Désintermédiation des données critiques et décentralisation des organisations. Le cas de la blockchain.

Auteur : Delva, Jean
Promoteur(s) : Hermans, Michel
Faculté : HEC-Ecole de gestion de l'Université de Liège
Diplôme : Master en sciences de gestion (Horaire décalé)
Année académique : 2016-2017
URI/URL : http://hdl.handle.net/2268.2/4288

Désintermédiation des données critiques et décentralisation des organisations.

Le cas de la blockchain.

Promoteur

HERMANS Michel

Lecteurs

ERNST Damien

SCHMITZ Stephan

Travail de fin d'études présenté par **Jean DELVA** en vue de l'obtention du diplôme de Master en Sciences de Gestion.

Année Académique 2016/21017

Table des matières

I Introduction

Les tendances économiques actuelles sont celles de Big Data, de l'Internet des Objets, des logiques de réseau, de l'ubérisation de l'économie, des plateformes web ou encore des mouvements collaboratifs.

Le thème qui apparaît comme récurrent dans ces notions et que plus aucune entreprise ne peut contourner ce sont les données et la gestion que l'on fait de celles-ci !

C'est dans ce sens que les business modèles changent. La transformation digitale qui est conduite, entre autres, par le Big Data et une compétition accrue, amène les entreprises à optimiser leurs processus mais aussi les pousse à créer de nouveaux business modèles. Grâce aux appareils constamment connectés de l'Internet of Things (IoT)[1], ces entreprises bénéficient de deux principaux avantages : premièrement elles ont la possibilité de collecter des informations toujours plus pertinentes et de manière automatisée sur l'utilisation et les habitudes de leurs clients ou le statut de performance d'un outil de production ; deuxièmement, ces données entrantes qui sont analysées chaque seconde peuvent ouvrir la voie à de nouvelles activités et générer de la croissance.

C'est ainsi que la compétition n'a plus vraiment lieu entre « grands » et « petits » mais plutôt entre « rapides » et « lents ». Avec l'avantage pour celui qui gèrera au mieux le changement !

Grâce à ces nouveaux outils les entreprises peuvent aller jusqu'à faire des analyses prédictives sur base des données disponibles. Pour la gestion de ces données les acteurs doivent souvent faire appel à un tiers.

Avec l'essor des médias sociaux qui occupent dans la vie des « connectés » une place prépondérante, le partage et la divulgation de données parfois très personnelles sont amenés à un stade avancé. Le mot réseau est devenu un terme en vogue, mais plus que cela c'est une stratégie à part entière.

Collatéralement, des stratégies novatrices basées sur ce réseau et les relations de pair-à-pair voient le jour. Des plateformes telles que AirBnB, BlaBla Car ou encore Uber révolutionnent la manière de faire

[1] Internet des Objets

des affaires. Cependant, le risque du tiers qui possède nos données persiste. A l'heure actuelle, le besoin d'un tiers de confiance est inévitable.

Le problème avec ce partage de données c'est qu'une fois mises en ligne, elles échappent à son propriétaire, particulier ou professionnel.

Alors, comment redonner la pleine maîtrise aux propriétaires de leurs données ? D'autre part, comment réduire les frictions dans l'accès, l'échange, le partage de ces données entre états, entreprises ou au sein d'une même organisation ? Comment réduire les contraintes des silos d'information en entreprise ?

Des cas récents de brèches informatiques et hacking de données – je pense localement aux entreprises Saint-Gobain[2] ou TNT[3] - m'ont motivé dans ma volonté de trouver une solution fiable pour gérer les données critiques, les sécuriser et les rendre inaltérables.

Ce que je souhaite aborder dans ce travail, c'est la manière dont la décentralisation et la désintermédiation peuvent aider les entreprises à mieux maitriser leurs données et aussi améliorer les processus. Cela dans le but d'accroitre la rentabilité de leurs structures. Dans ce cadre, nous mettrons en évidence l'utilisation de la blockchain …

Questions de recherche : Quelles opportunités pour la blockchain dans le monde de l'entreprise ? Et, quelles implications éthico-juridiques pour cette application ?

Dans un premier temps nous définirons certaines notions clés. Ensuite nous aborderons le fonctionnement d'une crypto-monnaie et plus précisément le Bitcoin - en tant que standard au sein des multiples devises digitales disponibles. Nous présenterons ce qui nous intéresse réellement au-delà des crypto-monnaies, l'infrastructure sous-jacente : la blockchain. Puis, nous détaillerons les différentes applications de cette technologie. Finalement nous analyserons les aspects juridiques et éthiques de l'utilisation des crypto-monnaies et de la technologie blockchain, avant de conclure.

[2] URL : http://www.lefigaro.fr/secteur/high-tech/2017/06/27/32001-20170627ARTFIG00256-de-grandes-entreprises-dont-saint-gobain-en-france-victimes-d-une-importante-cyberattaque.php
[3] URL : http://www.lavenir.net/cnt/dmf20170628_01024458/le-trafic-tnt-totalement-paralyse-par-la-cyberattaque

II Définitions & Concepts clés

Afin de comprendre clairement les concepts, la terminologie et les processus évoqués dans ce travail, il me semble opportun de débuter en abordant quelques définitions et concepts clés. Séparément mais aussi en les reliant afin de naviguer dans le milieu blockchain.

De plus, ces définitions me semblent correspondre à un besoin fondamental pour comprendre le monde digital qui nous entoure et ses paramètres essentiels qui établissent les tendances actuelles. Nous aborderons dans un premier temps le fonctionnement d'une monnaie centrale afin de mieux cerner et mettre en évidence les propriétés distribuées et décentralisées du Bitcoin et de la technologie blockchain sous-jacente.

Comment fonctionne une monnaie centrale ?

Une monnaie traditionnelle est créée et gérée par une institution monétaire centralisée : la banque centrale. Cette banque émet, régule, valorise cette monnaie par diverses actions. Sachons que lorsqu'on désigne cette monnaie, nous parlons bien de monnaie fiduciaire qui se constitue de billets et de pièces et des avoirs de banques de second rang. Elle est utilisée lors d'échanges commerciaux par des individus ou entités d'un même Etat ou d'une communauté supranationale. Elle peut aussi être utilisée lors d'échanges dépassant ces frontières. Environ 90% de la monnaie en circulation est scripturale, c'est à dire un jeu d'écritures comptables concentré dans une base de données centralisée d'une banque (paiements par carte bancaires, virements). Lorsque qu'une banque commerciale éprouve des besoins de financement elle se dirige vers une autre banque commerciale en excédent de liquidités qui va lui prêter les ressources nécessaires. La banque recevant ces fonds va en garder une partie en réserve (devoir légal) et prêter à son tour des fonds à une autre institution demandeuse de financement. C'est ce schéma qui permet de créer de la monnaie scripturale à l'infini. Lorsqu'une banque ne trouve pas de contrepartie, elle se tourne vers la banque centrale. Une autre manière de créer de la monnaie est l'émission de dette souveraine ou l'achat de titres sur les marchés financiers.

Système de pair-à-pair : (peer-to-peer, P2P) Ce modèle d'échange de ressources permet un échange direct de données entre différents utilisateurs d'un réseau connectés à Internet. Ce système représente une alternative au modèle client/serveur. Dans ces échanges, les pairs, aussi appelés nœuds, peuvent

soit fournir (serveur), soit demander (client) des ressources. Ce modèle permet de s'affranchir du besoin d'un serveur central.

Il me semble qu'il existe à l'heure actuelle une propension importante à confondre pair-à-pair et partage illégal de données ! Comprenons que nous parlons de la technologie pair-à-pair en tant que telle et donc par définition que cette technologie est neutre.

La force de calcul distribuée : cette notion invoque le besoin de répartir la puissance de calcul pour un projet en petites entités de calcul distinctes appelées « unités de travail » via différents ordinateurs reliés entre eux par un réseau de communication. Le but est d'utiliser les ressources réparties de plusieurs centaines, milliers d'ordinateurs afin de faire levier pour un unique projet. En mutualisant cette puissance de calcul, il devient possible de créer une machine virtuelle monumentale afin de répondre aux besoins du projet. Il existe certaines exigences dans l'utilisation d'un système distribué :

⇒ *L'extensibilité* : une expansion doit être réalisable si nécessaire

⇒ *L'ouverture* : les composantes d'un tel système (middleware) possèdent des interfaces extensibles et modifiables de manière aisée. Un service web est un exemple de système distribué qui jouit d'une grande ouverture.

⇒ *L'hétérogénéité* : les composantes peuvent être écrites en différents langages informatiques (Java, C++) et s'exécuter sur différents systèmes d'exploitation (Windows, Linux).

⇒ *La tolérance aux pannes* : les systèmes distribués sont moins exposés aux pannes car les composantes ne sont pas centralisées, elles peuvent être répliquées.

Qu'est-ce que la cryptographie ?

Un synonyme à la cryptographie pourrait être : écriture chiffrée. Il s'agit d'un ensemble de techniques visant à chiffrer un texte ou, en informatique, des données. Ceci dans le but d'en assurer leur inviolabilité. Il existe deux types de cryptographie : symétrique et asymétrique.

La cryptographie symétrique est basée sur l'utilisation de clés privées. Les clés nécessaires à l'encodage et au décodage sont confidentielles afin d'augmenter le niveau de sécurité des échanges

Dans le cas de la cryptographie asymétrique, l'utilisateur possède deux clés mathématiques complémentaires : une privée et une publique qu'il peut distribuer.

Clé privée : la clé privée est une clé qui permet à l'utilisateur d'une blockchain d'initier une transaction en signant de manière chiffrée son message mais surtout de déchiffrer un message dont il est le destinataire et qui a été chiffré avec la clé publique correspondante. Cette clé est connue de son unique propriétaire et utilisée par lui seul. La clé privée constitue la moitié confidentielle d'une paire de clés cryptographiques utilisée avec un algorithme de clé publique. Ainsi, tout utilisateur peut envoyer un message crypté à l'aide de la clé publique du destinataire alors que le destinataire pourra le décrypter avec sa clé privée, étant le seul à la connaître.

Clé publique : celle-ci sert d'adresse sur une blockchain. Elle est connue de tous et permet de désigner un destinataire.

Le minage : c'est le fait d'utiliser la puissance de calcul informatique permettant de traiter des transactions, de sécuriser un réseau et rendre tous les utilisateurs du système synchronisés. Toute personne qui connecte sur ce réseau une (ou plusieurs) machine(s) équipée(s) pour effectuer du minage est appelée un mineur. Chaque mineur est rémunéré en fonction de la puissance de calcul qu'il apporte au réseau. On les nomme ainsi en référence aux chercheurs d'or qui augmentaient la masse monétaire au fil de leurs découvertes pendant l'Eldorado.

Nœud : il s'agit d'un ordinateur relié au réseau qui utilise un programme permettant de relayer les transactions.

Proof-of-Work : « preuve de travail ». Il s'agit du traitement cryptographique qui permet de valider les transactions. Ce traitement demande un certain temps de calcul, nous parlons d'environ dix minutes pour cette validation.

Proof-of-Stake : « Le proof of stake est une méthode utilisée pour atteindre le consensus distribué dans un réseau blockchain. A l'inverse du Proof of work, le Proof of stake ne demande pas aux utilisateurs d'utiliser leur puissance de calcul, mais plutôt de prouver la propriété d'un certain montant de crypto-monnaie. Ainsi par exemple s'il y a 10 millions d'Ethers en circulation et que j'en détiens 1 million, j'ai 1 chance sur 10 de valider le prochain bloc de la chaîne. Cependant afin d'éviter que la

concentration de capital ne permette de valider plusieurs blocs à la suite, si je suis désigné "validateur" du prochain bloc, je ne peux pas participer aux prochains "tirages au sort" pendant un certain temps. »[4]

Token : ce terme désigne un jeton d'authentification ou jeton cryptographique. Il permet de prouver une identité électroniquement afin de garantir l'accès ou le stockage d'informations chiffrées. Un token matériel peut prendre la forme d'une petite calculatrice qui génère des réponses chiffrées en fonction d'un algorithme précis. Ils sont utilisés pour des système nécessitant une grande sécurité.

Ces différentes notions dessinent les premiers traits des liens qui vont s'établir dans ce travail. Nous tenterons de montrer comment ces tendances de partage de pair-à-pair, cette force de calcul distribuée et de cryptage des données nous aideront à réduire les risques d'hacking ou de brèches informatiques mais aussi comment grâce à cela nous pourrons nous passer des habituels tiers de confiance qui rendent périlleuse la gestion des données critiques.

III Comment fonctionne une crypto-monnaie ?

Une crypto-monnaie est une « devise digitale ». Une monnaie virtuelle. Elle permet de vendre ou acheter des biens et/ou services sur Internet. Une crypto-monnaie telle le Bitcoin nécessite différentes composantes :

⇒ Des développeurs de programmes
⇒ Un service de traitement des transactions
⇒ Des fournisseurs de portefeuilles électroniques
⇒ Des mineurs
⇒ Des échanges
⇒ Et des utilisateurs

Du point de vue de l'utilisateur, les éléments clés lors d'une transaction de crypto-monnaie sont :

1. Un programme de portefeuille électronique : il est installé sur son propre ordinateur et permet de stocker et gérer les données, en l'occurrence les Bitcoins.

[4] URL : https://blockchainfrance.net/le-lexique-de-la-blockchain/

2. Une adresse (clé publique) : là où les tiers peuvent envoyer les informations à échanger.
   Et, une clé privée : celle-ci permet l'envoi sécurisé via un secret cryptographique de données vers un tiers.

Il y a nul besoin de s'enregistrer ou de créer un compte centralisé pour permettre ces échanges. Le portefeuille virtuel peut aussi enregistrer une copie de la blockchain – le registre qui contient toutes les transactions – puisqu'il fait partie de ce schéma décentralisé dans lequel se vérifient les transactions.

L'un des principaux avantages de la technologie blockchain est qu'il s'agit d'une *Technologie Push* : l'utilisateur initie et transmet ses données personnelles au réseau dans le cadre d'une transaction. A l'inverse d'une *Technologie Pull* pour laquelle, à l'image d'une banque ou d'une carte de crédit, les données personnelles sont préenregistrées et « soutirées » au tiers dès qu'une transaction est autorisée par l'utilisateur.

