 35 000 dollars.

---

324. Lien : https://www.theglobaleconomy.com/rankings/remittances_percent_GDP/
325. Les valeurs centrales correspondent aux scénarios pour lesquels les variables ont une valeur proche de leur valeur moyenne.

Enfin, si le bitcoin est accepté comme monnaie par l'économie traditionnelle, il est probable qu'il porte, tout comme le dollar, une double utilité : usage transactionnel et réserve de valeur. Dans ce cas, l'équation quantitative de la monnaie est toujours applicable :

$$MV = pq$$

Il faudra néanmoins définir séparément les deux composantes de la demande – que l'on suppose additives – et calculer une vitesse moyenne de circulation correspondant à la moyenne des vitesses de chaque usage, pondérée par la demande associée.

Afin de donner un ordre de grandeur, reprenons nos hypothèses précédentes. L'usage réserve de valeur correspond à 5 % de la valeur de l'or, impliquant une demande de 385 milliards de dollars. Notons que cet usage pourrait également être chiffré en parts de marché du montant d'épargne mondial annuel. L'usage transactionnel est un flux et nous le supposerons égal à 4 % du PIB mondial, impliquant une demande de 3 171 milliards de dollars.

Ainsi le PIB total du réseau Bitcoin se chiffrerait au total à 3 556 milliards de dollars.

Une nouvelle fois, la vitesse de circulation reste une variable très difficile à estimer. Une façon de l'exprimer revient à calculer la vitesse de circulation moyenne sur les deux usages, pondérée par la demande associée à chaque usage. La vitesse de circulation du bitcoin s'exprimerait alors de la façon suivante :

$$v = \frac{V_{refuge} \times D_{refuge} + V_{transaction} \times D_{transaction}}{D_{refuge} + D_{transaction}}$$

Nous prenons l'hypothèse que la vitesse de circulation du bitcoin pour l'usage refuge de valeur est égale à 1 : un individu achète une fois des bitcoins pour les conserver sur le long terme. Pour l'usage transactionnel, supposons que la vitesse de circulation du bitcoin est inférieure à 6, vitesse moyenne de circulation de la masse monétaire M1 de dollars américains, car, à cause des frais de transaction, le bitcoin serait réservé à des transactions importantes uniquement. Nous fixons donc cette vitesse à 3. La vitesse de circulation globale du réseau Bitcoin est alors égale à :

$$v = \frac{385 + 3 \times 3171}{3556} = 2.8$$

La capitalisation de marché du bitcoin serait alors

$$M = \frac{3556}{2.8} = 1278 \text{ mds\$}$$

En considérant le nombre actuel de bitcoins en circulation, le prix unitaire du bitcoin serait alors :

$$Valeur_{BTC} = \frac{1\ 277\ 611}{17} = 75\ 154\ \$$$

Notons qu'ici nous considérons le nombre actuel de bitcoins en circulation, au même titre que nous calibrons la demande sur le PIB mondial 2017. De plus, nous n'intégrons pas le fait que le bitcoin est en fait en compétition avec d'autres protocoles et d'autres crypto-monnaies. S'il demeure toujours l'actif de référence sur ce marché naissant, il est envisageable qu'il soit attaqué stratégiquement par d'autres initiatives, comme ce fut le cas avec Ethereum par exemple.

IV.2.b Le cas des *utility tokens*

Revenons à la définition de la valeur d'un actif financier : il s'agit de la valeur future actualisée des flux générés par cet actif, c'est-à-dire prenant en compte la valeur-temps de l'argent, et rémunérant le risque de l'investisseur. Dans le cas d'une action par exemple, il s'agit des flux de dividendes perçus tout au long de la période de conservation du titre.

Cette définition est-elle applicable aux crypto-actifs ? La réponse est oui dans le cas des *security tokens*, imitant le comportement des actions, pour lesquelles les méthodes de valorisation sont connues et maîtrisées – et dépassent le cadre de notre étude.

La réponse est également oui dans le cas d'un *token utility* : le flux financier correspondra alors à la valeur du service associé lors son utilisation. Reprenons le cas du javelcoin. Lors de l'ICO, j'ai acheté un javelcoin pour 10 euros. Imaginons alors que le service prenne de la valeur ; dans notre cas, cela pourrait être dû à la fermeture de l'ensemble des autres lavomatiques du quartier. La demande sera alors concentrée sur le javelcoin, ce qui fera mécaniquement augmenter sa valeur utilitaire[326].

Quelle est alors la valeur fondamentale du javelcoin ? Elle sera égale à la valeur future utilitaire, sur un horizon d'investissement donné, en prenant en compte le risque que l'investisseur porte sur cette durée.

326. Ce qui suppose une offre fixe ou décroissante.

L'objectif est donc de projeter la valeur utilitaire future, en estimant la demande liée au service, et en la rapportant au nombre de *tokens* en circulation, à chaque date. La valeur utilitaire future doit cependant intégrer la probabilité de succès du projet, celui-ci n'étant pas, dans la plupart des cas, opérationnel au moment de l'ICO (l'objectif de l'ICO est justement de lever les fonds nécessaires à la livraison du produit).

L'objectif est donc de projeter la valeur utilitaire future du *token*, en fonction de la demande. La valeur fondamentale d'un *token* s'exprimera alors :

$$\text{Valeur intrinsèque} = \frac{\text{Valeur utilitaire future}}{(1 + r)^n}$$

Avec :

n : la période au bout de laquelle a lieu l'utilisation « cible », exprimée en années. Cette période correspond au nombre d'années nécessaires pour atteindre la phase de maturité du produit.
r : le taux d'actualisation, prenant en compte la valeur temps de l'argent et rémunérant le risque de l'investisseur. Il est usuellement déterminé grâce au MEDAF[327].

Notons d'ailleurs que ce modèle, très simple, est également valable pour le marché des crypto-actifs, mais la trop faible profondeur historique actuelle fausse l'application numérique. Dans les modèles actuels, ce taux est fixé arbitrairement autour 40 %.

La grande majorité des méthodes d'évaluation des crypto-actifs existant à l'heure actuelle indique que la valeur d'utilité peut être estimée par la prévision de la demande, engendrée par la ressource sous-jacente distribuée par le réseau – ce qui pourrait se rapprocher d'un PIB de réseau –, divisée par la base « monétaire » disponible. Il s'agirait donc d'une extrapolation de l'équation quantitative de la monnaie, dans la mesure où, dans un réseau Blockchain, le *token* se comporte comme unité de compte de référence. La valorisation des *tokens* étant encore à ses débuts, aucune étude n'a encore prouvé que cette équation s'applique bien aux crypto-actifs ; cependant, elle a l'avantage de répliquer les mécanismes de circulation monétaire. En effet, il est nécessaire de prendre la circulation monétaire en compte dans la modélisation, car l'unité de compte est circulante, ce qui a pour effet d'augmenter l'offre disponible. Durant cette étude, nous prendrons donc l'hypothèse que les crypto-actifs ont un comportement similaire à celui des monnaies au sein d'un réseau défini, afin d'utiliser l'équation quantitative de la monnaie.

327. Modèle d'évaluation des actifs financiers, ou CAPM en anglais. Il permet de calculer le rendement d'un actif en fonction de son risque systématique, c'est-à-dire non diversifiable.

Au même titre qu'un analyste financier réaliserait une projection de flux financiers liée à un plan d'affaires, l'objectif de l'exercice est de projeter une trajectoire de demande par rapport à un service, et de la rapprocher de l'offre disponible pour en déduire une valeur utilitaire unitaire. Formellement, la valeur utilitaire du *token* sera donc exprimée de la façon suivante :

$$w = \frac{pq}{M'V}$$

M' correspond à la masse monétaire en crypto-actifs (c'est-à-dire le nombre de *tokens* sur le marché) ; en multipliant l'équation par $M'V$, on retrouve l'équation quantitative de la monnaie.

Cette approche est similaire à celle appliquée au bitcoin par l'utilisation de l'équation quantitative de la monnaie, mais en diffère dans son application finale. Le bitcoin étant considéré comme une monnaie, il ne s'évalue pas, mais se valorise par rapport à une autre. Pour un *token*, il s'agit d'utiliser cette équation pour modéliser la circulation du *token* dans l'écosystème créé, et de projeter sa valeur utilitaire unitaire, en fonction d'une trajectoire de demande. La valeur utilitaire future sera ensuite actualisée pour obtenir la valeur fondamentale du *token*.

La grandeur *pq* peut être estimée grâce à une approche stratégique traditionnelle de type *market sizing* en estimant la taille de marché adressable et calibrant la demande par un taux de pénétration croissant, usuellement en suivant une courbe en S.

M' est une grandeur clé d'un crypto-actif, et souvent indiquée dans le *whitepaper* du projet lors de sa création. Son évolution dans le temps doit être connue. Aujourd'hui, la majorité des *tokens* utilitaires ont une offre de *tokens* fixe, et parfois même décroissante (on parle alors de *burn*). L'objectif du *burn* est simple : les *tokens* émis par l'entité ont une destruction programmée une fois utilisés, permettant de raréfier l'offre et donc de mécaniquement augmenter la valeur utilitaire par *token*.