La Technologie Pull requiert des bases de données centralisées contenant les informations privées des clients, qui ne sont pas nécessairement sécurisées pour un usage sur Internet. Elles sont malheureusement vulnérables et susceptibles de connaître des brèches informatiques ! Par contre, réaliser un achat avec des Bitcoins signifie qu'il n'y a pas besoin de confier ses données personnelles à un tiers de confiance, enregistrées dans des systèmes centralisés. Cela peut, par contre, aussi permettre des usages non souhaités.

Au vu de la place critique qu'occupent les données dans le monde des entreprises, il me semblait opportun de chercher et étudier un moyen de les sécuriser. Comment rendre ces informations sécurisées ? C'est à dire :

1. Confidentielles
2. Intègres
3. Disponibles

Comment les rendre infalsifiables et immuables ? Un élément de réponse se trouve dans le protocole utilisé par le Bitcoin…

IV Qu'est-ce que le Bitcoin ?

4.1 Le bitcoin

Bitcoin est une monnaie électronique. Il s'agit d'une devise digitale et d'un système de paiement en ligne dont les techniques cryptographiques sont utilisées pour réguler la création d'unités de monnaie et vérifier le transfert de fonds de manière indépendante, sans le besoin d'une banque centrale.

Une des innovations fondamentales du Bitcoin est qu'il se base sur des échanges de pair-à-pair, un réseau d'utilisateurs reliés entre eux par des nœuds. Les échanges s'effectuent directement entre les utilisateurs sans nécessiter l'intervention d'un tiers pour les réguler. C'est une « monnaie décentralisée ». Une autre avancée majeure réside dans le fait que les transactions sont chiffrées grâce à la cryptographie asymétrique. Les signatures des transactions Bitcoin découlent toutes de la clé publique ECDSA[5]. Un algorithme des plus sûrs actuellement.

Le terme Bitcoin avec un B majuscule fait référence à la monnaie digitale utilisant cette cryptographie. Par contre, le bitcoin avec un b minuscule nous réfère au protocole décrivant le fonctionnement du réseau sur lequel cette monnaie circule.

Le protocole qui permet l'utilisation des Bitcoins, c'est la blockchain. Elle permet la création monétaire et la validation des échanges qui sont faits horizontalement et de manière totalement transparente. Ce système n'a nul besoin d'autorité centrale ni de tiers de confiance pour être géré à l'inverse des monnaies distribuées et contrôlées par des banques, banques centrales ou autres gouvernements.

[5] Elliptic Curve Digital Signature Algorithm (**ECDSA**) est un algorithme de signature numérique à clé publique. Il fait appel à la cryptographie sur les courbes elliptiques.

L'histoire du Bitcoin débute en 2009. Cette monnaie a été lancée le 9 janvier 2009 par une personne ou entité inconnue qui utilise le pseudonyme de Satoshi Nakamoto. Ce dernier est par voie de conséquence aussi l'inventeur de la blockchain – infrastructure virtuelle sur laquelle repose le Bitcoin. C'est sous ce pseudonymes que le « whitepaper » à l'origine de ce qu'il qualifiait de « Peer-to-Peer Electronic Cash System »[1] a été édité. Dans ce document, on peut lire de manière compréhensible les composantes du concept et les détails opérationnels qui sont utilisés.

L'histoire du Bitcoin, bien que récente, a été mouvementée depuis ses débuts. La réelle première transaction a eu lieu en mai 2010 : 2 pizzas contre 10.000 BTC – au cours actuel cela représenterait 39.830.000 EUR !). Au vu de la rapide évolution du cours de cette crypto-monnaie, on pourrait croire à une très forte volatilité, qui remettrait en cause sa fiabilité. Néanmoins, début 2011, le bitcoin rejoint le dollar en terme de capitalisation boursière pour atteindre plusieurs millions de dollars de capitalisation. Actuellement, cette valorisation atteint des sommets :

Graphique 1 – Capitalisation boursière du Bitcoin depuis sa création[6]

C'est à ce moment que les premiers articles sur le Bitcoin commencent à apparaître aux Etats-Unis dans des journaux dédicacés. Après deux périodes de bulles en 2011 et 2013, le cours du Bitcoin connaît une tendance haussière continue.

[6] URL : https://blockchain.info/fr/charts/market-price?timespan=2years

En effet, l'intérêt pour le Bitcoin et la blockchain n'est apparu que très récemment (2015).

Bitcoin est la plus grande et surtout la première crypto-monnaie décentralisée. Son cours au 31.08.2017:

RÉCAPITULATIF DU MARCHÉ

Prix du marché	$4,792.34	Voir le graphique
Volume de transactions	$326,188,064.73	
Volume de transactions	68,064.39000000 BTC	

Printscreen 1 : Récapitulatif du marché Bitcoin au 11.10.2017[7]

4.2 Les autres crypto-monnaies

Il existe de nombreuses autres « altcoins » (alternative coins), c'est à dire crypto-monnaies alternatives, dont le code source est différent de celui du Bitcoin. Il existe plus de six cents crypto-monnaies alternatives, je vais vous présenter celles qui ont une capitalisation boursière significative, une singularité ou un potentiel dans l'usage :

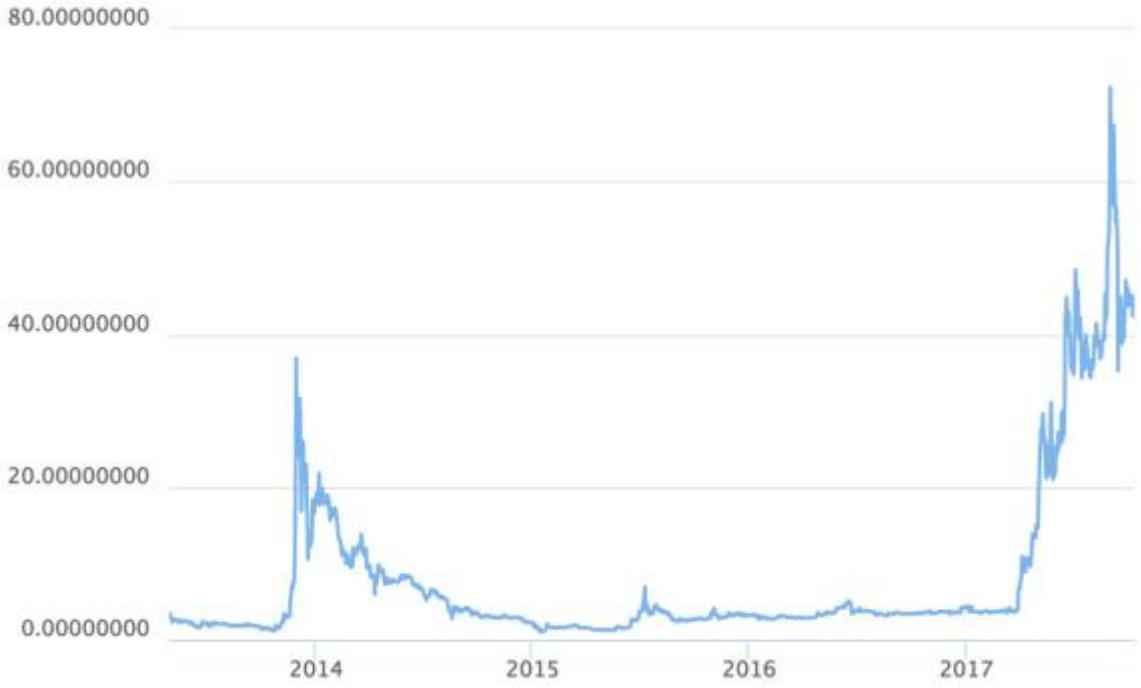
Le LiteCoin (LTC)

Il s'agit d'une monnaie alternative dont le code est à la base le même que celui du Bitcoin mais il a été amélioré pour proposer quelques avantages. Le principal étant que les blocs sont minés à intervalles plus rapides.

« Litecoin est une devise Internet peer-to-peer, qui permet des paiements instantanés, avec des coûts proches de zéro à quiconque dans le monde. Litecoin est un réseau de

[7] URL : https://blockchain.info/stats

paiement mondial open source, qui est entièrement décentralisé sans autorité centrale. Les utilisateurs peuvent maintenant contrôler leurs propres finances, sécurisées par un système basé entièrement sur des mathématiques. Par rapport à Bitcoin, les transactions Litecoin sont plus rapides à confirmer et ont une efficacité de stockage accrue. De par son utilisation par l'industrie, par son volume d'échanges et de liquidité sur les marchés, Litecoin est un moyen de commerce complémentaire à Bitcoin, qui a fait ses preuves. »[8]



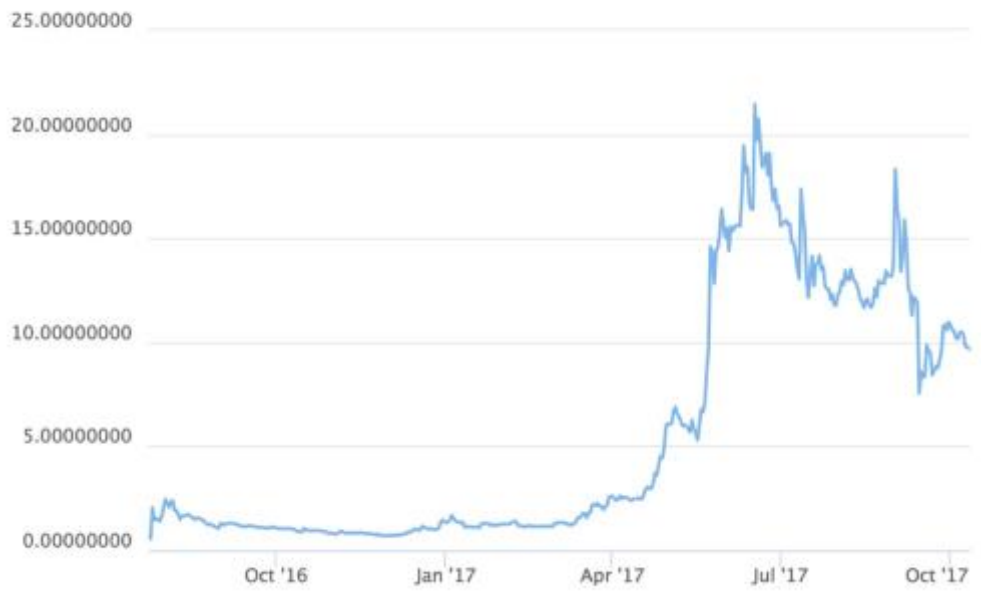
Graphique 2 : Evolution du cours LTC/EUR au 11.10.2017[9]

[8] URL : https://litecoin.org/fr/
[9] URL : https://www.coingecko.com/fr/graphiques_cours/ethereum-classic/eur

L'Ether (ETC)

Il s'agit de l'un des plus sérieux challengers du Bitcoin aujourd'hui en tant que monnaie infrastructure. Son USP (Unique Selling Proposition) vient du fait qu'il permet de faire tourner des programmes appelés « Smart Contracts » sur tous les ordinateurs du réseau simultanément (nous reviendrons sur ces processus dans un prochain chapitre…).

Elle veut permettre aux entreprises de se passer complétement des intermédiaires. Au-delà d'être une nouvelle technologie, la blockchain Ethereum propose une nouvelle forme d'organisation et de gouvernance économique…

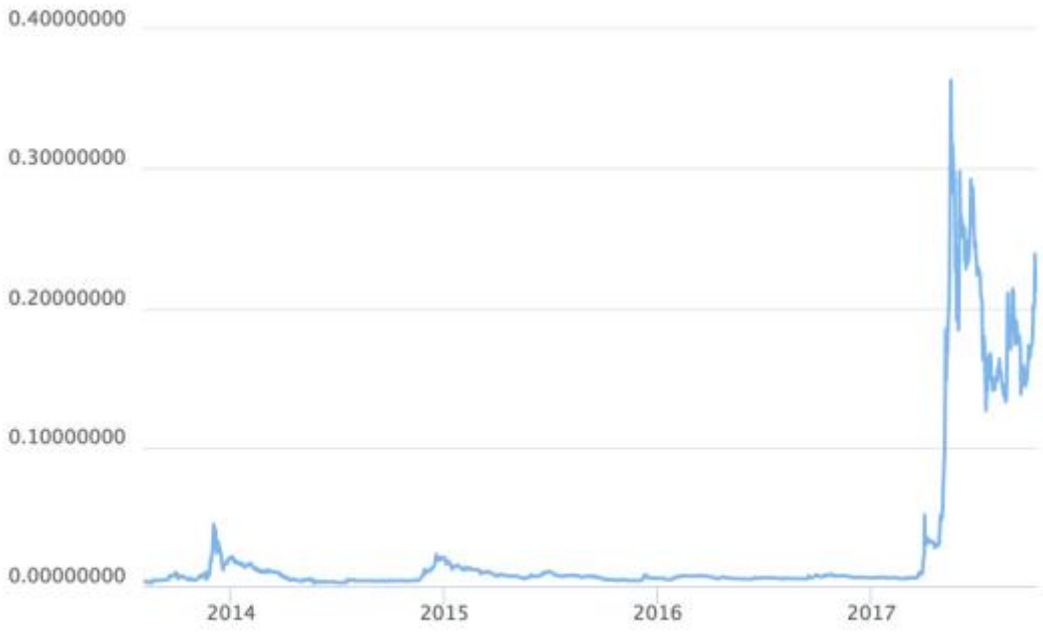


Graphique 3 : Evolution du cours ETC/EUR au 11.10.2017[10]

[10] URL : https://www.coingecko.com/fr/graphiques_cours/ethereum-classic/eur

Ripple (XRP)

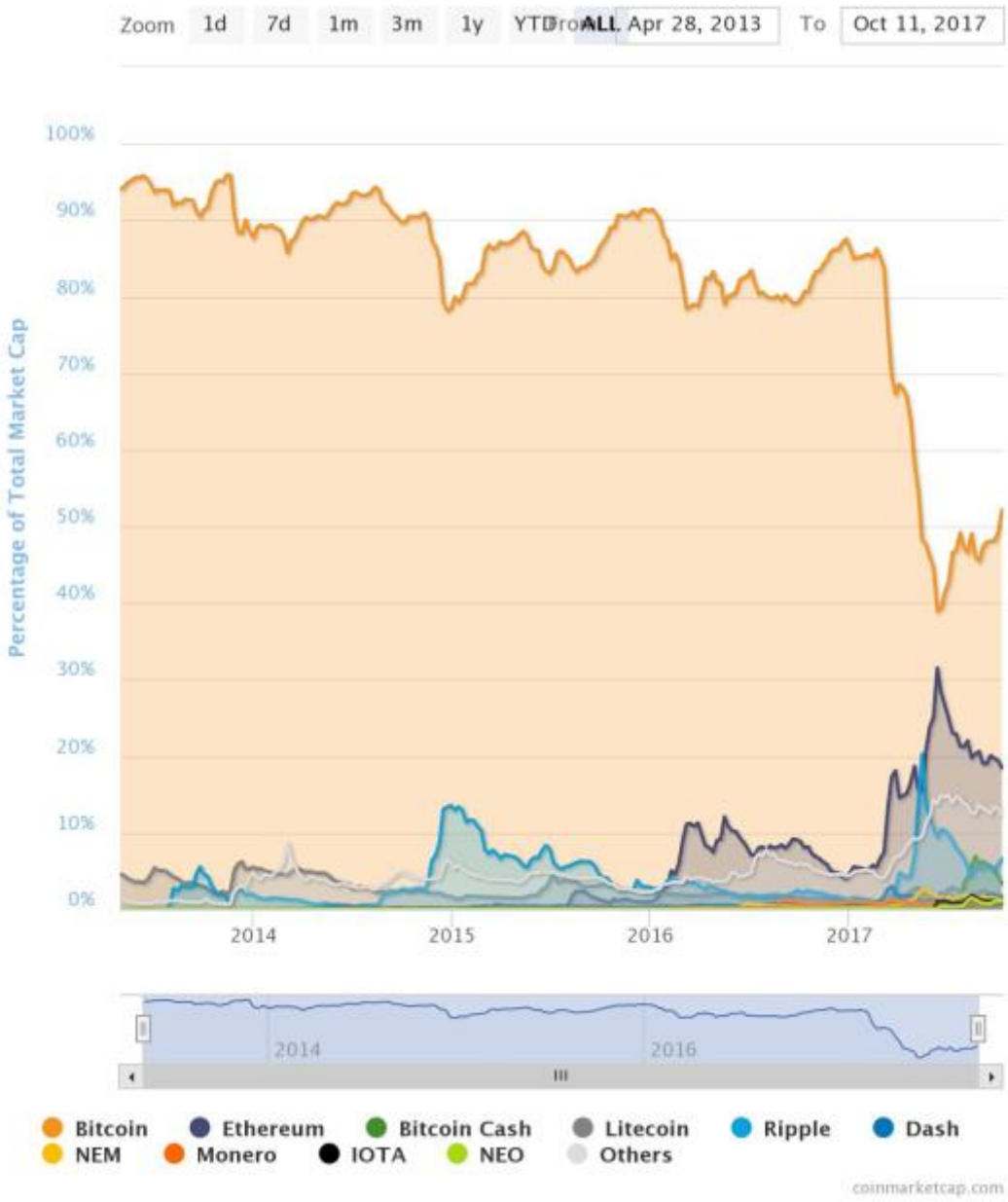
Il s'agit d'une autre monnaie infrastructure au même titre que l'Ether. « Ripple est un système de paiement construit sur un protocole distribué et open source, sur un registre de consensus, et sur une monnaie appelée Ripples (XRP). »[11] Cette crypto-monnaie permet des échanges financiers mondiaux sécurisés et instantanés sans aucuns frais. Ripple est une blockchain privée, son code est modifiable par ses développeurs, et est considérée comme le HTTP de l'argent[12]. Son protocole intéresse tout particulièrement les banques qui l'utiliseraient comme infrastructure de paiement. C'est notamment le cas d'UBS aux Etats-Unis.



Graphique 4 : Evolution du cours XRP/EUR au 11.10.2017[13]

[11] URL : https://blockchainfrance.net/le-lexique-de-la-blockchain/
[12] URL : http://www.coindesk.com/chris-larsen-ripple-is-http-for-money/
[13] URL : https://www.coingecko.com/fr/graphiques_cours/ripple/eur

Voici un aperçu des principales crypto-monnaies et leurs valeurs totales sur ce marché :



Graphique 5 : Evolution des principales « altcoins » du marché au 11.10.2017[14]

[14] URL : https://coinmarketcap.com/charts/

Malgré ces différentes devises alternatives, le Bitcoin occupe, début 2015, 90% de la capitalisation boursière des crypto-monnaies et représente ainsi le standard, bien que très fortement challengé par Ethereum !

Les payements qui utilisent cette devise virtuelle et décentralisée sont enregistrés dans un registre public qui est stocké/enregistré sur les ordinateurs de nombreux - voire tous les utilisateurs bitcoin et consultable de manière permanente sur Internet.

Les Bitcoins sont initialement créés pour récompenser le travail d'analyse et traitement informatique, aussi appelé minage. Ce travail réalisé par les utilisateurs consiste à offrir leurs compétences informatiques et leur puissance de calcul afin de vérifier et enregistrer les payements dans le registre public, aussi appelé le grand livre comptable distribué.

En plus du minage, les bitcoins peuvent évidemment être obtenus en échange de monnaies réelles, biens et services divers. Les utilisateurs peuvent envoyer et recevoir des Bitcoins électroniquement avec d'éventuels frais de transactions via des programmes de portefeuilles électroniques sur leur ordinateur, appareils mobiles ou applications web.

Il me semblait important de bien expliquer les origines et le fonctionnement de cette crypto-monnaie afin d'introduire et présenter la technologie qui se trouve derrière et qui constitue l'infrastructure virtuelle fondamentale : la blockchain. Cette dernière permet de rendre le stockage et la transmission des données sensibles sécurisés et infalsifiables.

V Qu'est-ce que la technologie Blockchain ?

Comme énoncé précédemment, la blockchain est une technologie qui permet le stockage et l'échange d'informations de pair à pair. Le fonctionnement de cette infrastructure informatique repose sur 3 caractéristiques majeures :

- ⇒ Elle est sécurisée
- ⇒ Elle est transparente
- ⇒ Elle fonctionne sans organe central de contrôle

Sécurisée, comme je l'expliquerai en détail plus loin dans ce travail.

Transparente, car chacun peut la consulter et voir l'ensemble des échanges inscrits sur la blockchain depuis sa création.

Décentralisée, car elle est basée sur les relations de pair à pair et le minage.

5.1 Définition

Selon Vitalik Buterin[15] (concepteur de la blockchain Ethereum), la blockchain se définit comme suit :

« A magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies. »

Cette définition manque certainement de rigueur scientifique, notamment par l'emploi du terme « magic » qui fait sans doute insidieusement référence à la nouveauté et la technicité de cette technologie.

Cependant, j'ai choisi volontairement cette définition car il me semble intéressant de souligner les propriétés que Buterin oublie de mentionner. En effet, en ne mentionnant pas les mots clés comme registre, monnaie électronique ou encore transactions financières, il met en évidence indirectement les propriétés bien plus étendues de la blockchain. Il démontre que l'essence même de cette technologie est le traitement de l'information et des processus en général et que le lien avec le secteur financier et économique est réducteur !

Cette définition n'est pas validée par les spécialistes de la cryptographie. La monnaie virtuelle apparaît comme faisant partie intégrante de cette technologie puisqu'elle est à la base du système de récompense du réseau qui en assure sa sécurité. Crypto-monnaie et blockchain semblent de facto inséparables !

Finalement, je trouve la définition de Buterin très intéressante et révélatrice. La crypto-économie et la finalité « paiements » de la blockchain ne sont pas des concepts qui définissent cette technologie mais

[15] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*.

bien des applications de celle-ci. La blockchain est la partie visible de l'iceberg sous lequel le réseau créé des tokens et les échange afin d'en assurer la traçabilité et l'authenticité, ce travail étant récompensé par des incitants (Bitcoins ou Altcoins).

5.2 Les problèmes informatiques de « Double Dépense » et du « Consensus Byzantin ».

Premièrement, sans même prendre en compte les multiples applications possibles de la technologie blockchain, le Bitcoin est déjà un bouleversement fondamental dans le domaine des sciences informatiques. Remettant en cause plus de vingt années de recherche en cryptographie, par des centaines de chercheurs, cette monnaie virtuelle amène une solution au problème de « double dépense » : le fait de dépenser un même Bitcoin plusieurs fois.

Avant que le Bitcoin n'existe, les monnaies virtuelles étaient copiables à souhait. En effet, comme on le fait pour la pièce jointe d'un e-mail, il était possible d'enregistrer et dupliquer n'importe quel type de donnée informatique.

Donc, sans autorité centrale, il était impossible de prouver qu'un certain montant de monnaie virtuelle avait déjà été dépensé auparavant ! il y avait alors un besoin indéniable d'un tiers de confiance pour réguler ces transactions et les enregistrer dans son propre registre (comme le fait par exemple PayPal) : c'est ce qu'on appelle le problème de « double dépense ».

De plus, dans un schéma blockchain, si nous considérons que la communication entre les nœuds d'un même réseau est lente, un utilisateur fraudeur pourrait encoder deux transactions simultanément avec un même montant limité de Bitcoins. Ces transactions seraient ainsi validées parallèlement par les utilisateurs. Il existerait alors deux copies du registre ! Chacune contenant une transaction différente. Une fois l'incohérence révélée, il faudrait alors choisir quel registre fait foi.

L'idée de base est de faire confiance au registre le plus long dont on a connaissance. Dans un contexte où la communication est assez rapide et où les nœuds jouent leur rôle de manière assidue, un registre significativement plus long devrait émerger. Une fois la transaction effectuée, il s'agira de laisser le temps à la synchronisation des registres afin que celle-ci soit validée dans le bon.

Il apparait que ce même fraudeur pourrait manipuler la longueur d'un registre en y enregistrant des transactions fictives (et donc accroître sa longueur) et ainsi faire des deux registres distincts des registres de référence. Alors, comment empêcher ce type de manipulation ?

La solution pour éviter ces possibilités de manipulation est de rendre couteuse la validation d'une transaction dans le bloc et ce endéans une dizaine de minute. Afin d'expliquer ce principe de validation nous devons introduire une nouvelle notion : le hachage. Il s'agit d'une opération qui consiste à faire d'un texte d'une longueur arbitraire un texte d'une longueur fixe. Pour reprendre l'exemple du Bitcoin, il s'agit d'une suite de 256 bits[16] que l'on appelle le hash du texte. L'algorithme de hachage utilisé est le SHA-256 (Secure Hash Algorithm), il fait partie intégrante du protocole Bitcoin. Cette suite doit vérifier un paramètre fondamental : il est strictement impossible de créer un deuxième texte avec le même hash ! Ainsi, avant de simplement valider la transaction (T_1) et l'ajouter au bloc, il faudra trouver la valeur de « x » tel que le message « T_1 + x » ait un hash qui se termine par « 1234567 » par exemple. De plus, la fonction de hachage permet de lier les différents blocs. En ajoutant à tout nouveau bloc le hash du bloc précédent, il devient ainsi impossible d'intercaler de nouvelles transactions dans le registre commun et la chaine est sécurisée…

Ce mécanisme permet de compliquer la mise à jour des registres. Trouver une bonne valeur de « x » demande du temps de calcul car ces calculs sont lourds. C'est ainsi que ces mineurs vont vérifier pour chaque bloc de transactions, que la valeur convient. Le premier à trouver cette valeur de « x » l'envoie aux autres qui pourront valider l'opération et aussi l'ajouter à leur copie du registre. Dans le vocabulaire des crypto-monnaies, ce mécanisme est appelé « the proof-of-work » (preuve de travail) ou encore le « minage ».

Deuxièmement, la technologie blockchain amène une solution supplémentaire. Elle permet de résoudre le problème du « Consensus Byzantin ». Ce challenge informatique fait référence aux difficultés des différents généraux byzantins à communiquer sur le champ de bataille. Ne se faisant pas confiance les uns les autres, il leur était indispensable d'avoir un système de communication coordonné.

D'un point de vue conceptuel, une technologie décentralisée telle que la blockchain, nécessite par voie de conséquence un consensus car les utilisateurs doivent s'accorder sur l'historique des transactions.

A propos du problème de consensus byzantin, différents chercheurs ont publié des modèles de solution à partir de 1982. Il apparaît dans l'ouvrage « Impossibility of distributed consensus with one faulty

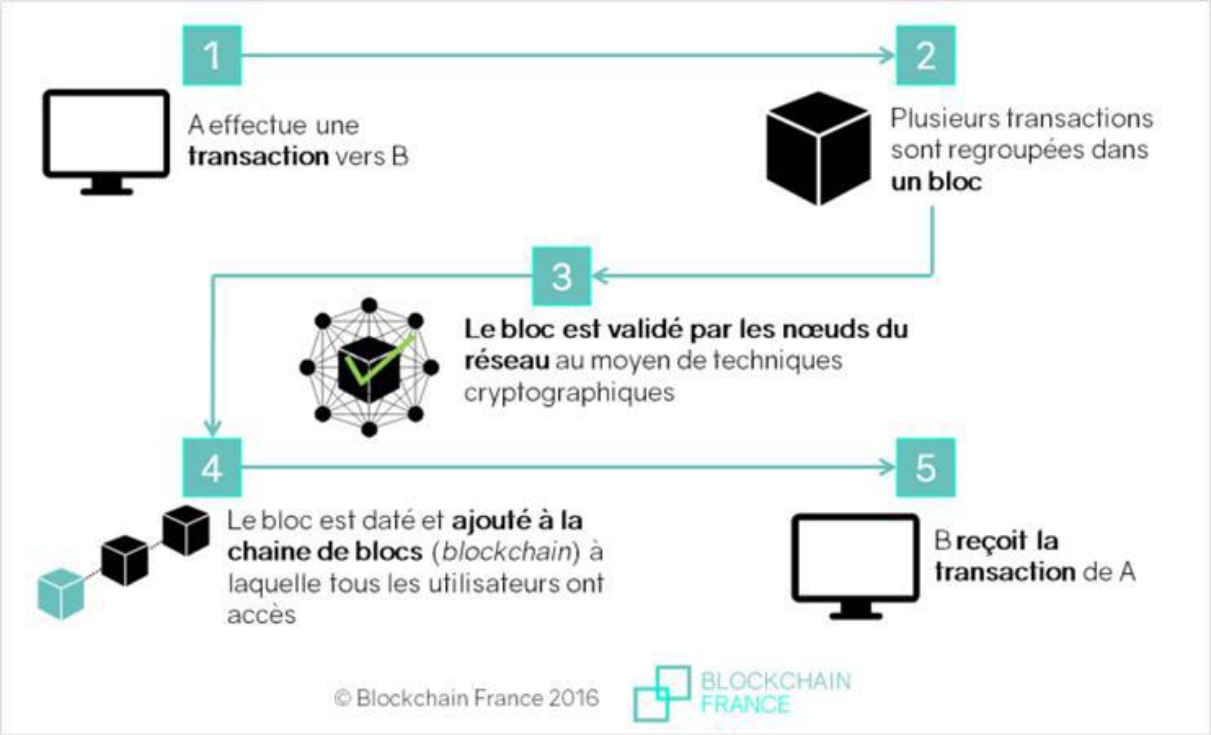
[16] Un bit est une unité binaire de quantité d'information. Elle est généralement représentée par un symbole à deux valeurs, 0 et 1, associées à deux états d'un dispositif.
(http://www.larousse.fr/dictionnaires/francais/bit/9639)

process. »[17] qu'arriver à un consensus déterministe dans un environnement asynchrone (délais pour le minage) est impossible ! C'est pourquoi beaucoup de solutions se concentrent sur des algorithmes probabilistes plutôt que déterministes, intégrant une certaine tolérance d'incorrections (<30% ou <51%). Ce protocole exige un nombre quadratique de messages échangés entre les différentes identités du réseau puisque la totalité des « n » utilisateurs cherche une valeur de « x », partage cette valeur et valide les transactions. C'est pourquoi il est efficace dans l'usage uniquement pour un nombre limité d'utilisateurs, une centaine au maximum. Ce type de protocole est donc connu pour consommer énormément de bande passante et donc d'énergie - puisque lié au nombre d'utilisateurs - et faire preuve de latence dès que quelques dizaines d'utilisateurs sont impliqués. Ce qui engendre aussi des couts de communication importants.