L'application de cette équation présente deux difficultés majeures, que nous détaillerons par la suite : la connaissance de la demande (pq) et l'estimation de la vitesse de circulation (V). Elle nécessite également de prendre comme hypothèse une durée d'investissement, et un taux d'actualisation.

Focus sur la demande

La demande pour un *token* peut se décomposer en trois parties principales, et s'écrire de la façon suivante :

$$Demande_{token} = Demande_{utilitaire} + Demande_{spéculative} + Demande_{StoreofValue}$$

La demande utilitaire est liée à l'usage en lui-même. Elle correspondra à une part du marché adressable, dont on déduit la demande de *tokens* nécessaires associée (l'accès au service ou produit ne peut se faire qu'avec le *token* créé). Dans le cadre du calcul de la valeur fondamentale, seule cette demande est prise en compte, permettant de calculer la valeur utilitaire future. La demande spéculative permet de rationaliser la demande lorsque le service n'est pas encore opérationnel.

La demande spéculative est liée à la recherche de gains financiers sur l'achat, puis la vente d'un *token*. À la suite d'une ICO, lors de la cotation sur les plates-formes d'échanges, le produit ou service associé au *token* n'existe généralement pas. Cependant le prix de marché ne tombe pas pour autant à zéro, puisqu'il est soutenu par une demande spéculative du marché, représentant une anticipation de la valeur utilitaire future. À l'équilibre du marché, cette demande spéculative prend en compte une probabilité perçue de réussite du projet.

À date, trois approches principales ont été données pour apprécier cette demande spéculative :

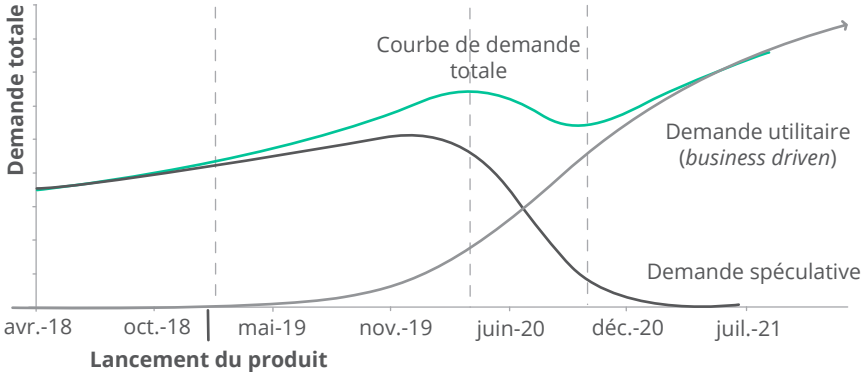
a. Chris Burniske[328] la modélise comme étant une pression de vente, c'est-à-dire qu'il considère que l'offre réelle n'est qu'un pourcentage du nombre de *tokens* en circulation, en raison de la rétention de *tokens* par certains investisseurs. Initialement, la pression de vente est faible, la plupart des détenteurs de *tokens* les conservent en attendant que le produit soit opérationnel. Peu à peu, ce pourcentage augmente au fil de l'accroissement de la demande utilitaire (associée au service lui-même).

b. Nous considérons que la demande spéculative n'existe que lorsque le produit n'est pas encore opérationnel. En effet, une fois qu'il l'est, le prix de marché du *token* devrait se stabiliser – et l'investissement spéculatif devrait alors se reporter sur d'autres actifs non matures. Ainsi, si l'acceptation du produit (c'est-à-dire la demande utilitaire) suit une courbe en S, alors la demande spéculative devrait suivre une courbe plus ou moins symétrique, de la façon suivante :

---

328. Chris Burniske, septembre 2017. Lien : https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7

DÉCOMPOSITION DE LA DEMANDE TOTALE



La première phase correspond au lancement du projet et à l'adhésion au concept. Le produit/service n'étant pas encore fonctionnel, la demande est purement spéculative, liée à l'anticipation de la valeur utilitaire future. Le lancement du produit constitue la deuxième phase ; la demande reste néanmoins principalement spéculative, et augmente car la probabilité d'échec du projet est désormais négligeable. La troisième phase est une correction de la demande spéculative pour s'ajuster sur l'utilité réelle. Finalement, la demande sera principalement utilitaire, et nous supposons dans ce cas que la demande spéculative est négligeable.

Notons qu'en théorie, la demande spéculative ne devrait pas dépasser la demande utilitaire, dans la mesure où elle incorpore la probabilité de succès du projet, par définition inférieure à 1. Dans le cas contraire, c'est que le produit est surévalué par le marché.

La demande réserve de valeur correspond au cas où le *token* est en circulation et qu'il est stable. Dans ce cas, un investisseur pourrait l'acheter en tant que réserve de valeur pour la confiance qu'il apporte dans sa capacité à transférer des valeurs dans le futur. Cependant, peu de *tokens* utilitaires présentent aujourd'hui les caractéristiques d'une réserve de valeur, ce qui n'est d'ailleurs pas leur objectif initial. Nous supposerons donc que cette composante de la demande est négligeable.

L'estimation de la vitesse de circulation

C'est le paramètre le plus compliqué à estimer. Trois approches existent :

a. Dans le cas d'un projet centralisé, la vitesse de circulation est un paramètre. Dans l'exemple du lavomatique, c'est l'entreprise à qui je verse mes *tokens* qui décide du rythme de remise en circulation sur le marché. Ce paramètre est fondamental : en conservant les *tokens*, l'entreprise peut artificiellement créer de la rareté et faire augmenter le prix. Notons que dans le cas où les *tokens* ne sont pas remis en circulation (c'est-à-dire qu'ils sont brûlés lorsqu'utilisés), il n'y a pas de problème de circulation monétaire ; le *token* se comporte alors comme une forme de chiffre d'affaires.

b. Chris Burniske définit la vitesse de circulation comme constante, étant égale à la vitesse pondérée des demandes spéculatives et utilitaires, supposées constantes également. C'est une hypothèse évidemment peu probable.

c. Alex Evans contourne la question, en définissant un nombre de transactions optimal, calculé en fonction des frais de transfert. La limite principale de cette méthode est la projection des frais de transactions dépendant de nombreux facteurs exogènes (prix du bitcoin, de l'ether, frais des plates-formes d'échange…).

Outre la valeur elle-même de cette vitesse, la réelle question, soulevée par Alex Evans, est de savoir comment elle varie avec la demande. Trois cas de figure apparaissent :

a. Si la demande (pq) est fortement corrélée à la vitesse de corrélation, alors la vitesse aura un impact stabilisateur sur la valeur utilitaire du *token*.

b. Si la vitesse et la demande ne sont pas corrélées, alors la valeur utilitaire évoluera proportionnellement à la demande sous-jacente.

c. Si la demande est négativement corrélée à la vitesse de corrélation, alors la vitesse aura un aspect déstabilisateur sur le prix du *token*. En effet, si la demande baisse et que la vitesse (donc l'offre) augmente, le prix chutera automatiquement.

Il faut donc comparer l'évolution du taux de croissance de la vitesse et de la demande. Si la vitesse croît plus vite que la demande, alors la valeur utilitaire du *token* baissera.

IV.2.c Étude d'un cas réel : Peculium

Contexte et cadre général d'analyse

Nous avons déployé au premier trimestre 2018 une méthodologie similaire au côté de la start-up Peculium, combinant approches stratégique et financière adaptées à l'économie de la Blockchain.

Cette start-up française a pour ambition de devenir la première plateforme de gestion d'épargne, gérée par l'Intelligence Artificielle (outil dénommé AIEVE), sur le marché des crypto-actifs.

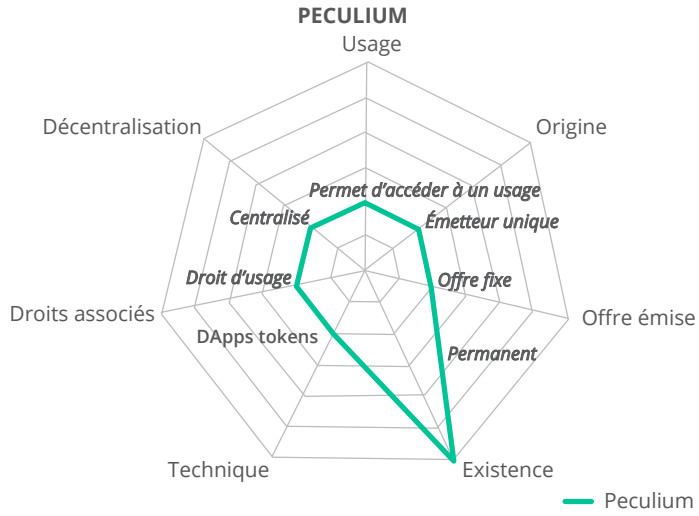
Peculium a réalisé une ICO à destination des investisseurs individuels qui s'est achevée au mois de janvier 2018, avec environ 8,1 millions d'euros collectés. Lors de l'ICO, Peculium a cédé son *token*, le PCL, au cours initial de 1 PCL = 0.01 euro.

Peculium propose deux types de services :

a. Gestion personnelle de l'épargne (nommée « singulus » pour la clientèle particulière, « alterus » pour les professionnels) : un client place une somme, par exemple 100 euros, sur les crypto-actifs de son choix (bitcoin, ether, litecoin…). Lorsqu'il le souhaite, l'investisseur peut demander des conseils d'investissements à l'outil d'intelligence artificielle AIEVE, qui lui indiquera comment il doit modifier la répartition de son portefeuille correspondant à son profil de risque. Il reste libre de suivre ou non le conseil d'AIEVE. Dans tous les cas, il verse à Peculium un certain nombre de PCL, rémunérant ces mêmes conseils.

b. Gestion automatique de l'épargne (le « solidus »). Un client place une somme, et indique ses préférences d'investissement : choix des crypto-actifs sous-jacents, profil de risque, durée d'investissement… Le portefeuille est alors géré automatiquement par AIEVE. À chaque fois qu'AIEVE réussit un mouvement sur le portefeuille, des frais – en PCL – sont prélevés du compte du client.

Le PCL est un *utility token*, donnant droit au service de Peculium, à savoir notamment l'accès à sa solution d'Intelligence Artificielle, AIEVE. En plaçant le *token* sur les axes analytiques définis précédemment, nous obtenons la représentation suivante :

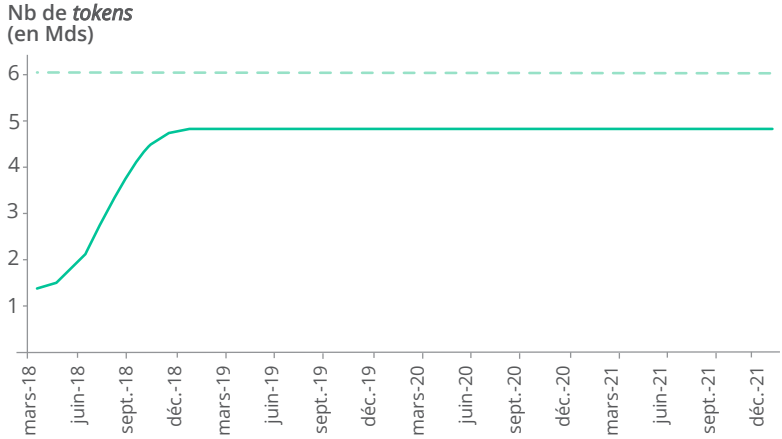


Afin de définir la trajectoire financière du *token*, nous avons utilisé l'équation quantitative de la monnaie. En effet, si le PCL n'a pas d'objectif monétaire à proprement parler, il constitue néanmoins une valeur permettant d'acheter un service et circulant de main à main :

$$w = \frac{pq}{M'V}$$

Détermination de la trajectoire d'offre, M'

Le nombre de *tokens* en circulation correspond au nombre de *tokens* vendus lors des deux phases d'émission de *tokens*, l'ICO et la CCO. Nous avons obtenu la trajectoire suivante :



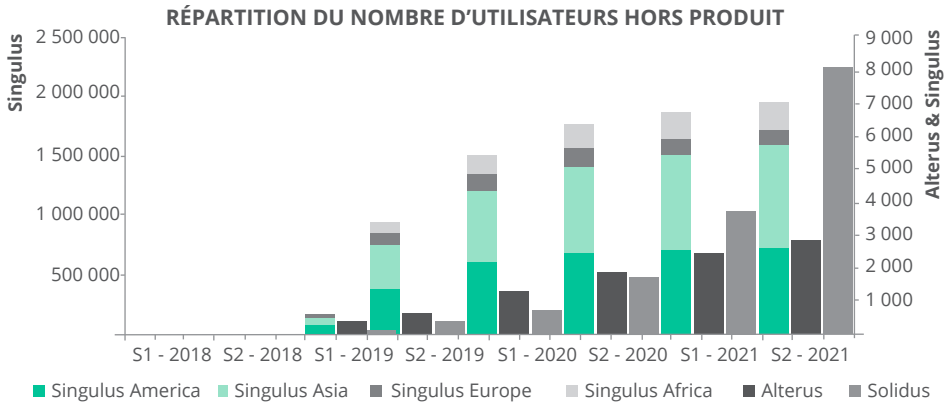
La ligne en pointillé correspond à l'offre maximale théorique en circulation, tandis que l'offre réelle dépend du succès commercial (ligne pleine illustrative). En effet, les *tokens* non vendus dans le cadre des deux opérations de levée (ICO et CCO) seront brûlés.

Détermination de la vitesse de circulation

Le modèle de projection étant mensuel, nous avons pris comme hypothèse une vitesse mensuelle de 1, soit une vitesse annuelle de 12. Cet élément est néanmoins paramétrable, dans la mesure où, dans le cas de modèle centralisé comme Peculium, la rapidité de la remise en circulation est à la main de l'entreprise. Ici, nous supposons que cette dernière conserve le *token* un mois après son versement par un client pour accéder à son service.

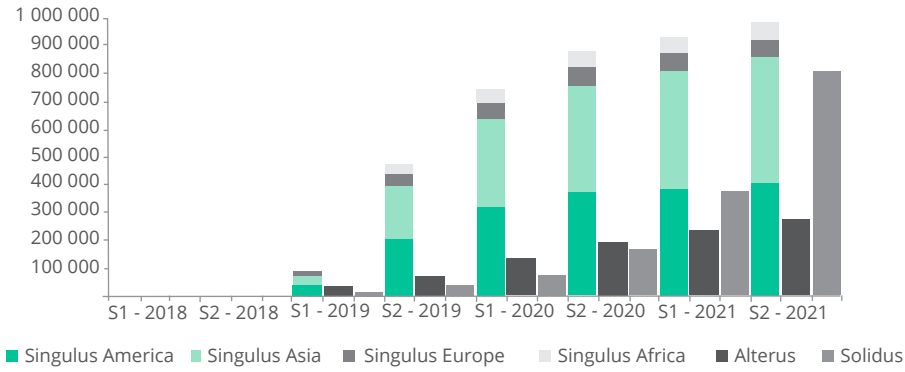
Détermination de la demande

Sur le plan stratégique, nous avons adopté une approche de type *market sizing*, permettant d'anticiper la clientèle intéressée par le produit. Nous proposons une segmentation selon un axe géographique, jugé pertinent au regard de l'analyse des données statistiques du nombre de visites sur le site Internet, fournies par *Google analytics*. Deux foyers d'intérêt se distinguent ; entre les pays occidentaux *digital friendly* et les pays émergents en demande de solution d'épargne alternative[329]. Sur la base du mix-client géographique et produit, et tenant compte de paniers moyens cibles en termes d'*Asset under Management* (AuM), nous déduisons une trajectoire future de demandes de PCL. En effet, ce dernier est la porte d'entrée aux services de l'entreprise.



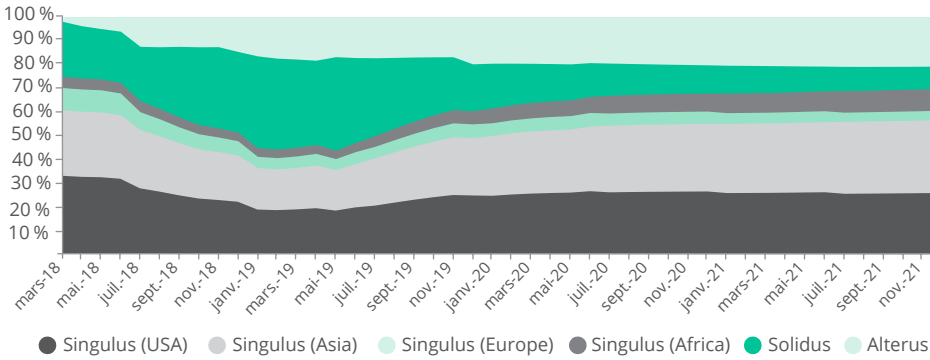
329. Se référer à notre chapitre dédié à l'économie, dans lequel nous présentons dans le détail les motivations des catégories de clients, illustrées par une cartographie des visites sur le site.

ACTIFS SOUS GESTION, PAR PRODUIT (EN K €)



Nous émettons l'hypothèse que la demande spéculative de PCL n'existe que tant que le produit n'est pas opérationnel. Nous supposons que la demande spéculative à date n'est que l'anticipation de la valeur transactionnelle future liée à la consommation du service. Dès lors, la valeur spéculative décroît et tend vers zéro, à mesure que la valeur transactionnelle augmente, consécutivement aux lancements des produits. En respectant la *roadmap* technique (c'est-à-dire le planning de sortie de chaque produit), nous déduisons une demande pour chaque produit[330].