C'est la raison pour laquelle Satoshi Nakamoto a proposé un nouveau protocole : le consensus Nakamoto. Grace à la « preuve de travail », un seul des « n » utilisateurs trouve la valeur de x et la partage aux autres. Ainsi le besoin en bande passante n'est plus proportionnel au nombre d'utilisateurs. Comme expliqué précédemment la chaine de blocs la plus longue fera foi et c'est celle-là que l'on continuera dans le protocole Nakamoto.

[17] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson. Impossibility of distributed consensus with one faulty process. J. ACM,32(2):374–382, April 1985

5.3 En pratique, comment fonctionne une blockchain ?



Quand une transaction est introduite sur le réseau Bitcoin, elle est dirigée vers un nœud aléatoire. Ensuite, elle est redirigée vers les autre nœuds du réseau. Les transactions sont ainsi regroupées en blocs. Afin de sécuriser, vérifier et synchroniser ces transactions, il est nécessaire de disposer d'une certaine puissance de calcul : le minage. En plus de valider les transactions et les ajouter aux blocs, les mineurs doivent résoudre des problèmes mathématiques complexes. Cette complexité varie de manière constante en fonction du nombre de mineurs connectés au réseau. En plus de sa complexité, la résolution dépend d'une variable aléatoire afin que ce ne soit pas toujours le même mineur qui valide les blocks. C'est un des points fondamentaux de sécurisation de la blockchain.

Une fois le block validé, il est inséré temporairement dans la blockchain afin que les autres utilisateurs authentifient la preuve de travail.

Les mineurs sont rémunérés en bitcoins. C'est le seul moyen de créer de nouveaux bitcoins et donc l'unique moyen d'accroitre la masse monétaire. En 2009, la rémunération était de 50 BTC par bloc ajouté. La règle veut que la rémunération est divisée par deux tous les 210.000 blocks créés. De nos jours, les mineurs perçoivent 12,5 BTC par bloc.

Ce mécanisme prévoit ainsi que cette récompense va décroître au fur et à mesure que le temps avance. On sait donc que la masse monétaire Bitcoin va converger vers un maximum absolu de 21 millions de BTC. Chaque Bitcoin est divisible jusqu'au 100 millionième. Ce mécanisme est donc totalement transparent.

5.4 Distinction entre blockchains publiques & privées

Il existe différents types de blockchain. Caractéristique commune : il s'agit d'un registre distribué.

Une blockchain publique est accessible à n'importe quel utilisateur d'Internet (comme par exemple : Bitcoin ou Ethereum). Le caractère public de ce registre vient du fait que la participation de chacun est gratuite et inconditionnelle, cela afin de déterminer quels blocs peuvent être ajoutés à la chaine et quel est leur état dans le système. Cette décentralisation repose sur un mécanisme de consensus : le « proof-of-work » ou « proof-of-stake ».

Dans le cas d'une blockchain privée, les autorisations de validation, d'écriture, sont monitorées par un pool décisionnel central, représenté par un nombre restreint de nœuds. Par contre les autorisations de lecture peuvent être aussi bien publiques que privées. L'accès au registre est restrictif et un processus organisationnel de « Know-Your-Business » et « Know-your-Customer » permet d'autoriser ou refuser l'accès aux utilisateurs.

La différence entre le caractère public ou privé d'une blockchain réside dans deux facteurs opposés :

1. L'étendue donnée à la décentralisation de la blockchain
2. L'anonymat qu'on lui confère

De plus, l'existence d'une crypto-monnaie dans une blockchain privée n'est pas nécessaire puisqu'il n'y a en effet pas de besoin de rémunérer les membres pour la validation des transactions.

Entre les deux, il existe aussi des blockchains hybrides qui sont partiellement décentralisées. Elles varient en fonction du niveau de confiance qui leur est donné. Je ne développerai pas davantage ce type de structure.

VI La Blockchain et ses applications

6.1 La blockchain version 1.0 : la crypto-monnaie

De la même manière que l'*Internet of Things* (IoT) connecte les objets, il semble que le Bitcoin – et la technologie sous-jacente de la blockchain – représente déjà la monnaie de l'Internet mais aussi un système de payement digital. Dans la manière dont il connecte les finances, on pourrait appeler la blockchain l'*Internet of Money* (IoM).

Comme nous l'avons démontré jusqu'ici, la technologie blockchain a le potentiel de révolutionner les applications et redéfinir l'économie digitale. Ses possibilités s'étendent bien au-delà de la crypto-monnaie, ce que nous développerons plus tard dans ce rapport.

Le principe du grand registre décentralisé/distribué infalsifiable définit ce que l'on appelle la blockchain 1.0 : la blockchain, le protocole et la monnaie virtuelle. Ces trois éléments représentent les couches qui sont empilées pour constituer la technologie blockchain 1.0 :

1.	La crypto-monnaie	Bitcoin, Ethereum, Litecoin
2.	Le protocole Bitcoin et les clients	Programmes qui conduisent les transactions
3.	La blockchain	Registre décentralisé

Comme le montre le *Graphique 1* en page 12, le cours du Bitcoin s'est mis en action dans le courant du mois de novembre 2013. Peu de temps avant cela, la crise Chypriote et un nombre de transactions soutenu en Chine (dus à une absence de frais taxant les échanges) ont créé un pic de demandes en Bitcoin faisant grimper son cours à 800 USD. Peu de temps après, le gouvernement chinois a régulé l'utilisation de cette crypto-monnaie en empêchant les personnes morales de l'utiliser. Le cours est finalement redescendu à son niveau initial d'environ 350 USD en novembre 2014. Lorsqu'on connaît

la valeur actuelle d'un Bitcoin, il apparaît que cette devise est très volatile. Cette volatilité pouvant freiner voire empêcher une adoption de masse.

Cependant, il semble que cette barrière que représente la volatilité n'en soit pas tout à fait une. En effet, certains outils développés par des entreprises spécialisées permettent de contrecarrer cette instabilité de la crypto-monnaie. Lors de mes recherches j'ai pu identifier différents outils aidant à cela. Voici les plus sérieux d'entre eux :

Uphold[18], qui bloque les réserves de Bitcoin à un taux de change fixé.

Tether[19], qui permet une indexation fonction du cours du dollar américain.

Coinapult's LOCKS[20], qui donne la possibilité de « tracker » le cours de l'or, de l'argent, de l'USD, de l'EUR ou du GBP.

D'autres préfèrent mettre en avant le fait que cette crypto-monnaie est clairement moins volatile que certaines devises réelles et aussi moins exposée à l'inflation.

Finalement, contrairement aux devises réelles, pour lesquelles les gouvernements et banques centrales peuvent imprimer toujours plus de billets et augmenter les volumes en circulation, le Bitcoin est régulé à un rythme prédéterminé et pour une quantité plafonnée. Cette crypto-monnaie créée par l'ajout de nouveaux blocs dans la chaine l'est à un rythme connu et régulier. Nous savons ainsi qu'en 2140 le nombre maximum plafonné de Bitcoins en circulation atteindra 21 million d'unités.

Cette première partie du travail a permis de bien cerner le fonctionnement des Bitcoins et de sa technologie sous-jacente. L'aspect financier de son utilisation nous a permis de cerner l'efficacité de ce protocole et ses caractéristiques open source, infalsifiables et la sécurisation qui en découle. Nous allons dans la suite de ce travail élargir le champ d'application de la blockchain à d'autres secteurs d'activité et mettre en évidence comment les informations de manière générale peuvent y être stockées et échangées de manière transparente.

6.2 La blockchain version 2.0 : les Contrats

En 2010, Satoshi Nakamoto indiquait dans une communication :

[18] URL: https://uphold.com/
[19] URL: https://tether.to/
[20] URL : https://coinapult.com/

« Cette technologie supporte une variété incroyable de types de transactions possibles que j'ai conçues il y quelques années (…). C'est ce que nous souhaiterons explorer dans le futur, mais il fallait que la structure conçue dès le départ le permette. »

C'est pourquoi le deuxième volet de la blockchain fait à présent référence à cette structure en tant que marché, considéré comme un lieu d'échange de données.

Nous pourrions très synthétiquement comparer la blockchain à un protocole analogue à celui du Web. En effet, une fois que le réseau Internet a été mis en place en tant que technologie et infrastructure, des services ont pu être créés afin d'utiliser cette technologie. Airbnb, Amazon, Booking, sont des entreprises qui complexifient constamment leur offre et leur utilisation de cette infrastructure web afin d'en tirer avantage.

L'idée clé est ainsi de comprendre le fonctionnement décentralisé de la gestion des interactions entre membres d'un même réseau dans un but de stocker, confirmer ou transférer tout type de propriété ou contrat.

Il serait, par exemple, réalisable de migrer vers la blockchain des titres de propriété immobiliers, des contrats de mariage, des registres d'immatriculations de véhicules ou encore des licences professionnelles, l'identité digitale et donc l'accès à ces données pouvant être confirmés via la blockchain grâce à des cartes d'identité ou passeports solidement codés. Pour la sphère privée, on imagine l'enregistrement de crédits, contrats, signatures.

Dans la logique de la preuve-de-travail, on aurait alors des possibilités de « preuve-d 'assurance » ou « preuve-de-propriété » … La blockchain étant toujours connectée, on pourrait imaginer un agriculteur assuré contre les intempéries ou la sècheresse et dont le contrat est encodé dans la blockchain, se voir indemnisé automatiquement lorsque le niveau de pluviométrie est inférieur à « x » pendant « n » période…

Néanmoins, un des premiers champ d'application de la blockchain reste le secteur financier. Il me semble évident que cette technologie constitue une rupture avec la banque traditionnelle que nous connaissons actuellement, bien que sur les voies de la digitalisation, surtout dans l'offre qu'elle fournit à ses clients. La blockchain se positionne comme un outil pour une gestion des couts, une gouvernance plus efficace et une plus grande transparence dans les échanges. En effet, l'intérêt pour une blockchain privée présente certains avantages notamment pour le secteur financier : facilité d'audit, compliance, connaissance des intervenants. Dans ce cas, vu l'intervention des acteurs humain (ce qui va à l'encontre

du principe fondamental de la blockchain), nous devrions plus précisément parler de l'utilisation d'une technologie du registre distribué (Distributed Ledger Technology - DLT).

Une autre application possible pour la blockchain est le crowdfunding. L'idée de ce modèle de levée des fonds grâce à un réseau pair-à-pair est d'éviter d'emprunter du capital à risque. Actuellement, un service central tel que, entre autres, Indiegogo ou Kickstarter, est nécessaire pour cette levée de fonds. La blockchain permet d'éviter l'intervention d'un intermédiaire. Une plateforme de crowdfunding basée sur la technologie blockchain permettrait aux entrepreneurs d'acquérir du financement en générant leurs propres monnaies digitales en vendant leurs parts sociales cryptographiées. Les investisseurs recevraient ainsi des parts sociales des projets qu'ils supportent sous forme de tokens.

Les avantages :

- ⇒ Plus besoin de prestataire de service de paiement pour sécuriser les transactions financières.
- ⇒ Plus besoin de prestataire de certification électronique pour certifier la bonne souscription aux titres financiers.
- ⇒ Conservation des registres de titres
- ⇒ Création d'un marché secondaire pour les titres financiers « crowdfundés » assurant une certaine liquidité à ces titres en toute transparence.
- ⇒ Garantie, traçage des dons promis, qui ne le sont que moralement actuellement.

6.2.1 Les types d'usages de la blockchain

Le transfert d'actifs

La blockchain permet évidemment d'effectuer des transferts monétaires. Le cas du Bitcoin est le plus flagrant en la matière. Cependant, ce protocole permet aussi de transférer d'autre types d'actifs tels que des actions, obligations, titres de propriété, votes. En plus de sa valeur propre, chaque token peut recevoir des métadonnées contenant des informations diverses. Il devient ainsi une preuve de propriété.

La blockchain comme registre

Les caractéristiques de transparence et de non répudiation de la blockchain en font un outil intéressant pour le stockage de données. Elle peut revêtir un enjeu crucial lorsqu'il s'agit de certification ou de

traçabilité d'informations. Tous types de documents légaux peuvent être concernés : contrat de mariage, actes de naissance, …

« Lorsque je me suis inscrit à HEC-ULg, j'ai dû fournir un diplôme qu'il m'était impossible de retrouver ! Il me semble que la blockchain aurait pu m'aider en gardant un enregistrement inviolable de mon diplôme. Cela m'aurait évité des démarches couteuses auprès des autorités publiques. »

Plus loin dans ce travail, nous verrons comment cette technologie peut aider la gestion des chaines logistiques dans le secteur de l'agroalimentaire ou de la santé.

La blockchain n'apporte pas la preuve qu'un document est légalement « vrai ». Mais, il montre qu'il existe bien et horodate sa création dans la chaine de blocs.