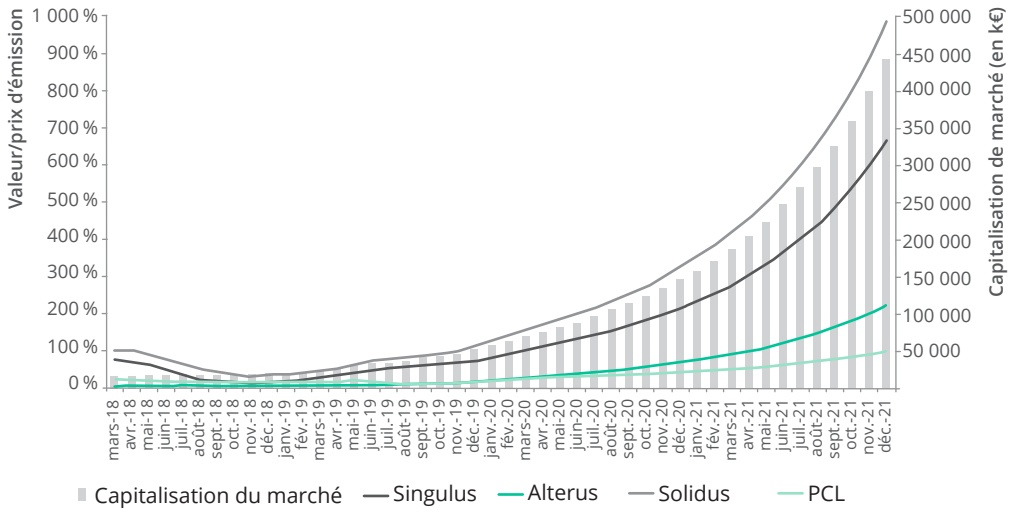
PROJECTION DE LA DEMANDE DE PCL PAR PRODUIT



En divisant la demande modélisée à chaque date par le nombre de *tokens* en circulation à chacune des dates, nous obtenons la courbe de projection de valeur utilitaire. La valeur utilitaire du PCL est exprimée en pourcentage de son prix d'émission lors de l'ICO.

330. Somme des courbes présentées précédemment pour chaque produit.

COURBE DE PROJECTION DE LA VALEUR UTILITAIRE DU PCL, AVEC UNE DÉCOMPOSITION PAR PRODUIT



On retrouve l'impact de la croissance du nombre de *tokens* en circulation sur la valeur utilitaire unitaire. Le modèle ci-dessus prévoit alors la valeur du PCL autour de 0,1 en 2021 (dix fois le prix de l'ICO), représentant une capitalisation de marché de 450 millions d'euros.

Dans un cadre d'analyse fondamentale, quel prix devrait donc coter le PCL sur un marché efficient dénué de spéculation irrationnelle (nous avons vu que ce n'était pas le cas) ? Théoriquement, le prix du PCL devrait s'établir à sa valeur utilitaire à terme, actualisée en tenant compte du prix du temps et du risque. De façon simplifiée et en négligeant l'effet-temps, on peut considérer que le prix à date devrait être la valeur utilitaire future multipliée par une probabilité de succès du projet.

V.
Création de valeur et investissement

V.1 Des opportunités pour les fonds d'investissement

L'introduction du *token* comme nouvel instrument financier brouille les cartes de la répartition de la valeur économique créée. L'investissement en capital est-il toujours pertinent ? Le crypto-actif va-t-il accaparer la totalité de la valeur, une partie seulement ou celle-ci restera-t-elle logée dans le capital[331] ? La répartition de la valeur dépend fortement de la nature du projet et du crypto-actif.

Pour comprendre de façon simplifiée ce que devrait représenter le prix d'un crypto-actif, prenons deux exemples : un exemple d'*utility token* centralisé et le cas d'une crypto-monnaie parfaitement décentralisée.

a. Les projets centralisés : si la Blockchain est la technologie de la décentralisation, plusieurs projets Blockchain sont en réalité centralisés : une entité centrale exécute le service. Dans le cas du lavomatique, l'utilisation des machines est assurée par un acteur central. En recourant à l'ICO, l'entrepreneur cède un droit d'usage en l'échange d'un *token* « javelcoin ». Deux cas de figure s'offrent alors :

- Le prix du service est fixé en euro, par exemple un lavage = 15 euros. Dans ce cas, le client paiera en javelcoins, au cours correspondant sur le marché. Le nombre de javelcoins nécessaire à la consommation du service s'ajustera en conséquence. Dans ce cas, le rôle du *token* au sein de l'équation économique de l'entité est plutôt limité. Ce point fait écho à nos réflexions sur la *due-diligence* à mener dans le cadre d'une ICO ou d'un investissement en crypto-actifs. Pourrait-on envisager de réaliser le même service sans *token* ? Dans le cas présent, la réponse est oui, le client pourrait payer en euros, bitcoins ou autres, pour un service équivalent, d'ailleurs largement répandu dans nos villes. Doit-on considérer dans ce cas que le crypto-actif ne sert à rien ? Non, car il représente la contrepartie de la participation communautaire de type *crowdfunding* à un projet, matérialisée par une fraction de l'usage mis en marché.

331. Du point de vue des actionnaires.

- Le prix du service est fixé en javelcoins[332], par exemple un lavage = 1 javelcoin. Dans ce cas, quelle que soit la parité de cette métrique en euros, le consommateur réglera un lavage avec un javelcoin. Si le prix de la lessive est libellé en unité créée, c'est donc le marché qui va définir – par la dynamique de l'offre et de la demande – en équivalent euros, le prix qu'il attribue à ce service. En effet, imaginons que le prix initial lors de l'ICO était de 1 javelcoin = 5 euros. Le cours du javelcoin évoluera au gré de l'offre et de la demande jusqu'à atteindre le prix de marché du service. Dans ce cas absurde, il n'y a pas de raison de penser, à service équivalent, que ce prix soit différent d'un lavomatique traditionnel. Ni la technologie Blockchain ni les mécanismes économiques activables autour d'elle ne s'appliquent ici, il est donc raisonnable de penser que le marché attribuerait une valeur au service, au mieux, équivalente aux autres lavomatiques[333]. Mais cette logique peut s'avérer très puissante sur des modèles existants aux mécanismes de formation des prix plus complexes, *a fortiori* dans le cas de nouveaux modèles économiques dont on ne connaît pas *a priori* le prix du service. Le risque d'erreur de *pricing* est important lors de la mise en marché d'un service nouveau, dont on connaît mal la valeur que les consommateurs lui attribueront. La mise en marché de l'usage par ICO permet en théorie de connaître rapidement cette information. Bien que le nombre d'unités en circulation puisse être fixe, l'offre disponible est un paramètre à la main de l'émetteur. Lorsqu'un client achète un lavage, il verse un javelcoin à l'entreprise. Celle-ci peut alors remettre immédiatement ou non le *token* en circulation *via* une place de marché. Si elle le réinjecte directement sur le marché, alors l'offre disponible sera mécaniquement plus élevée que si elle décide de le conserver à son actif pendant un mois. Dans ce cas, la rétention d'offre, même temporaire, impacterait positivement le prix du *token*. La vitesse de circulation est donc une variable d'ajustement de l'initiative centralisée. Concrètement, la principale limite à cette analyse réside dans la nature des investissements réalisés en *tokens*, qui repose encore peu sur une analyse fondamentale. Ainsi, le prix constaté sur le marché peut être décorrélé de l'appréciation par les consommateurs de la valeur du service, forçant l'entreprise à revoir le *pricing* libellé en *tokens* (pour maintenir un prix équivalent euros en ligne avec la réalité du produit).

  À noter que les actions ne disparaîtront pas ! Plusieurs modèles centralisés œuvrant sur le sujet Blockchain ne font pas d'ICO et lèvent des montants significatifs en capital. On peut citer notamment la

332. Nom de *token* fictif créé pour l'exemple.
333. En fait, ce nouvel acteur serait peut-être même à terme moins compétitif que ses concurrents du fait de l'ajout d'un facteur de complexité inutile (utilisation d'un *token*).

levée de l'entreprise de *mining* Bitfury (80 millions de dollars), les tours de table de Ledger (75 millions de dollars) ou plus récemment les levées de ACinq (1,4 million d'euros) pour développer le « *lightning network* ».

b. Les projets décentralisés : en exploitant toute la puissance technologique et économique de la Blockchain, autour notamment du pair-à-pair, des effets de réseaux et des alignements d'intérêts fidèles au *mechanism design*, ces écosystèmes proposent des systèmes conceptuellement complexes mais aux logiques franches et lisibles. Dans le cas d'un système parfaitement décentralisé, la valeur du crypto-actif cristallise toute la valeur ajoutée créée par le produit ou service. Tout comme dans un modèle centralisé, la demande en crypto-actifs sera le principal *driver* de la valeur. Aucune entité centralisée ne maîtrise en revanche l'offre disponible, calibrée par le code lui-même (comme dans le cas du bitcoin).

En revanche, sur le plan financier, la difficulté réside dans la détermination de la vitesse de circulation qui n'est plus sous le contrôle d'une entité centralisée et dépend uniquement du comportement des utilisateurs réseau. À quelle vitesse les acteurs du réseau vont-ils s'échanger le bitcoin, par exemple ? La tendance du marché est à l'hybridation des formes ; décentralisation et centralisation ne constituent que les extrémités d'une palette de nuances, compliquant (encore) l'analyse. Nous rencontrons en effet des entrepreneurs avec un projet d'application, mais qui souhaitent adosser ce projet à leur propre chaîne publique, pour des motifs d'indépendance et d'adéquation entre les caractéristiques techniques de la Blockchain et les besoins de l'usage. Ce choix conduit à une sorte de bitcoin semi-décentralisé, comportant des effets de réseau mais ancré dans une entreprise. Quelle sera la répartition de la valeur entre l'*equity* et les crypto-monnaies du réseau dans ce cas ? Une chose est sûre, un travail, au cas par cas, d'analyse de la *token economy* et des dynamiques sous-jacentes au projet est clé pour décider.

V.2 Quelle création de valeur sur la chaîne de valeur de la Blockchain ?

V.2.a Quelle répartition de la valeur entre applications et sous-couches ?

Contrairement à Internet, il est probable que les sous-couches accaparent une grande part de valeur[334]. En effet, le *Web* fonctionne grâce aux protocoles (TCP/IP, HTTP…) qui accaparent peu de valeur, contrairement à la couche applicative, qui a vu naître des entreprises internationales comme Facebook ou Google.

Au contraire, pour qu'une application puisse fonctionner sur un protocole Blockchain, comme le Bitcoin ou l'Ethereum, elle doit payer des frais, en utilisant l'actif sous-jacent. Les applications acceptent de payer ces frais afin de bénéficier des avantages technologiques du protocole (sécurité, traçabilité…). Ainsi, plus les applications fonctionnant sur un protocole sont nombreuses, plus les informations stockées dans la chaîne sont importantes, plus la demande pour le crypto-actif associé sera forte (dans la mesure où c'est le seul moyen d'accéder à ces informations), et donc plus le protocole aura de la valeur.

Il reste néanmoins difficile de déterminer si cette situation s'explique par le caractère « *early stage* » de la technologie, ou si elle est structurelle.

V.2.b Le *token utility* : un actif jetable ?

La question de la durée de vie d'un *token utility* mérite d'être abordée. En tant qu'entrepreneur, une fois émis, quelle durée de vie donner à mon *token* ? Plusieurs scénarios sont envisageables.

Option 1 : conservation des *tokens* comme unique moyen d'accéder aux services.

Les crypto-actifs se développent, et de plus en plus d'applications utilisent leur propre monnaie digitale correspondant à un service. Le problème que pourrait soulever un tel fonctionnement, tel qu'expliqué par John Pfeffer[335], est qu'il faudrait alors posséder un *token* pour chaque usage (javelcoin pour le lavomatique, pizzacoin pour la livraison de

334. Joel Monegro, août 2016. Lien : www.usv.com/blog/fat-protocols
335. John Pfeffer, avril 2018. Lien : https://medium.com/john-pfeffer/doubts-about-the-long-term-viability-of-utility-cryptoassets-db04350b1f55

pizzas…), ce qui représente un certain capital bloqué pour une utilisation bien précise et qui compliquerait la gestion individuelle de trésorerie. D'une certaine manière, cela consisterait à un retour à une forme de troc digital, séduisant intellectuellement mais probablement plutôt inefficace. En réponse à cette analyse, on peut imaginer un système de paiement automatique où les *tokens* utilisés pour le service seront achetés automatiquement par l'application à partir d'un compte libellé en bitcoin ou en monnaie traditionnelle, à condition que le marché se régule et que le risque de change reste limité.

Option 2 : destruction progressive des *tokens*

Une fois la solution lancée, il pourrait être décidé (après une certaine durée) de libeller le prix du service, en *token*, en monnaie traditionnelle et en bitcoin. En fonction de la stratégie de *pricing* par rapport aux différentes monnaies, l'entrepreneur peut influencer le comportement commercial des utilisateurs, et peu à peu les amener à utiliser le service en réglant en monnaie traditionnelle. Les *tokens*, qui n'auront donc servi qu'à financer l'investissement et éventuellement à découvrir le prix du service par le marché, pourront donc être détruits *(burn).*

Option 3 : transformation des *tokens*

Une troisième option serait de ne laisser en circulation qu'un nombre limité de *tokens*, et d'en changer l'usage principal. Ils ne seraient plus liés à un usage mais représenteraient un actif à conserver sur le long terme. Nous pourrions alors imaginer une transformation en actions (qui donnerait donc droit à des dividendes ou au vote).

En synthèse, le statut et le fonctionnement ne doivent pas être vus comme des éléments homogènes. En effet, chaque projet est différent et présente une *token-economics* particulière ; l'analyse doit être réalisée au cas par cas pour maximiser la création de valeur. De plus, le statut et le fonctionnement ne sont pas forcément figés dans le temps et peuvent évoluer au fil de la vie du projet.

V.3 Une réglementation balbutiante en cours de structuration

Dans ce cadre mouvant, encore exploratoire et en structuration, le risque réglementaire quant à la caractérisation de la nature de ces investissements reste majeur, tant du point de vue des investisseurs que des entrepreneurs.

Une première distinction possible est celle de la *Securities and Exchange Commission* (SEC), le gendarme financier américain. Il distingue les *security tokens*, matérialisant un droit de propriété sur un actif (part d'une entreprise par exemple), des *utility tokens* formalisant le droit d'accès aux services et produits d'un projet[336].

Le test de Howey, dessiné en 1946, permettrait de classifier une transaction comme un investissement de type *security*. Il faut pour cela qu'elle respecte les quatre règles suivantes : existence d'un investissement financier, attente de profits, investissement financier réalisé dans un projet commun et tout profit provient de l'effort d'une partie tierce. Ce test, très controversé, permet de clarifier grossièrement la différence entre un *security token* et un *utility token* :

- la majorité des ICO ne répond pas réellement à la définition des investissements financiers, et correspond davantage à une mise en vente de *tokens (utility)* ;
- les *tokens utility* ont par définition un usage autre que la simple attente de profit – ils sont liés à un service ; j'achète un *token* car je considère que son service est utile/a de la valeur ;
- il y a effectivement un projet commun, mais rarement une entreprise structurée. La notion de communauté dans la Blockchain constitue-t-elle un mode de projet commun au sens de la SEC ? ;
- lorsqu'un *token* est utilisé dans une communauté, il va générer de la valeur de pair-à-pair, sans nécessiter une entité tierce.

Un article daté du 20 avril 2018 du *New York Times* fait état d'une possible nouvelle régulation à venir clarifiant le cadre réglementaire des crypto-actifs aux États-Unis. Les résultats des réflexions de la SEC semblent s'orienter vers un cadre légal unifié autour de la définition de titre financier classique *(securities)*, qui mettrait donc fin à la dichotomie *utility vs security*. En tant que tels, ils devront obéir à certaines règles d'inscription auprès de la SEC pour toute nouvelle émission soumise à validation, mais aussi de cotation puisque seules des « places de marché transparentes et encadrées » pourraient être habilitées à lister ces actifs. Il semble que, sous l'impulsion des *venture capitalists* (dont notamment Andreessen Horowitz and Union Square Ventures), les crypto-monnaies décentralisées comme le bitcoin (et peut-être l'ether) pourraient être exemptées, dans la mesure où les créateurs n'ont pas le contrôle sur le réseau. Si une telle mesure devait se confirmer, plusieurs

336. Lien : https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

éléments resteraient à clarifier, comme le devenir des *tokens* déjà émis : seraient-ils reclassifiés en *securities*[337] ?

Le cadre réglementaire autour de la classification financière des crypto-actifs est en cours de structuration et devrait influencer significativement l'évolution du marché et la stratégie des acteurs. Les *security token offerings* (STO), sorte d'IPO nouvelle génération via Blockchain, pourraient être la nouvelle tendance. Plus contraignantes, elles seraient plus facilement arrimables au droit positif existant et mieux adaptées à la réglementation américaine notamment. Le projet Polymath travaille d'ailleurs à la mise en place d'une plateforme permettant l'émission facilitée de *security tokens*[338].

Parmi les avancées récentes majeures, on peut citer la publication du décret d'application de l'ordonnance Blockchain n° 2017-1674 du 8 décembre 2017, le 26 décembre 2018. Ce décret vient apporter des précisions quant aux conditions d'utilisation de « dispositifs d'enregistrement électronique partagé » prévus par l'ordonnance en ce qui concerne la transmission de titres financiers non cotés.

La loi PACTE (plan d'action pour la croissance et la transformation des entreprises) comporte également des avancées majeures en lien avec les problématiques Blockchain et crypto-monnaies et apporte un cadre juridique nécessaire pour la structuration, le développement de l'écosystème ainsi que la protection des consommateurs. La loi a effectué un effort de définition juridique du *token* et de l'ICO, bien que la qualification juridique du *token* reste une zone grise et fasse peser un risque juridique majeur, tant pour les émetteurs de jetons que pour les acheteurs de ces jetons (ce qui explique l'attrait majeur à date pour les *security tokens*, présentant des avantages de la Blockchain mais avec un arrimage au cadre existant du droit plus aisé). La loi PACTE prévoit également un visa optionnel délivré par l'AMF préalablement à l'ICO avec pour objectif d'accroître la qualité des projets lancés et de limiter les fraudes et levées non solides, nombreuses lors du foisonnement de la fin 2017 et début 2018. Le choix d'une « *flat tax* » à 30 % sur les gains liés aux crypto-monnaies a déçu une grande partie des acteurs de l'écosystème en raison de son caractère dissuasif, mais le dispositif a le mérite de créer un cadre auparavant inexistant et d'apporter sécurité et stabilité juridique et fiscale. À date, un des obstacles majeurs des jeunes pousses françaises reste l'accès à un compte bancaire, très souvent refusé par les banques qui invoquent un risque réglementaire du fait de la difficile traçabilité de l'origine des fonds versés en crypto-monnaies.