Le concept de « smart property » ou propriété intelligente.

En utilisant la blockchain de cette manière, nous ouvrons évidemment une nouvelle gamme d'applications possibles. Une donnée, un bien, ou une propriété qui utilise l'infrastructure blockchain via un « smart contract » devient par voie de conséquence une « smart property ». C'est pourquoi ce dernier devient alors transférable et exposé à faire partie d'une transaction.

Ce concept permet de contrôler la propriété (l'appartenance) d'un bien, d'un actif en l'enregistrant dans la blockchain comme un actif électronique et en y ayant accès via sa clé privée. Dans certains cas, nous pourrions même imaginer le contrôle de biens réels. Nous pourrions par exemple ouvrir l'accès à une maison, une propriété ou un véhicule via son smartphone grâce à son identité digitale codée dans la blockchain. Cet accès se ferait via l'utilisation de technologies embarquées telles qu'un QR Code, une puce NFC (Near Field Control), des iBeacons[21] ou via un accès Wi-Fi.

Comment cela fonctionnerait-il ?

Lorsqu'un utilisateur soumet une demande d'accès en temps réel, le « smart contract » encodé dans la blockchain pourrait instantanément envoyer un token ou une confirmation au bien réel (connecté via l'Internet of Things) ou à l'utilisateur – sans besoin d'un token préconfiguré. Elle prendrait la forme

[21] Ibeacon est un composant logiciel s'appuyant sur la technologie Bluetooth 4.0 Loud Energy (BLE). Il se base sur la « micro localisation » via des balises très simples qui émettent en Bluetooth un signal particulier. (Http://www.mywebmarketing.fr/quest-ce-que-l-ibeacon/)

d'un QR Code utilisable une seule et unique fois pour donner l'accès à un véhicule de location ou une chambre d'hôtel… C'est ce que cette technologie permet de faire ! Elle réinvente l'authentification des données, l'accès aux données en les rendant beaucoup plus flexibles et orientées vers le « real-time ». Tout cela étant rendu possible par l'utilisation du réseau Internet et l'intégration des biens physiquement réels dans ce réseau via des programmes et technologies basées sur le Net.

Ce concept de « smart property » est totalement nouveau et constitue une rupture avec la définition de la propriété que nous connaissons actuellement. Nous ne sommes clairement pas habitués à détenir un bien digitalement, cryptographiquement du fait que ce droit de détention est auto-appliqué par le codage. Or, ce code étant lui-même auto-appliqué par l'infrastructure blockchain, il ne peut dévier.

Cette notion d'accès sécurisé est bien évidemment déjà connue. Il se fait via des mots de passe, des identifiants ou des programmes de gestion de sécurité. Ce que changent la blockchain et la notion de « smart property » c'est que rien n'est préconfiguré ou centralisé. Donc, ces informations ne sont pas falsifiables. Il n'y a pas ce phénomène de confiance à un tiers qui doit intervenir puisque ces accès sont autogérés et ce en temps réel !

Nous pouvons alors aisément imaginer les gains d'efficacités financière, temporelle et de gestion des couts pour une entreprise qui intégrerait ce protocole dans son Business Model.

Un exemple concret : les « colored coins ».

Une des toutes premières implémentations du concept de « smart property » dans la blockchain sont les « colored coins ». Afin de faire correspondre certains actifs bien spécifiques à une contre-valeur Bitcoin certains Bitcoins étaient coloriés dans la chaine de transaction. Donc, certains Bitcoins sont codés pour faire référence à d'autres actifs et peuvent être échangés en toute sécurité via la blockchain.

En réalité, il me semble que ce modèle réclame un certain niveau de confiance entre les utilisateurs, ce qui normalement n'est pas nécessaire. En effet, dans ce cas l'actif auquel fait référence le bitcoin colorié devra être déployé, fourni comme convenu ! Par conséquent, ces « colored coins » seront plutôt utilisés dans des communautés fermées.

L'idée de base est bien de mettre en évidence que ces crypto-monnaies peuvent être liées à des actifs digitaux ou réels et permettent de faire levier afin d'effectuer des transactions bien plus complexes menées via la blockchain.

Les « smart contracts »

Selon l'article 1101 du Code Civil, un contrat est « une convention par laquelle une ou plusieurs personnes s'obligent, envers une ou plusieurs autres, à donner, à faire ou à ne pas faire quelque chose. »

Dans le contexte blockchain, un contrat ou plutôt un « contrat intelligent » désigne une transaction qui va au-delà d'un simple rapport d'achat/vente. Il peut intégrer des implications bien plus complexes.

Lorsque que l'on parle de contrat traditionnel, les parties doivent se faire confiance afin qu'elles remplissent leur part de l'obligation. Les contrats intelligents permettent ce même type d'accord mais font disparaître ce besoin de confiance relative. Pourquoi ? Tout simplement parce qu'ils sont définis par le code et exécutés, appliqués par le code, automatiquement.

Il y a 3 caractéristiques clés lorsque l'on parle de contrat intelligent :

Il est autonome : cela signifie qu'une fois qu'il est lancé et fonctionne, ce contrat et l'agent qui l'a initié ont par la suite plus aucun besoin d'être en contact.

Il est auto-suffisant : ce contrat est capable de mobiliser les ressources nécessaires. Par exemple, lever des fonds via la fourniture d'un service ou l'émission d'actions. Puis dépenser ces fonds pour l'achat d'espace de stockage ou de données.

Il est décentralisé : il ne se trouve pas sur un serveur unique et centralisé. Il est distribué et s'auto-exécute au travers des nœuds du réseau.

Les trois principaux apports des contrats intelligents sont : une vitesse accrue, une meilleure efficacité et une certitude que le contrat sera exécuté comme convenu[22].

Un contrat intelligent ne peut faire autre chose qu'exécuter le code prédéfini. Il n'y a pas de place pour les sentiments ou les interactions qui pourraient altérer le processus d'échange ou d'exécution d'un contrat. Comme le dit Lawrence Lessig, un juriste américain de renommée mondiale notamment connu pour avoir fondé le « Center for Internet & Society » : « code is law » (le code est la loi).

Pour moi, ce type de contrat ne rend pas possible quelque chose qui était impossible auparavant. Il amène une solution au problème de confiance entre les parties en sortant de l'équation la partie

[22] Blockchain France Associés (Mai 2016). La Blockchain décryptée. Les clefs d'une révolution. (pp 11)

subjective de l'humain, l'aléa moral. Le fait de confier ses données à un tiers représente un danger. C'est ce risque que tend à éliminer la technologie blockchain.

D'autre part, cela permettra aussi de réduire les couts de vérification, d'exécution ou d'arbitrage et les risques de fraude.

Si ce genre de contrat se développe vers une utilisation globalisée. Il apparaît clair qu'un organe de contrôle et de régulation devra être créé dans le but de faire la différence entre nos contrats tangibles qui sont légalement interprétables et flexibles et ces contrats virtuels qui s'exécutent peu importe les éléments extérieurs et les situations auxquelles ils font face !

D'autre part, ces contrats intelligents n'ont pas en eux d'autorité juridique. Ils posent un défi de taille concernant l'aspect éthique et juridique de leur utilisation. Je pense notamment à la détermination de la responsabilité légale et la protection des consommateurs !

L'exemple de Slock.it

Slock.it est la première DAO (Decentralized Autonomous Organisation) à voir le jour. Son but est de faire le lien entre la blockchain Ethereum et des objets concrets, réels. Son slogan : « louez, vendez, ou partagez n'importe quel objet – sans intermédiaire »[23]. Slock.it rend les « smart contrats » utiles en les rendant exécutables.

Elle rend cela possible en utilisant un « slock », un verrou intelligent lié à un contrat Ethereum, qui permet d'ouvrir n'importe quoi.

« Slock.it vise à rendre certains objets entièrement autonomes ; nous pourrions ainsi directement signer des contrats avec eux, sans intermédiaire »[24]. Location d'un appartement, d'un bureau, d'un véhicule ; recevoir des paiements. Slock.it développe toute une série de technologies qui peuvent être couplées à des objets pour les rendre intelligents grâce à Ethereum. Le tout sans dépendre d'intermédiaires tels que des opérateurs de paiements ou être à la merci de hackers !

Prenons le cas d'une location d'appartement du type Airbnb. Le propriétaire équiperait son appartement d'un verrou intelligent Slock.it connecté à la blockchain et gèrerait sa location via son mobile grâce une interface web classique. En liant cette serrure à un « smart contract », dès qu'un

[23] https://slock.it/
[24] Ibid

utilisateur souhaite louer ce bien, il effectue le paiement Dès qu'il est confirmé, il ouvre automatiquement l'accès à l'appartement.

En pratique cela semble très confortable comme utilisation mais plusieurs questions font surface quand je pense à l'utilisation réelle de ce modèle :

Les paiements se font en Ethers. Quelle proportion de propriétaires serait d'accord d'être payée en crypto-monnaie ? (Même si Slock.it travaille sur une application de conversion automatique des Ethers en euros et l'utilisation de moyens de paiements classiques tels que cartes bancaires, de crédit ou virements…)[25].

Quelle adoption de masse pour ce type de processus ?

Quelle juridiction règlera ces problèmes transnationaux en cas de litige ?

Sur le plan éthique, comment vérifier la réelle identité des locataires qui peuvent être des trafiquants ou autres gangsters ?

6.3 La blockchain version 3.0 : Applications

La blockchain peut sembler abstraite quand on n'expose pas concrètement ses applications. J'ai choisi de présenter ci-après les utilisations les plus marquantes concernant l'implémentation de cette infrastructure de rupture dans la gestion des données de l'entreprise mais aussi plus généralement dans la gouvernance des organisations privées ou publiques.

D'après moi, la plateforme la plus capable d'accueillir le développement d'application distribuées (Dapps) est celle d'Ethereum, j'avais déjà utilisé la définition que son fondateur – Vitalik Buterin - donnait à la blockchain car elle me semblait volontairement non-réductrice dans son champs d'application. Cette volonté d'ouvrir le champs d'application de cette technologie se traduit dans l'infrastructure qu'elle met à disposition. Mais finalement, qu'est-ce qu'Ethereum ?

[25] URL : https://www.ethereum-france.com/slock-it-la-promesse-des-objets-connectes-surla-blockchain/

6.3.1 La blockchain Ethereum

Plus qu'une crypto-monnaie : l'Ether (évoquée dans la première partie de ce travail), Ethereum délivre une infrastructure qui tend à fournir une solution complète avec un langage dit « Turing-Complete »[26], en référence à la force de calcul de la machine de Turing qui est capable de calculer toutes les fonctions calculables, en l'occurrence, la capacité à traiter tout protocole, crypto-monnaie ou blockchain. Elle est considérée comme la blockchain la plus prometteuse en terme d'avenir et de potentiel.

En effet, le plan de Satoshi Nakamoto prévoyait trois étapes dont deux ont uniquement été déployées : la blockchain (le registre open source décentralisé) et le protocole Bitcoin (système de transactions sans besoin de tiers de confiance). Ces étapes permettent dans le cadre de Blockchain 1.0 de réaliser des transactions de crypto-monnaies simples mais lorsqu'il s'agit de transactions plus complexes dans Blockchain 2.0, comme par exemple l'enregistrement de « smart properties » ou de « smart contracts », il est nécessaire de mettre en place une troisième étape… c'est ce que permet Ethereum.

En tant que blockchain publique, la volonté d'Ethereum est d'être considéré comme l'infrastructure fondamentale permettant d'exploiter n'importe quelle blockchain ou protocole. Je la qualifierais de plateforme de développement universelle.

Le but est de fournir un compromis différent qui serait utile pour un nombre important d'applications. Cette version de programmation Turing-Complet permet à chacun d'encoder des « smart contracts » et des « Dapps » (Decentralized Applications) en instaurant ses propres règles de propriété et de formats.

Le principe fondamental d'Ethereum est de coupler les caractéristiques de la blockchain avec des « smart contracts », ces programmes autonomes qui exécutent de manière systématique des conditions prédéterminées. Ce sont eux qui représentent le plus grand potentiel applicatif !

L'inventeur de l'Ethereum est Vitalik Buterin, en 2013. Pensant que la blockchain Bitcoin était perfectible il lança son projet en 2015 après avoir levé 19 millions de dollars pour le financer. Cette première version est dédiée spécialement aux développeurs. La deuxième version du projet arrive en 2016 avec Homestead. Cette version plus stable que la précédente fait bondir le cours de l'Ether (*Graphique 3*).

[26] URL : http://dictionnaire.sensagent.leparisien.fr/Turing-complet/fr-fr/

Quelles différences par rapport à la blockchain Bitcoin ? Quels avantages pour Ethereum ?

Ces deux infrastructures ont des points communs tels qu'une crypto-monnaie liée, l'utilisation du protocole blockchain, un mécanisme de consensus décentralisé et des mineurs qui valident les blocs. Néanmoins, lorsque l'on étudie plus précisément les caractéristiques de ces deux blockchains, on s'aperçoit qu'il existe de nombreuses différences. J'en ai identifié neuf [27] :

1. Sur Ethereum, un nouveau bloc est miné toutes les 12 secondes alors que sur Bitcoin, il faut 10 minutes. Cette rapidité est permise par l'utilisation du protocole Ghost[28] (Greedy Heaviest Observed Subtree).
2. Le modèle de création monétaire (Ether et Bitcoin) n'est pas le même. Pour le bitcoin, la récompense pour avoir miné un bloc est divisée par 2 tous les 4 ans alors que l'Ether reste constant chaque année et à l'infini.
3. Le calcul du cout des transactions n'est pas identique. Sur Ethereum il dépend de la force de calcul utilisée et de la complexité de la transaction. Ce cout est discrétisé en unités d'Ether et appelé Gaz. Sur Bitcoin il reste le même dans tous les cas.
4. Ethereum propose un langage interne Turing-Complet alors que Bitcoin est beaucoup moins flexible et puissant.
5. Ethereum a été fondé grâce à du Crowdfunding alors que Bitcoin est apparu soudainement par le biais d'un anonyme. C'est pourquoi l'avancement d'Ethereum est public tandis que les premiers mineurs bitcoin possèdent la majeure partie des unités jamais extraites.
6. L'utilisation de Ghost décourage le minage par pools centralisés car il n'y a pas d'avantage en terme de gains lors de l'émission de nouveaux blocs.