---

337. Nathalie Popper, « Venture Capitalists Seek 'Safe Harbor' for Virtual Currencies », 19 avril 2018. Lien : https://www.nytimes.com/2018/04/19/technology/virtual-currency-securities.html
338. Mickael K. Spencer, mai 2018. Lien : https://medium.com/futuresin/security-token-offerings-sto-are-the-new-icos-d697ece5b6f9e.

Il est à noter que les analyses qui suivent sont purement économiques et financières et ne tiennent pas compte du cadre comptable (en construction) traitant des *token* et des ICO. On relevera néanmoins la progression intéressante des travaux en la matière, marquée notamment par la publication du règlement ANC (autorité des normes comptables) n°2018-07 du 10 décembre. De façon synthétique, si l'ICO est analysée comme une dette remboursable, le jeton est comptabilisé en « emprunts et dettes assimilées ». Si elle induit une obligation de fournir des services ou des biens non encore livrés, les jetons seront comptabilisés en produits constatés d'avance.

CONCLUSION : QUELLES PROSPECTIVES ?

Dans sa forme la plus innovante, la Blockchain est une technologie rendant possible la fabrication d'une machine à générer des comportements sur un réseau. Les transactions effectuées sur ce dernier sont enregistrées de façon immuable et traçable, de façon autorégulée. La révolution Blockchain ne se limite pas à une mutation technologique profonde mais questionne notre système de valeurs philosophico-politique et incarne un potentiel changement historique de paradigme économique et financier.

Nos convictions sur l'avenir :

a. La Blockchain a un potentiel révolutionnaire et représente une innovation fondamentale, comparable à l'invention de la machine à vapeur, de l'imprimerie ou d'Internet. Sa valeur économique et ses valeurs philosophico-politiques sont majeures. Elle s'inscrit à la fois dans la continuité de l'Histoire et en rupture avec elle, par la valeur de décentralisation qu'elle incarne. La Blockchain est d'une certaine manière ce qu'Internet aurait dû être. Jacques Attali voyait, en 1997, dans le 7e continent Internet : « un gigantesque commerce entre les agents virtuels d'une économie de marché pure et parfaite sans intermédiaire, sans impôt, sans État [qui deviendrait] un lieu indemne de nos carences, un paradis du libre-échange[339] ». Si Internet s'est effectivement imposé massivement comme il l'avait prédit, « l'Eldorado » sans friction et sans intermédiaire n'est pas advenu, en témoignent les GAFA, géants du *Web*, incontournables mais loin d'être irréprochables. La Blockchain est l'Internet des valeurs et répond pour la première fois, grâce au Bitcoin, à la contrainte des dépenses doubles. On peut, grâce à une Blockchain, transférer un crypto-actif (actif digital constituant l'unité de compte de la Blockchain, valeur attachée au réseau créé) de pair-à-pair grâce à un code informatique, sans intervention d'un tiers centralisé. Cette possibilité paraît dérisoire, mais peut révolutionner notre manière de commercer, notre rapport à la confiance, la structure de l'économie et être déclinée dans des formes d'applications et cas d'usages.

b. Globalement, la diffusion de la technologie va non seulement se poursuivre mais s'intensifier. La principale erreur de ses détracteurs est de juger l'avenir sur les bases du présent. Nous croyons à la complémentarité des technologies. Siècle de la donnée établie comme le nouvel or noir, ce XXIe siècle sera fait par une combinaison de l'intelligence artificielle (effectuer des prédictions), de l'Internet des objets (connecter les mondes physique et digital) et de la Blockchain (sécuriser les valeurs

339. Article de Jacques Attali, 1997. Lien : blogs.lexpress.fr/attali/2017/10/23/blockchain-catalogne-et-autres-sujets-dimportance/

digitales et leurs échanges). Nous anticipons deux points de bascule : l'acceptation par des grands distributeurs de crypto-actifs (il ne serait d'ailleurs pas très surprenant qu'Amazon crée sa crypto-monnaie) et le déploiement à grande échelle d'applications concrètes, basées sur la Blockchain, mais transparentes pour le consommateur. Le système reste trop complexe et l'expérience trop peu séduisante. Personne ne connaît le fonctionnement du protocole TCP/IP : pour envoyer un e-mail, il suffit de cliquer sur « Envoyer ». Le progrès technique va se poursuivre et contribuer au développement de la Blockchain tout en catalysant son évolution. L'ordinateur quantique et sa puissance de calcul immense pourraient par exemple constituer un tournant majeur.

c. Les débats entre centralisation et décentralisation sont cristallisés dans les discussions sur la Blockchain. Si les cas de Blockchains privées sont intéressants, concrets et peuvent être économiquement viables, leur potentiel révolutionnaire peut paraître moindre (elles adressent en effet majoritairement des sujets d'optimisation de coûts et d'infrastructures IT). Peut-être, mais il est aussi temps de cesser cette compétition puérile autour de degrés autoproclamés de disruption. À chaque situation son besoin, nous prônons le dépassement de l'opposition centralisation *vs* décentralisation.

d. En effet, nous considérons le besoin de décentralisation important et croissant (affaire Cambridge Analytica/Facebook, monopoles…), mais de façon très différenciée en fonction des secteurs et des situations. Plus que la fin des tiers de confiance annoncée à l'emporte-pièce, nous prévoyons une restructuration des chaînes de valeur et un rebrassage des cartes au profit de la simplicité et de la transparence. Cette vague se traduira certes par la destruction de certains types d'intermédiaires, mais au profit de nouvelles formes de tiers et de modèles plus ou moins décentralisés. De manière générale, il faut cesser d'opposer ancienne et nouvelle économie, ou pouvoir centralisé et décentralisé. Les forces à l'œuvre sont bien plus subtiles et la coopération devrait être une fois de plus le pari gagnant. Quoi qu'il en soit, la pression pour plus de transparence et d'horizontalité ne cessera de croître. Le comportement stratégique des GAFA et BATX sur les sujets Blockchain est à suivre de près.

e. D'un point de vue stratégique, le potentiel de la Blockchain va continuer à se traduire par une course à la valeur entre acteurs traditionnels et start-up, à l'image d'une ruée vers l'or digital, marquée par l'irruption de centaines de projets. Nous devrions par conséquent assister à trois phénomènes :

- un mouvement de consolidation, du secteur traditionnel vers les nouveaux acteurs ;
- un mouvement de consolidation entre les nouveaux acteurs pour réaliser des gains d'échelle ;
- un processus de sélection naturelle va s'opérer, de nombreux projets ne survivront pas.

f. Sur le plan monétaire, il est peu probable que nous assistions à un remplacement généralisé et absolu des monnaies de banques centrales par le bitcoin (ou autres). Nous devrions plutôt constater une coexistence entre quelques crypto-actifs privés et les monnaies étatiques. Dans les pays développés, l'usage monétaire restera encore longtemps poussé par la spéculation, la *hype* et le *FOMO*. La première raison ? Les cas d'usage transactionnels concrets et performants sont encore en cours de stabilisation mais restent un des segments les plus prometteurs, notamment avec le développement en cours du *lightning network* sur lequel reposent de nombreux espoirs de la communauté. Surtout, l'euro et le dollar restent des monnaies qui rendent plutôt bien leur service. Les banques centrales qui les gèrent ne sont pas exemptes de critiques et on peut avoir des réserves sur les effets néfastes des gonflements des bases monétaires après 2008. Mais l'euro et le dollar restent parfaitement utilisables dans la vie de tous les jours. Seule une crise monétaire qui, par exemple, ferait craindre l'éclatement de la zone euro, pourrait générer des conversions massives de monnaies légales en crypto-actifs. À court terme, les crypto-actifs vont donc rester cantonnés à l'écosystème et au service de transactions confidentielles, donc parfois illégales. Dans les pays en développement, on peut s'attendre à une croissance plus rapide des usages, du fait des problématiques que connaissent les populations (déficit d'infrastructures, inflation, contrôle des changes, bancarisation faible mais développement technologique rapide).

g. L'économie va connaître d'ici cinq à dix ans une vague de tokenisation massive au service de l'efficacité, du recul des asymétries d'information, des alignements d'intérêts et de l'économie de bien commun 2.0. Nous anticipons le futur comme une somme de services, de biens (et d'humains ?) tous connectés à une ou plusieurs Blockchains, circulant – en tant que crypto-actifs – comme des wagons sur des rails. Dans un premier temps, les biens digitaux immatériels, dont l'ensemble des actifs financiers, seront tous associés à un *token*, suivis des actifs physiques (le passage du monde réel à la Blockchain est plus complexe). La Blockchain va progressivement devenir l'infrastructure généralisée de toutes les banques et remplacer toutes les structures existantes. Les contours entre propriété et usage vont

par ailleurs être rebattus, dans la continuité de la croissance de l'économie collaborative. La tokenisation conduira à la propriété partagée et à la liquidité d'un plus grand nombre d'actifs.