   « Un bloc orphelin (ou ***stale bloc***) est un bloc qui n'est pas retenu lorsque deux nœuds trouvent la solution en même temps, c'est-à-dire un bloc qui a été propagé dans le réseau, vérifié par d'autres nœuds comme étant correct et proposé pour l'insertion dans la blockchain, mais finalement rejeté puisque la chaîne plus longue dominante ne l'a pas intégré. Dans le Bitcoin, la probabilité de trouver un bloc en même temps est relativement basse, puisque l'émission de

[27] URL : http://blogchaincafe.com/ethereum-vs-bitcoin-les-differences

[28] URL : https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/

deux blocs est espacée de dix minutes. Les blockchains dites rapides comme celle d'Ethereum ont des temps de bloc beaucoup plus courts (12 secondes) et souffrent donc davantage du problème des *stale blocs*. »

Ghost permet d'éviter ce problème et de dissuader la centralisation du minage.

7. La taille des blocs est limitée sur Bitcoin à 1MB ce qui limite le nombre de transactions possibles. Ethereum n'a théoriquement pas de limite dans la taille des blocs.
8. Ethereum va lancer (normalement en 2017) un nouveau type de consensus : le « proof-of-stake ». Cette technique est plus efficace et plus fiable, elle permet des économies de calcul et est plus difficile à attaquer.
9. « Le fait que Ethereum intègre des langages spécifiques à sa plateforme permet d'avoir une réponse en temps réel de l'activité transactionnelle de la base de données. »

Ethereum ne se positionne pas comme un concurrent de Bitcoin. Les utilisations sont différentes. Bitcoin est utilisée principalement pour les devises, les transactions de crypto-monnaies. Ethereum permet de créer tout type d'applications, elle est beaucoup plus flexible.

6.3.2 Application au Cloud Computing

Les services de cloud computing n'ont pas été épargnés par la blockchain. Ces services peuvent prendre différentes formes :

⇒ Infrastructure as a Service (IaaS) : permet d'héberger des données
⇒ Platform as a Service (PaaS) : permet de disposer des services et applications via Internet
⇒ Software as a Service (SaaS) : met à disposition des logiciels

Ce type d'application est de plus en plus utilisé par les entreprises car elle permet de se passer de l'achat ou du stockage de matériel informatique.

Microsoft a notamment décidé d'utiliser ce type de service pour lancer sa propre plateforme : Azure[29], blockchain-as-a-service (BaaS). Elle commercialise ainsi une Platform-as-a-Service (PaaS) dont voici deux cas pratiques d'utilisation et d'implémentation :

[29] https://azure.microsoft.com/en-us/solutions/blockchain/

Le cas Swiss Re[30]

Swiss Re est le deuxième plus important réassureur dans le monde. Ils sont présents dans plus de 25 pays avec un chiffre d'affaires en 2016 de 33 milliards d'USD.

Bien que le modèle d'activité de la firme soit basé sur un système de réassurance traditionnel : vendre de la réassurance aux compagnies d'assurance afin de les assurer contre les pertes, avec un focus sur les « gros contrats », Swiss Re a décidé de proposer un nouveau modèle de micro-services basés sur les risques simples en offrant une expérience client totalement automatisée.

C'est en s'associant avec une de leurs filiales : FlightStats, fournisseur de données sur les vols aériens, qu'ils ont mis en place une assurance contre les vols en retard qui indemnise automatiquement les passagers sinistrés

Cela a permis à Swiss Re de montrer au marché son caractère innovant et acquérir des nouveaux clients en supprimant le besoin de remplir de manière fastidieuse des formulaires en cas de vols en retard. De plus, cela permet de réduire les investissements structurels en back office pour la gestion de ces sinistres.

La création et l'implémentation de ce projet ont pris huit mois à l'entreprise helvétique.

Le cas ASOS[31]

Asos est un des leaders de la vente en ligne d'articles de mode. Cette firme anglaise possède plus de douze millions de clients dans le monde, quatre-vingt mille SKU (Sales Keeping Unit) et plus de huit cents marques sur leur site web.

La raison pour laquelle Asos a choisi de faire confiance à la PaaS Azure est qu'elle permet une distribution sur trente « data centers » ce qui leur assure un haut niveau de performance et une disponibilité n'importe où dans le monde pour leurs clients. N'étant plus liée à un serveur central, l'entreprise élimine le risque de panne générale d'un serveur unique.

[30] URL : https://customers.microsoft.com/en-US/story/swissre

[31] URL : https://customers.microsoft.com/en-US/story/asos

Par contre, cela remet en cause le principe fondamental de l'esprit blockchain : la décentralisation des données !

Pour offrir une solution au problème de centralisation des données d'entreprise, une start-up a vu le jour : Storj. Celle-ci permet de stocker des données dans le cloud mais de manière décentralisée. Comment cela fonctionne-t-il ? Les utilisateurs mettent leur espace de stockage libre à la disposition des autres. Les fichiers qui doivent être stockés sont dispersés sur plusieurs serveurs et fragmentés. Le propriétaire peut y accéder et les reconstituer uniquement à l'aide de sa clé privée. Les utilisateurs qui mettent leur espace à disposition sont rémunérés.

Cette solution offre aussi une opportunité pour éliminer les problèmes de silos d'informations en entreprise. Dans le cas d'une gestion de projets qui impliquerait différents départements, d'une même société ou d'un consortium, cela permettrait de réduire la probabilité d'erreurs ou d'incompréhensions. De plus les données seraient sécurisées et les fuites causées par des intervenants malveillants seraient éliminées.

Plus globalement, le cloud devient ainsi plus efficient, plus sécurisé et moins onéreux.

6.3.2 Dapps, DAOs et DACs

Qu'est-ce qu'une Dapp ?

Une Decentralized Application, Dapp, (Application décentralisée) est une application qui s'exécute sur la blockchain de manière distribuée, sans organe de contrôle centralisé, sans besoin de tiers de confiance. C'est une forme complexifiée et plus autonome d'un « smart contract » qui devient en fait une entité autogérée. La Dapp exécute des opérations préprogrammées ou même autoprogrammées sur la blockchain. Voici quelques exemples d'applications décentralisées dans des domaines divers :

Nom du projet et URL	Activité	Equivalent centralisé
LaZooz ***http://lazooz.org/***	Covoiturage, taxi, incluant Zooz, une monnaie preuve-de-mouvement	Uber

Nom du projet et URL	Activité	Equivalent centralisé
Twister ***http://twister.net.co/***	Réseautage social, microblogging de pair-à-pair	Twitter, Facebook
Storj ***http://storj.io/***	Stockage de données	Dropbox
Swarm ***https://www.swarm.co/***	Plateforme de crowdfunding	Indiegogo, Kickstarter

[32]

Qu'est-ce qu'une DAO ?

Il d'agit d'une « Decentralized Autonomous Organisation », organisation autonome décentralisée. C'est une forme plus complexe de Dapp. Elle se définit comme un logiciel qui tourne sur la blockchain et qui détermine quelles règles de gouvernance et de fonctionnement sont à appliquer en rapport avec une « constitution » publique sur la blockchain. Les DAOs sont utilisées par des communautés qui se concentrent autour d'un objectif commun. Elles ont aussi comme mission d'assurer la mise en place des mécanismes de financement de l'organisation - via l'émission d'actions ou via du crowdfunding par exemple. A l'exemple d'un gestionnaire de fonds d'investissement, la DAO va prendre les décisions stratégiques en adéquation avec la vision, la ligne de conduite de l'organisation. Les détenteurs de tokens vont décider collectivement et de manière transparente des orientations à prendre, des projets à suivre ou non, et de distribuer les risques et récompenses liés.

Il s'agit en réalité d'un concept dérivé de l'intelligence artificielle. Dans le cas d'un réseau décentralisé des agents autonomes exécutent les taches. Avec les DAOs, les « smart contracts » sont ces agents et exécutent des taches prédéfinies et pré approuvées en fonction des conditions changeantes.

[32] Swan, M. (2015). *Blockchain : Blueprint for a new economy*. " O'Reilly Media, Inc.".

Selon Stephan Tual, cofondateur de Stock.it, « il s'agit d'une organisation incorruptible qui appartient aux personnes qui ont aidé à la créer, à la financer, et dont les règles sont publiques. Il n'y a donc pas besoin de faire confiance à qui que ce soit, tout étant dans le code, auditable par chacun. »

Concrètement, comme le Bitcoin « réinvente » le marché des transferts de fonds en le rendant plus efficient, les DAOs pourraient avoir le même impact sur les entreprises. Une entreprise qui s'établit doit remplir des obligation d'enregistrement à la BCE (Banque Carrefour de Entreprises), contracter des assurances pour couvrir sa responsabilité civile, occuper des locaux, payer des taxes et cotisations.

Ces procédures, ou du moins certaines d'entre elles, pourraient selon moi être optimisées en intégrant la blockchain pour être rendues plus efficientes ou même éliminées. Les organisations pourraient aussi s'émanciper des limites territoriales et juridiques liées à un Etat, une région ou un accord commercial. Les « smart contracts » peuvent prévoir l'intervention d'une partie prenante assurant la conformité aux règles nationales ou supranationales : Etat, gouvernement, région.

Grâce aux DAOs, les entreprises seraient avant tout globales, universelles en premier lieu et pourraient être rattachées à une juridiction désignée quand le cadre juridique de l'utilisation de la blockchain sera déterminé…

La blockchain : voie vers l'intelligence artificielle

Les « smart contracts » sont conçus pour être toujours plus complexes et autonomes. Les Dapps et DAOs offrent des possibilités intéressantes vers des comportements très proches de ceux de l'Intelligence Artificielle (IA).

On pourrait intégrer dans la blockchain de simples systèmes de comportements « if-this-then-that » (IFTTT) afin de créer des agents capables de gérer certaines situations du quotidien ou agir en binôme d'un être humain.

Si l'on couple Ethereum et AI, il serait possible de créer de la vie artificielle. En effet, en couplant des agents IA à des DAOs, on arriverait à créer des entreprises sophistiquées et totalement autonomes telles que des banques par exemple. On imaginerait même l'agent IA créer un nouveau « smart contract » quand le précédent deviendrait obsolète afin qu'il soit mieux adapté.

Il est très difficile de définir l'IA : on pourrait la qualifier comme « un algorithme qui apprend à prendre des décisions à partir d'expériences. »[33] Les algorithmes d'IA ont besoin de s'entrainer pour évoluer, d'apprendre de leurs propres expériences, au contact de bases de données. L'un des enjeux de l'IA est donc de constituer des bases de données fiables et de qualité. A l'instar de Facebook ou Google qui, non seulement utilisent gratuitement les données de leurs utilisateurs, mais aussi contrôlent leur qualité via les « likes » et partages.

Contrairement à ces deux géants, leurs concurrents doivent payer pour accéder à des bases de données de qualité et garantir le bon usage éthique de celles-ci. A mon sens, la blockchain semble représenter une opportunité pour l'IA dans le sens où elle permet cet échange d'informations et de moyens de manière autonome et sécurisée. En effet, les « smart contracts » permettent cette honnêteté et cette absence de frais de transactions.

Il apparaît qu'AI et blockchain souffrent du même défaut : leur manque de reconnaissance (ou plutôt une certaine méconnaissance) et leur jeunesse. Ces deux technologies sont disruptives et peuvent être assimilées à un danger par les populations. (Pertes d'emplois, défi technologique, gestion du changement). C'est pourquoi elles devraient évoluer ensemble.

Grâce à l'IoT, les machines, objets et humains communiquent ensemble, et ce de manière indifférenciée… Qu'advient-il alors des échanges sociaux ?

6.3.3 Applications au secteur Bancassurance.

Concernant le secteur des Assurances.

C'est un des premiers secteurs à avoir marqué son intérêt pour la blockchain. Des acteurs tels que AXA, Allianz, Lloys ont très rapidement lancé des recherches dans ce domaine afin de trouver quelles applications étaient réalisables.

Un exemple d'application concerne les assurances voyage. Il apparaît qu'un grand nombre (environ 60%) de voyageurs assurés contre le retard de leur vol ne réclament jamais une indemnisation le cas

[33] Damien ERNST – "L'intelligence artificielle avec Damien Ernst de l'Ulg", Radio RCF (31 mars 2017)

échéant. Alors, pourquoi ne pas systématiser l'indemnisation de ces passagers via un « smart contract » encodé dans la blockchain ?

C'est ce que propose la plateforme Etherisc[34], via le service d'un oracle – un oracle est ce qu'on appelle un SGBD (Système de Gestion de Base de Données) qui donne accès de manière sécurisée aux données du web et gère les données des « smart contracts » pour déterminer si les conditions sont bien remplies – en l'occurrence Oraclize[35]. Cette plateforme propose le développement de Dapps permettant d'indemniser automatiquement ces voyageurs mis en retard involontairement. Cette application décentralisée permet aux entreprises qui l'utilise de rendre la vente d'assurance plus efficiente, engendrer des couts opérationnels moindres et créer une relation de confiance avec leurs clients en leur fournissant une plus grande transparence comparativement aux opérations d'assurance traditionnellement plus opaques (détermination des responsabilités, valorisation, taux d'indemnisation).

Le rôle de la blockchain est de créer de la confiance et de la sécurité pour automatiser les déclarations de sinistre sans avoir recours à un tiers.

Un autre champ d'application dans les produits d'assurance, que l'on a déjà évoqué plus haut dans ce travail, est celui des assurances de dommages dites indicielles. Celles-ci sont liées à un indice, un paramètre de référence tel que la température ou le niveau de pluviométrie.

Le « smart contract » conclu entre assureur et agriculteur stipulera que passé un certain niveau de sècheresse ou de pluie, l'indemnisation aura automatiquement lieu. Cette décision sera prise sur base d'un accès fiable à des données certifiées correctes, par exemple l'IRM (Institut Royal de Météorologie). Cela permettra aux oracles de déclencher le paiement sans l'intervention couteuse d'un expert ou la déclaration du sinistre par l'assuré (couteuse en temps).

La blockchain rend le processus de décision fiable, efficient, automatique, libre de tout jugement subjectif et moins couteux structurellement.

Il me semble que si l'on pousse le raisonnement encore plus loin, on pourrait même aller jusqu'à coupler ces assurances à des DAOs (Decentralized Autonomous Organizations). Ainsi, si l'on s'inscrit dans la logique des « Communaux Collaboratifs » développée par Jeremy Rifkin dans son ouvrage

[34] URL : https://etherisc.com/#hero
[35] URL : http://www.oraclize.it/

« La Société du Cout Marginal Zéro » (2014), on imaginerait un groupe d'assurés rassemblés dans une organisation sans unité centrale de contrôle, ainsi gouvernés par eux-mêmes. Dans cette configuration, les risques seraient mutualisés, les primes seraient capitalisées et serviraient à indemniser les sinistres déclarés ! les couts d'organisation et d'infrastructure étant réduits à leur plus simple expression, on envisagerait que les capitaux non utilisés en fin de période seraient reversés au assurés sociétaires…

J'ai pu identifier quelques initiatives d'assurances pair-à-pair de ce genre dans des pays frontaliers à la Belgique. En Allemagne avec Friendsurance (https://www.friendsurance.com/), au Royaume-Uni avec Heyguevara ou en France avec Inspeer.me, des plateformes proposent des assurances d'affilié à affilié. Sans intermédiaire !

Ce paradigme collaboratif déplace évidemment le pouvoir de décision du tiers vers l'assuré, un système de vote pouvant être mis en place pour décider de l'indemnisation ou non. Cependant cette prérogative soulève clairement le problème de régulation de cette activité, les contrats ne souffrant plus de restrictions de territorialité ou d'exclusivité. Le code exécute les conditions prédéterminées et donc constitue le pouvoir décisionnel. Alors, comment déterminer qui est légalement responsable du code contenu dans les DAO ? Il est clair que voilà une problématique qu'il est trop tôt à l'heure actuelle de pouvoir fixer au niveau législatif.

Concernant le secteur bancaire

Les grands acteurs bancaires aujourd'hui ne sont pas seulement des banques, on les appelle des entreprises de « Bancassurance ». C'est-à-dire qu'ils commercialisent aussi bien des produits bancaires que des produits d'assurance vie, décès et IARD. Vu l'intérêt des assureurs pour la blockchain, c'est tout logiquement que les banques se sont rapidement tournées vers cette technologie disruptive.

Les banques connaissent, comme nombre d'autres secteurs, un phénomène de concentration, les plus gros acteurs rachètent les plus petits et certains fusionnent entre eux. Cette dynamique fait des banques des entreprises très volumineuses, très structurées, hiérarchisées et standardisées. Mais surtout, centralisées. Ces mégastructures ne seraient-elles pas ubérisables ?

D'autre part, des scandales financiers tels que la crise des Subprimes en 2008, celle du Libor, ou encore les Panama Papers concernant l'évasion fiscale des grands groupes bancaires mondiaux, sont régulièrement révélés. Par conséquent, l'image que reflètent ces institutions est ternie et la confiance que les clients leur accordent s'en voit détériorée.

Selon David François, Chief Technical Officer de la plateforme bitcoin Paymium : « Un des grands avantages de la blockchain Bitcoin réside dans le fait qu'il n'existe aucune barrière à l'entrée : n'importe qui peut créer un service qui fonctionne sur la blockchain. En particulier, n'importe qui, moyennant un capital confiance, peut créer une banque en bitcoin qui accepte les dépôts des clients et émet des crédits en bitcoins. C'est en ce sens que le bitcoin peut challenger la banque sur l'activité de crédit, en faisant tomber cette barrière à l'entrée. (…) Les acteurs qui réussiront le mieux seront ceux qui auront réussi à générer un capital confiance très important et à capitaliser dessus. »

D'autre part, les frais d'intermédiation basés sur le protocole bitcoin sont très faibles. Contrairement aux frais bancaires classiques.

Le problème de l'activité crédit dans le secteur bancaire réside dans le fait qu'elle est très fortement règlementée. Cette réglementation représente quant à elle une importante barrière à l'entrée. C'est pourquoi il me semble que le développement du bitcoin devrait en premier lieu se faire dans les pays en voie de développement. Pays dans lesquels la monnaie nationales est mal maitrisée et peut-être moins liquide. Elle peut alors représenter une valeur refuge comme ce fut aussi le cas en Grèce au bord de la faillite récemment.

D'autre part, lorsque l'on parle de se passer d'intermédiaires pour conduire des transactions monétaires, je pense aux transferts d'argent initiés par les travailleurs émigrés vers leurs familles restées dans leur pays d'origine. Ces transferts de cash, pris en charge par des intermédiaires tels que 'Western Union' sont frappés de frais qui peuvent varier entre 10% et 20% en fonction des pays concernés. La blockchain permet de réduire drastiquement ces frais pour qu'ils ne représentent plus que quelques centimes. De plus, là où il faut normalement plusieurs jours pour que les fonds soient disponibles à l'arrivée, la blockchain permet de réduire ce laps de temps à quelques minutes.

Cette proposition semble idéale. Cependant, à ce stade-ci du développement de cette technologie, les frais liés au change en BTC des monnaies au départ et à l'arrivée et la volatilité de cette crypto-monnaie qu'il faudrait couvrir par une assurance, sont des frais qui annihilent tant que maintenant la compétitivité de cette solution prometteuse.

Plus globalement, les banques connaissent un phénomène de digitalisation sans précédent depuis quelques années. C'est dans cette logique que l'on voit apparaître un nombre toujours plus important de 'FinTech' (technologie financière) – ces start-up qui ont pour but de numériser divers métiers au sein de la banque traditionnelle. Ce rouleau compresseur digital représente un challenge prioritaire

pour les banques généralistes car ces nouvelles techniques attirent l'attention et les investisseurs. Cette visibilité incite la législation à s'adapter rapidement afin de permettre à ces nouveaux acteurs de croitre plus aisément. C'est dans cette dynamique que les FinTech Blockchain s'inscrivent et ainsi menacent les acteurs traditionnels qui s'adaptent plus lentement !

L'exemple du consortium R3 CEV[36] :

R3 est une société qui fournit des logiciels d'entreprise. Elle travaille actuellement avec plus de cent acteurs bancaires, institutions financières et régulateurs. Partant du principe que les institutions financières ont des technologies de plateformes financières différentes et de génération différente qui ont beaucoup de mal à interagir et qui causent des inefficiences, du risque et des couts importants, ils ont mis en évidence l'utilisation d'un registre distribué grâce à son effet de réseau afin de créer le plus grand groupe collaboratif dans le secteur financier. Leur ambition est de mettre en place une nouvelle forme de compensation interbancaire via un registre distribué qui remplacerait à terme le réseau SWIFT que l'on connaît actuellement. Le résultat des recherches qu'ils ont effectuées pendant 2 ans : CORDA[37], une plateforme qui permet, dans n'importe quel scénario commercial d'échanger sans le besoin d'une autorité centrale.

L'exemple du Ripple Transaction Protocol (RTXP)[38]

Il s'agit d'un système de règlement en temps réel, un réseau d'envoi de fonds basé sur la blockchain Ripple. Il vise à permettre des transactions financières mondiales et sécurisées via un registre de consensus distribué. Son atout est qu'il prend en charge n'importe quelle crypto-monnaie ou monnaie fiduciaire. Parmi les validateurs de cette blockchain on retrouve notamment le MIT (Massachusetts Institute of Technology). Le protocole Ripple est de plus en plus accepté par les banques (dont UBS ou Santander) comme infrastructure de paiement.

On pourrait croire que la blockchain représente un moyen de substitution aux banques traditionnelles : une autorité centrale, cet intermédiaire bancaire, pourrait en effet devenir obsolète. Il me semble que

[36] https://www.r3.com/
[37] https://www.corda.net/
[38] http://blogchaincafe.com/ripple-http-pour-largent

cette technologie représente une opportunité plutôt qu'une menace ! En s'appropriant la blockchain pour l'adapter aux services et systèmes actuels, les banques peuvent faire levier sur la gestion de leurs données, rester « compliant » (en conformité) en toutes circonstances et réduire leurs couts opérationnels. Cela se fera, pour moi, via une blockchain privée permissionnaire ou hybride plutôt qu'un registre totalement distribué publiquement.

Les banques ne restent donc pas les bras croisés. En 2015, un consortium composé des neuf plus grandes banques de Wallstreet s'est formé dans le but de développer l'utilisation de la blockchain dans le secteur financier. Un des projets phare est le remplacement du standard SWIFT pour certifier les transactions[39].

Finalement, les sources de revenus dans le secteur bancaire ont été bouleversées par une structure de taux continuellement bas. La marge sur les crédits octroyés est fortement réduite, les dépôts des clients ne rapportent pas et les dépôts des banques à la BCE (Banque Centrale Européenne) se font à un taux négatif ! Avec cette tension sur les marges, les banques cherchent de nouvelles sources de revenus, notamment en convertissant les dépôts en investissements mobiliers et en se concentrant sur les segments Retail les plus rentables comme par exemple les clients professionnels. Un autre moyen d'augmenter la profitabilité de l'organisation est d'agir sur les couts. C'est là que, pour moi, la blockchain a un rôle à jouer.

Les marchés financiers (via le courtage notamment) offrent encore des revenus intéressants aux banques. Il s'agit aussi d'un domaine dans lequel la technologie du registre distribué peut intervenir à bon escient. Je pense notamment à des cas de produits dérivés comme des contrats Forward ou des Options utilisés comme couverture contre le risque de change. Selon D. Yermack[40], à l'image de l'utilisation des matières premières comme outil de diversification et donc réduction du risque systématique dans la gestion de portefeuilles d'actifs financiers, comme l'or et le Bitcoin, sont dé-corrélés (-0,088), le Bitcoin pourrait être utilisé dans le même sens !

[39] Ribeiro, A. (2016). La Blockchain et ses potentielles applications.
[40] Yermack, D. (2013). *Is Bitcoin a real currency? An economic appraisal* (No. w19747). National Bureau of Economic Research.

6.3.4 Applications au secteur de l'Agroalimentaire et du Transport maritime

J'ai choisi d'aborder l'application de la blockchain dans ces deux secteurs car il me semble qu'elle est la plus probante en terme d'impact sur ces activités.

Concernant l'Agroalimentaire

Dans le secteur de l'agroalimentaire, des scandales sont fréquemment mis à jour lorsqu'il s'agit de traçabilité. Que ce soit en Europe ou aux Etats-Unis, ils se sont multipliés ces dernières années. On peut ainsi énoncer : en 2008, le cas du lait frelaté en provenance de Chine ; en 2013, le cas de la viande de cheval : plus de quatre millions de plats censés contenir du bœuf contenaient en fait de la viande de cheval ; en 2015, le cas des restaurants Chipotle aux Etats-Unis en cause dans une contamination à la bactérie E.coli ; en 2017 : le cas des œufs au Fipronil. Autant d'exemple qui nous montrent de sérieuses lacunes dans le contrôle et la traçabilité des produits/aliments commercialisés.

Il semble que la blockchain pourra aider à « renforcer la transparence et accélérer l'identification de la source des contaminations »[41].

En tant que technologie distribuée et totalement transparente, la blockchain permettrait aux différents intervenants d'une chaine logistique d'enregistrer leur intervention et d'instaurer une traçabilité tout au long du processus – de la fabrication du produit jusqu'à sa vente - et en temps réel. Le caractère distribué et inaltérable unilatéralement de la blockchain permet de garantir au cycle de vie du produit une fiabilité digne de confiance.

Concrètement, les différentes étapes du processus pourraient être enregistrées dans le registre via une plateforme dédicacée (i.e Azure), via le scan de QR codes ou même, grâce à l'Internet des objets, via des senseurs connectés.

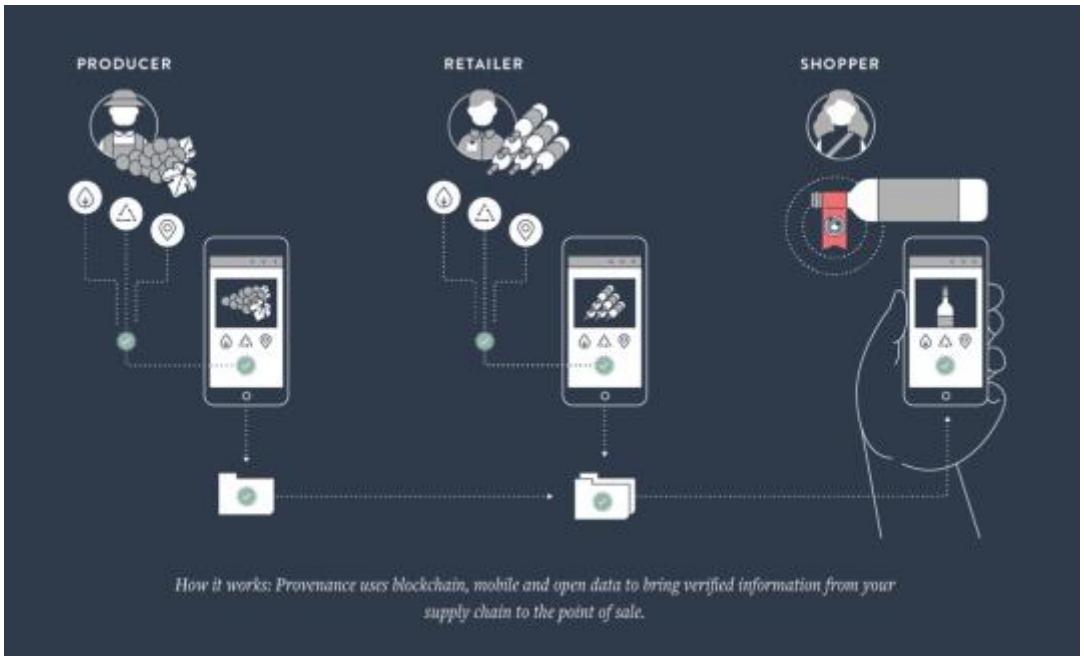
En 2016, dans leur ouvrage « Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance », Henry M. Kim et Marek Laskowski posent une contribution spécifique. Ils ont codé et testé sur la blockchain Ethereum des « smarts contracts » qui ont pu répondre à des contraintes de traçabilité déterminées en amont.

[41] Supply Chain, Traçabilité & Blockchain (2016). Blockchain Partner

Voici deux exemples d'applications permettant d'améliorer la traçabilité sur la chaine logistique :

Provenance.org est une plateforme qui permet à ses clients aussi bien professionnels que privés de suivre le cheminement des articles qu'ils produisent où qu'ils achètent. Elle garantit une totale transparence entre la production et l'achat (cfr schéma ci-dessous). A chaque produit est attribué un passeport digital afin d'authentifier les informations clés, éviter les plaintes abusives et combattre les contrefaçons.