h. La régulation va se structurer, avec une première tentation des forces publiques à interdire, ou du moins limiter, l'émergence des monnaies concurrentes privées, à grande échelle, pour préserver leur souveraineté. Définir la régulation opportune n'est pas simple et l'interdiction, même si elle était prononcée, serait très difficilement applicable dans un contexte décentralisé[340]. Mais le sujet est global et dépasse largement la question monétaire. Les États pourraient en fait être beaucoup plus cléments qu'initialement attendu. La position progressiste de la France, avec notamment la loi PACTE en est un bon exemple. L'invention libertaire et désétatisée est finalement au cœur d'un chambardement géopolitique mondial. Il est probable à ce titre que les États soient prudents dans leur approche, de peur de voir partir cette manne économique mondiale sous d'autres cieux. Nous assistons également à l'émergence de champions nationaux, portée par les gouvernements. La Blockchain serait-elle la nouvelle conquête de l'espace ? Les États-Unis seront-ils une seconde fois en vingt ans les premiers à planter leur drapeau sur ces nouveaux territoires, comme ils l'avaient fait sur le septième continent ? La France semble en avoir décidé autrement, et c'est tant mieux, en prônant une position exemplairement mesurée, sérieuse et positive à l'égard du sujet. L'incertitude réglementaire reste toutefois à ce jour le principal facteur de risque, notamment pour les entrepreneurs souhaitant réaliser des ICO. À propos de ces dernières, la régulation va se durcir pour protéger les investisseurs. La coopération de l'écosystème avec les régulateurs est à la fois une nécessité pour le bien commun et l'unique voie de succès pour les entrepreneurs.

i. Les périodes de destruction créatrice ne sont pas toujours propices à l'évaluation rationnelle de la valeur des actifs et il est peu probable que ces nouveaux actifs fassent exception. De nombreux observateurs anticipent l'éclatement de ce qu'ils considèrent comme une bulle. Mais un tel constat ne remet pas en cause l'intérêt des crypto-actifs et de la Blockchain. L'éclatement de la bulle Internet au début des années 2000 n'a pas empêché le monde connecté contemporain. De même, la faillite de John Law n'a empêché personne de détenir des

340. De fait, il empêcherait ces monnaies dématérialisées d'acquérir la liquidité qui leur permettrait de devenir des monnaies à part entière. Parmi les plus grandes économies, c'est en Chine que ce « risque réglementaire » semble le plus développé, dans la mesure où le *renminbi* est volontairement sous-évalué par les autorités monétaires chinoises. La puissance publique chinoise oblige donc les Chinois à utiliser une monnaie dont le pouvoir d'achat est artificiellement dévalué.

billets de banque aujourd'hui. Les cours des crypto-actifs sont largement manipulés et ce, du fait d'exactions d'une minorité qui ne respecte pas les valeurs de la Blockchain. Le manque de transparence de ce marché financier, certes jeune, est un paradoxe évident, jurant avec les valeurs d'horizontalité et d'asymétrie d'information réduite de la technologie. Ce marché doit rapidement être régulé de manière adéquate pour lui permettre de réaliser son potentiel.

j. Pour autant (et on rira peut-être de nous dans cinq ans), nous pensons que si la capitalisation totale est très mesurée par rapport au potentiel long terme, s'il est probable que nous ne connaissions pas le nom du projet qui remportera la mise, nous considérons, contrairement à de nombreux observateurs, que le Bitcoin est différent. Il constitue à la fois la première Blockchain et la plus marquée sur le plan identitaire, l'érigeant en véritable totem. Il a démontré sa sécurité, et les projets en cours, comme le *lightning network*, sont prometteurs pour accroître la scalabilité et adapter le niveau de sécurité à la criticité de l'opération. Le cours du bitcoin devrait donc continuer à croître, mais de façon plus linéaire sur le temps long.

k. Toujours sur le terrain financier, nous sommes en ligne avec plusieurs acteurs comme Chris Burniske : la valeur devrait être accaparée par les sous-couches (Blockchain comme Bitcoin, Ethereum, NEO…), bien davantage que par les applications bâties sur ces Blockchains. Rappelons que, dans le cas d'Internet, les infrastructures ont été rapidement transformées en commodité. Les *token utilities* sont néanmoins les plus nombreux aujourd'hui, ce qui ne sera pas nécessairement toujours le cas dans le futur. La réglementation jouera un rôle majeur dans l'évolution du marché : les *security tokens*, émis dans le cadre de *security token offerings*, sont fréquemment cités comme une étape clé, car plus facilement arrimable au droit positif.

l. L'arrivée massive de capitaux de fonds d'investissement et institutionnels n'est qu'une question de temps et devrait progresser à mesure que la maturité de l'agencement entre *token economics* et financement classique augmentera, en parallèle d'un cadre réglementaire et comptable de plus en plus abouti. Là encore, les *security tokens* seront une étape, de même qu'un futur ETF Bitcoin s'il est accepté par les régulateurs !

m. Dans le sillage de quelques grandes universités mondiales, le champ académique va s'approprier progressivement ces réflexions et les alimenter ; il reste tant à penser et construire. La *crypto-economics* va s'imposer comme nouvelle discipline majeure enseignée dans les

meilleures universités, de même que la philosophie appliquée à la Blockchain, la finance (évaluation notamment) et, bien sûr, le droit.

Nous sommes convaincus que le train de la Blockchain sera la « locomotive du XXIe siècle », pour reprendre l'expression de Jacques Attali sur Internet en 1997. Lucidité et humilité doivent rester de mise, au service de l'innovation et de la création, fidèles aux valeurs des pionniers. Nous ne sommes qu'au début. Vitalik Buterin, le fondateur d'Ethereum, appelait d'ailleurs à l'humilité dans un tweet au début d'année 2018 : « La capitalisation totale des *crypto-assets* a atteint 500 milliards de dollars aujourd'hui : l'avons-nous mérité ? [...] Combien de non-bancarisés avons-nous bancarisé ? Combien de Vénézuéliens avons-nous protégé de l'hyperinflation ? [...] La plupart des réponses à ces questions n'est bien sûr pas zéro et, dans certains cas, les résultats sont significatifs. Mais ce n'est pas assez pour justifier 500 milliards d'euros de capitalisation[341]. »

Jusqu'où iront le Bitcoin et la Blockchain ? Visiblement, au moins jusque dans l'espace. Jeff Garzik a récemment annoncé son souhait d'envoyer dans l'espace des petits cubes satellites[342] qui feraient office de nœuds complets (détenant l'intégralité de l'information de la Blockchain[343]) et permettraient de faire subsister la traçabilité passée, quelle que soit la catastrophe survenue sur terre. Science (ou) fiction ?

---

341. « La réponse à toutes ces questions n'est définitivement pas nulle, et dans certains cas, elle est au contraire plutôt significative. Mais pas assez pour justifier une capitalisation de 500 milliards de dollars. Pas assez. », citation de Vitalik Buterin.
342. Cubesate.
343. Lien : www.vernon1.com/le-developpeur-bitcoin-jeff-garzik-veut-mettre-des-noeuds-bitcoin-complets-dans-l-espace/

BIBLIOGRAPHIE

Cette bibliographie n'est pas exhaustive, l'ensemble des sources utilisées est détaillé en note de bas de page au fil de l'ouvrage.

HISTOIRE (PARTIE A)

- Michel AGLIETTA, *La Monnaie. Entre dettes et souverainetés*, Odile Jacob, 2016.
- Jacques ATTALI, *Une brève histoire de l'avenir*, Fayard, 2006.
- Jean-Luc BAILLY, *Économie monétaire et financière*, Bréal, 2000.
- Nicolas BOUZOU, *L'innovation sauvera le monde, manifeste pour une planète pacifique, prospère et durable*, Plon, 2016.
- Luc FERRY, *L'Innovation destructrice*, Plon, 2014.
- Denise FLOUZAT, *Le Concept de banque centrale*, Bulletin de la Banque de France, n° 70, octobre 1999. Lien : https://www.banque-france.fr/sites/default/files/medias/documents/bulletin-de-la-banque-de-france_70_1999-10.pdf
- Jean Fourastié*, La Comptabilité,* « Que sais-je ? », PUF, 1998, 21e éd.
- Yuval Noah HARARI, *Homo Deus, Une brève histoire de l'humanité*, Albin Michel, 2015.
- David GRAEBER, *Dette : 5000 ans d'histoire*, traduction Françoise et Paul CHEMLA, Les Liens qui libèrent, 2013 ou Actes Sud, « Babel », 2016.
- Roland MARX, « Banque, crédit et monnaie en Angleterre de 1640 à la fin du XVIIe siècle », *Revue de la Société d'études anglo-américaines des XVIIe et XVIIIe siècles*, 1980.
- Philippe NEMO, *Qu'est-ce que l'Occident ?*, PUF, 2005.
- Philippe RODRIGUEZ, *La Révolution Blockchain*, Dunod, 2017.

PHILOSOPHIE (PARTIE B)

- ARISTOTE, Éthique à *Nicomaque*, traduction de Richard Bodeüs, Paris, GF, 2004.
- Ernest ARMAND, *Initiation individualiste anarchiste*, La Lenteur-Le Ravin bleu, 2015, *in* Alain Laurent, *L'Autre Individualisme, une anthologie*, Les Belles Lettres, 2016.
- Pierre BOUTANG, *Ontologie du secret*, PUF, Quadrige, 1998.
- Primavera DE FILIPPI, « La fin de l'idéal *trustless* ». Lien : https://Blockchainfrance.net/2016/07/20/la-fin-de-lideal-trustless/
- Lawrence LESSIG, « Code is Law. On Liberty in Cyberspace », *Harvard Magazine*, 2000. Lien : https://harvardmagazine.com/2000/01/code-is-law-html
- Primavera DE FILIPPI, Danièle BOURCIER, « Réseaux et gouvernance. Le cas des architectures distribuées sur Internet », *Pensée plurielle*, 2014/2 (n° 36). DOI : 10.3917/pp.036.0037. Lien : https://www.cairn.info/revue-pensee-plurielle-2014-2-page-37.htm
- Byung-Chul HAN, *La Société de transparence*, PUF, 2017.
- Friedrich NIETZSCHE, *Aurore. Pensées sur les préjugés moraux*, traduction d'Éric Blondel, GF, 2012.
- Olivier REY, *Quand le monde s'est fait nombre*, Stock, 2016.
- Murray ROTHBARD, *L'Éthique de la liberté*, traduction de François Guillaumat, Les Belles Lettres, 1991.

TECHNOLOGIE (PARTIE C)

- Andreas ANTONOPOULOS, *Mastering Bitcoin*, O'Reilly, 2016.
- Vitalik BUTERIN, *A Next-Generation Smart Contract and Decentralized Application Platform*, 2013.
- Henning DIEDRICH, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, 2016.
- Gideon GREENSPAN, *Blockchains vs centralized databases.* Lien : https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/
- Bertrand HARTMAN, *La Chine, puissance dominante du Bitcoin, crypto-monnaie libertaire*, 12/09/2017. Lien : https://asialyst.com/fr/2017/09/12/chin-puissance-dominante-bitcoin-crypto-monnaie-libertaire/
- Gavin HOOD, Andreas ANTONOPOULOS*, Mastering Ethereum*, 2018. Lien : https://ethereumbook.info/Valentin KALINOV, *How is Blockchain technology similar to torrent technology? How is it different?*. Lien : https://www.quora.com/How-is-blockchain-technology-similar-to-torrent-technology-How-is-it-different
- William MOUGAYAR, *The Business Blockchain*, Wiley, 2016.
- Satoshi NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009.

ÉCONOMIE (PARTIE D)

- A. AGRAWAL, C. CATALINI, A. GOLDFARB, *Some Simple Economics of Crowdfunding, Innovation Policy and the Economy*, University of Chicago Press, 2014.
- Darcy ALLEN, *The Private Governance of Entrepreunership* : an Institutional A*pproach to Entrepreneurial discovery*. Lien : http://researchbank.rmit.edu.au/view/rmit:162196
- K. J. ARROW, G. DEBREU, « Existence of an Equilibrium for a Competitive Economy », *Econometrica: Journal of the Econometric Society*, 1954.
- Dave BABBITT, Joel DIETZ, *Cryptoeconomic Design: a Proposed Agent-Based Modelling Effort* , SwarmFest 2014. Lien : https://www3.nd.edu/~swarm06/SwarmFest2014/Crypto-economicDesignBabbit.pdf
- W. J. BAUMOL, « Contestable Markets: an Uprising in the Theory of Industry Structure », *American Economic Review*, vol. 72, n° 1, 1982.
- R. CASTANIAS, C. HELFAT, « Managerial and Windfall Rents in the Market for Corporate Control », *Journal of Economic Behavior and Organization,* 1992.
- Christian CATALINI (MIT), Joshua S. GANS (université de Toronto), *Some Simple Economics of the Blockchain*, 2016. Lien : http://ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf
- Jeremy CLARK, Andrew MILLER, Joseph BONNEAU, Edward W. FELTEN, Joshua A. KROLL, Arvind NARAYANAN, *On Decentralizing Prediction Markets and Order Books*, 2014. Lien : http://www.econinfosec.org/archive/weis2014/papers/Clark-WEIS2014.pdf
- Sinclair DAVIDSON, Primavera DE FILIPPI, Jason POTTS, *Economics of Blockchain*, 2016.
- Nicolas EBER, *Théorie des jeux*, Dunod, 2013, 3e éd.
- Alexander EVANS, *A Crash Course in Mechanism Design for Cryptoeconomic Applications*, 16 octobre 2017. Lien : https://medium.com/blockchannel/a-crash-course-in-mechanism-design-for-cryptoeconomic-applications-a9f06ab6a976

- Ildar FAZULYANOV, *Blockchain and Nash Equilibrium in Health Care*, oh my!, 18 septembre 2017. Lien : https://medium.com/@ildarfazulyanov/Blockchain-and-nash-equilibrium-in-healthcare-oh-my-1-6ba0e80ea03b
- Frédéric FRÉRY, « Le management 2.0 ou la fin de l'entreprise », *L'Expansion Management Review*, 2010/2, n° 137. Lien : https://www.cairn.info/revue-l-expansion-management-review-2010-2-page-52.htm
- Milton FRIEDMAN, *Capitalisme et Liberté*, traduction d'A. M. Charmo, À contre-courant, 2010.
- Robin HANSON, « Shall we vote on values, but bet on beliefs? », *Economics*, George Mason University, 2007. Lien : http://mason.gmu.edu/~rhanson/futarchy.pdf
- F. HAYEK, *Pour une vraie concurrence des monnaies*, traduction de G. Vuillemey, PUF, 2015.
- Mathew O. JACKSON, *Mechanism Theory*, 2014. Lien : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2542983
- Gregory MANKIW, *Principes de l'économie*, Economica, 1998.
- Pascal SALIN, *La Vérité sur la monnaie*, Odile Jacob, 1990.
- Yonathan SOMPOLINSKY, Aviv ZOHAR, *Bitcoin's underlying incentives,* vol. 15, issue 5 acm queue, Association for computing machinery, 2017. Lien : https://queue.acm.org/detail.cfm?id=3168362
- M. SPENCE, « *Job Market Signaling* », *Quarterly Journal of Economics*, 1973.
- J. STIGLITZ, A. WEISS, « Credit Rationing in Markets with Imperfect Information », *American Economic Review*, 1981.
- Don et Alex TAPSCOTT, *Blockchain Revolution*, Portfolio Penguin, 2016.
- O. WILLIAMSON, « Transaction Costs Economics: the Governance of Contractual Relations », *Journal of Law and Economics,* 1979.

STRATÉGIE ET CAS D'USAGE (PARTIES E ET F)

Principaux médias et sources d'information :

- https://medium.com
- https://Reddit.com
- https://Bitcointalk.com
- https://www.coindesk.com
- https://Blockchainmag.fr
- http://whitepaperdatabase.com
- https://www.ccn.com
- https://cointelegraph.com
- https://www.cryptocompare.com
- https://bitcoinfees.info/
- https://hackernoon.com/
- https://icowatchlist.com
- https://api.blockchain.info/
- https://coinmarketcap.com/
- https://api.blockchain.info/

FINANCE (PARTIE G)

- Chris BURNISKE, Jack TATAR, *Cryptoassets, The Innovation Investor's Guide to Bitcoin and Beyond*, 2017.
- Aswath DAMODORAN, *The Bitcoin Boom: Asset, Currency, Commodity and Collectible*, 24 octobre 2017. Lien : http://aswathdamodaran.blogspot.fr/2017/10/the-bitcoin-boom-asset-currency.html
- Alex EVANS, *On Value, Velocity and Monetary Theory*, janvier 2018. Lien : https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f
- David MAYER, *Cryptocurrencies like Bitcoin are Commodities, Federal Judge says. Here's why that matters*, 7 mars 2018. Lien : http://fortune.com/2018/03/07/bitcoin-cftc-commodities-coin-drop-markets
- Nathalie POPPER, *Venture Capitalists Seek "Safe Harbor" for Virtual Currencies*, 19 avril 2018. Lien : https://www.nytimes.com/2018/04/19/technology/virtual-currency-securities.html
- Tomo UETAKE, Hideyuki SANO, « Interview: Bitcoin a New Asset Class, not a Crypto-currency – CME's Melamed », 7 novembre 2017. Lien : https://www.reuters.com/article/cme-group-bitcoin/interview-bitcoin-a-new-asset-class-not-a-crypto-currency-cmes-melamed-idINKBN1D7159
- Pierre VERNIMMEN, Pascal QUIRY, Yann LE FUR, *Finance d'entreprise*, Dalloz, 2018

INDEX

D

E

F

G

O

P

R

S

T

U

V

W

Z