Cette méthode peut permettre de créer du capital confiance vis à vis des clients et ainsi renforcer leur image de marque pour générer de la croissance. De plus, l'interopérabilité de la technologie blockchain permet de créer une continuité entre les différents intervenants qui peuvent améliorer leurs processus et ainsi faire des économies structurelles sur les procédures de traçabilité. Le registre étant inaltérable, il confère une sécurité aux données enregistrées. Le contrôle est automatisé…



Printscreen 2 : Schéma Provenance.org[42]

[42] URL : https://www.provenance.org/how-it-works

Skuchain[43] est un acteur de l'écosystème blockchain qui fournit aux entreprises une solution de gestion des stocks dans le but d'éliminer la complexité et les couts engendrés par cette tâche, le tout en promouvant les principes du commerce collaboratif.
Grâce à leur plateforme BRACKETS® pour la gouvernance et l'exécution de « smart contracts », les organisations ont la possibilité de placer sur une blockchain privé l'entièreté de leur chaine logistique. Cela leur permet de tracer en temps réel les items en transit et d'interagir avec les intervenants dans le processus logistique.

Chaque intervenant ayant reçu l'autorisation d'accéder à la blockchain peut consulter ou ajouter une information à n'importe quel moment. Grâce à ce suivi, il est possible de détecter en temps réel où et quand une éventuelle fraude est commise. Il en résulte que les délais d'intervention des autorités concernées peuvent être réduits drastiquement, limitant ainsi le risque de propagation en cas de contamination.
Il me semble que la portée de l'application de cette technologie dans le secteur de l'agroalimentaire peut aller au-delà de la traçabilité sanitaire. En effet, les modes de consommation changent vers une meilleure considération des modes de production, du bien-être animal ou l'empreinte écologique, ces comportements assimilés à la tendance « bio ». La blockchain m'apparait être un « enabler » de croissance pour ces entreprises dont la stratégie est basée sur l'éthique et la transparence des processus énoncés ci-dessus.
Cependant, pour que ces objectifs soient atteints, il faudra que l'entièreté des intervenants utilisent cette technologie. Si l'un d'entre eux est réticent, c'est toute la chaine qui est remise en cause. Se pose donc le problème d'adoption de masse de cette technologie de rupture et des couts engendrés par la numérisation de la chaine logistique.

[43] URL : http://www.skuchain.com/

Concernant le transport maritime

Dans les années 1950, un américain, Malcom McLean, lance un nouveau moyen de transporter des marchandises qui va bouleverser le monde, en tout cas celui du transport multimodal : le container. Cette invention a permis de développer le commerce international et réduire les couts de transport de manière conséquente.

Dans le domaine du transport maritime, cela a aussi permis à certains ports de se développer pour accueillir et transiter des marchandises venant du monde entier. De la même manière que le container a permis de faciliter et accélérer le transport, ici aussi, l'utilisation de la blockchain représente une nouvelle étape marquante pour moderniser le transport maritime.

C'est ainsi que le port de Rotterdam, le premier port d'Europe a développé des applications blockchain pour le fret maritime. Le projet intègre une quinzaine d'entreprises et institutions néerlandaises regroupées dans un consortium visant à intégrer cette technologie dans la chaine logistique.

D'autre part, le géant Maersk, armateur danois, a lancé début 2017 un projet basé sur le blockchain Hyperledger Fabric pour la numérisation de l'entièreté de sa chaine d'approvisionnement. En inscrivant de manière transparente et inviolable les containers dans le registre distribué, il les rend traçables en temps réel, et permet de contrôler les interventions des parties prenantes aux différentes étapes du transport : expéditeurs, douanes, transitaires, ports, …

Concrètement, les démarches administratives liées au transport maritime se font traditionnellement sous format papier et sont lourdes et chronophages. De plus, les possibilités d'erreurs liées à l'intervention humaine sont nombreuses (mauvaise transcription, mauvaise compréhension, perte, altération des données). En créant une blockchain privée accessible uniquement aux intervenants, on peut numériser ces documents et les sécuriser par des clés cryptographiques. L'empreinte numérique du document étant codée dans la blockchain, elle est accessible à tout moment, son statut évolue au fur et à mesure des interventions et reste inaltérable car crypté et distribué.

En outre, pour faire le lien avec les denrées alimentaires, l'utilisation de capteurs tels que des puces NFC ou RFID permettent de contrôler les conditions de transport (humidité, niveau de CO2), l'état

des marchandises et de localiser le container tout au long du processus.[44]

Au final, l'intégration de cette technologie dans le transport maritime devrait permettre de réduire les fraudes, les erreurs et améliorer, accélérer le transit des containers (immobilisation en cas de problème avec les documents de transport). Sans compter les économies structurelles pour les organisations. Sachant que le transport maritime représente 90% du transport mondial et que les couts de traitements documentaires et d'administration valent pour un cinquième des couts de fret, l'enjeu me paraît être de taille !

Pour conclure concernant l'application de la blockchain dans la gestion de la chaine logistique dans l'agroalimentaire et le transport maritime, je dirais qu'il s'agit là de secteurs encore très dépendants de procédures papier. Ce type de fonctionnement est source d'inefficiences, d'erreurs et même de fraudes – souvent dans le but de maximiser les profits dans le chef des entrepreneurs ! En numérisant ces différentes chaines d'approvisionnement, la blockchain permet de réduire ces inefficiences. La clé sera de garantir le lien entre le monde virtuel du registre et le monde réel des marchandises et containers, ce lien se faisant via des capteurs bénéficiant de l'IoT.

La blockchain n'est pas un outil miracle qui fera disparaître totalement les scandales liés aux problèmes de traçabilité des denrées diverses mais tendra à les réduire considérablement. De plus, les entreprises qui utiliseront cette technologie pourront mettre en avant une certaine transparence et intégrité qui feront levier sur la confiance des clients et la mettront en ligne avec les tendances du « mieux consommer ».

6.3.5 Application au secteur de la Santé

Lorsque l'on parle de « mieux consommer », un secteur dans lequel il y a aussi un rôle à jouer pour la blockchain est celui de la santé. En effet, le développement de cette infrastructure dans le secteur de la santé peut prendre plusieurs visages.

Premièrement, la traçabilité des médicaments. L'OMS (Organisation Mondiale de la Santé) estime à environ 700.000 le nombre de décès dus à l'ingestion de médicaments contrefaits. A l'image de ce qui

[44] Supply Chain, Traçabilité & Blockchain (2016). Blockchain Partner

se développe dans le secteur de l'agroalimentaire, on pourrait imaginer un système transversal garantissant la traçabilité des médicaments. La propriété distribuée du registre blockchain permettrait aux entreprises pharmaceutiques, aux organes de contrôle et même aux patients d'accéder à une base de données unifiée qui échapperait ainsi au contrôle central et exclusif d'une seule entité.

Deuxièmement, ce même principe d'authentification pourrait s'appliquer aux données médicales des patients. En sécurisant davantage les dossiers médicaux sur la blockchain, toute mise à jour se ferait sans qu'il soit nécessaire de télécharger les documents sur un serveur central.

Troisièmement, une application qui me semble constituer une totale rupture avec ce qui se pratique actuellement et qui aurait le plus d'impact sur la gestion des données médicales est la réappropriation de ces données par les patients. En gardant le contrôle de son dossier médical, le patient peut en donner l'accès à qui il souhaite : un hôpital, du personnel soignant, un médecin de famille. Il pourrait aussi décider que l'ouverture dudit dossier ne serait possible que par la fourniture de plusieurs clés privées, par exemple celle du médecin, du conjoint et de l'hôpital (utile en cas de malaise ou d'inconscience).

On peut ensuite aisément imaginer, via l'intégration d'un « smart contract », que le paiement de prestation se ferait tout au long du parcours médical ou hospitalier d'un patient.

Les applications que nous avons abordées ne sont pas exhaustives. Les crypto-monnaies et la blockchain peuvent avoir un impact dans de nombreux autres domaines. Nous avons énuméré les avantages de l'infrastructure blockchain et son caractère disruptif. Néanmoins, ces applications soulèvent de nombreuses questions d'aspects juridique, éthique ou politique.

VII Les limites, les défis, les enjeux juridiques, éthiques et pour la blockchain

Comme nous avons pu le découvrir précédemment, la blockchain offre de nombreuses opportunités et semble promise à un avenir prometteur tant le champ d'application semble large. Néanmoins, l'utilisation de cette nouvelle technologie comporte un certain nombre de risques. Notamment parce que son champ d'application est vaste ! La blockchain pose donc de nombreuses questions sur le plan juridique, politique et surtout éthique.

7.1 Les risques et limites de la blockchain Bitcoin et autres

L'une des caractéristiques principales du Bitcoin est qu'il garantit aux utilisateurs un anonymat total. Il apparaît que cet anonymat est tout relatif. En effet, la blockchain se veut être un registre transparent et distribué ce qui veut dire que n'importe qui peut à n'importe quel moment connaître vos dernières transactions et le solde de votre compte si, par exemple, votre identité est connue lors d'une opération d'achat.

Le Bitcoin est une crypto-monnaie très jeune. Cela implique qu'elle est très volatile. En effet, le cours du BTC varie fortement depuis sa création ce qui le rend peu fiable. Cette crypto-monnaie n'est pas utilisée (ou très peu) pour acheter des biens et des services mais plutôt pour être échangée contre des monnaies réelles. Cela soulève deux problématiques : l'investissement dans l'économie réelle et le blanchiment d'argent.

D'autre part, puisque sa masse monétaire est encore faible, le bitcoin souffre, à l'image des marchés financiers des pays en développement, d'un manque criant de liquidité, contrairement aux marchés traditionnels.

Une autre limite qui, selon moi, pose un défi de taille pour l'avenir est le nombre limité de transactions qu'autorise la blockchain Bitcoin (le standard) par seconde. Le seuil est fixé à 7 opérations alors que les systèmes traditionnels autorisent des milliers de transaction à la seconde. Le réseau VISA par exemple permet 2000 opérations à la seconde[45]. Twitter, jusque 15.000 opérations[46]. La différence est plus que considérable ! De plus, il y a une certaine latence entre le moment d'encodage de la transaction et la confirmation. Pour une sécurité suffisante, il faudrait attendre environ une heure (ceci afin d'éliminer le risque de double dépense), quand le réseau VISA ne prend que quelques secondes au maximum.

Finalement, le talon d'Achille du bitcoin est sans doute l'écosystème autour de ce protocole. En effet, la blockchain, de par son caractère inaltérable, est sécurisée et normalement inattaquable, mais pas les intermédiaires qui gravitent autour et fournissent des services basés sur cette dernière ! Ceux-ci sont vulnérables et cela s'est vérifié notamment à deux reprises avec les cas MT Gox et Bitfinex[47].

[45] Blockchain France Associés (Mai 2016). La Blockchain décryptée. Les clefs d'une révolution
[46] Swan, M. (2015). *Blockchain : Blueprint for a new economy*. " O'Reilly Media, Inc.". (pp 82)
[47] Ribeiro, A. (2016). La Blockchain et ses potentielles applications.

MT Gox était le plus important marché d'échange de BTC en devises réelles. Sa faillite fut prononcée en février 2014 lorsque 650.000 BTC ont disparu. Contre-valeur en USD à ce moment : 384.104.500 millions. On ne sait toujours pas si cette plateforme fut hackée, si les pirates ont dérobé ces fonds ou si c'est son CEO, Mark Karpelès, qui les a subtilisés ? Plus récemment, en 2016, la plateforme Bitfinex, un autre marché de change de bitcoins en monnaies traditionnelles s'est fait hacker 119.756 BTC pour une contre-valeur de marché en UDS de 66 millions.

Ces problèmes se posent dans l'utilisation de blockchains publiques. Comme je l'ai annoncé plus tôt dans ce travail, je préconise l'utilisation de blockchains privées ou hybrides dans l'environnement de l'entreprise afin de limiter les intervenants anonymes. Les décisions concernant la sécurité et le contrôle seraient prises par la personne morale qui gèrerait la gouvernance et engagerait sa responsabilité. C'est là que l'opportunité se trouve pour l'utilisation de cette technologie !

La gouvernance me paraît aussi être une des limites de la blockchain, notamment dans le cadre des DAOs. Ces organisations qui permettent aux individus de se coordonner de manière décentralisée sont capables de générer et de gérer les ressources nécessaires à leur fonctionnement en toute autonomie. En s'affranchissant des intermédiaires, et donc des tiers de confiance, pourquoi ne se passeraient-elles pas non plus de leurs administrateurs ? Cette force semble être la prochaine étape dans la conception d'une organisation décentralisée et désintermédiée. Cette étape permet de mettre en exergue les besoins cruciaux d'un cadre juridique pour règlementer les blockchains.

7.2 Les enjeux juridiques

A l'heure actuelle, les règlementations concernant le bitcoin sont très variables en fonctions des pays concernés. Il n'existe aucun accord entre eux pour cadrer légalement l'utilisation de cette crypto-monnaie. La nature juridique du bitcoin n'est pas uniformément tranchée.

Un des enjeux majeurs de la blockchain est celui du statut juridique des crypto-monnaies (Bitcoin, Ether), c'est à dire les tokens. En fonction des législations, cet actif est considéré comme une monnaie à part entière, comme un actif financier ou un bien meuble ! Ainsi, en Allemagne il est considéré comme une monnaie, avec les conséquences juridiques qui en découle. Par contre au niveau fiscal, il est considéré comme un revenu d'actif mobilier et donc frappé de précompte. En France, il n'est pas qualifié juridiquement et est donc considéré comme un bien meuble. En réalité il existe un flou

juridique actuellement autour des crypto-monnaies avec des différences marquantes même pour des pays limitrophes. Certains bannissent même l'utilisation des crypto-monnaies par les entreprises sur leur sol. Tel a été la décision prise par la Chine en 2017 par exemple. Alors que l'essence même d'une crypto-monnaie est de tomber les frontières territoriales, aucune cohésion juridique globale n'existe. Il apparaît fondamental d'harmoniser les législations supranationales et créer une autorité globalisée à l'image de l'ADN de cette technologie.

Si on considère que ces tokens ont une valeur, alors les échanges de tokens entrainent un transfert de valeur. Cela soulève un problème de responsabilité dans le cas où une des parties est lésée, notamment dans le cadre de blockchains publiques.

Dans le secteur financier, les banques sont obligées de respecter des directives européennes visant à empêcher le blanchiment d'argent et le financement du terrorisme. Elles doivent identifier formellement tous leurs clients (KYC – Know Your Customer). Comme c'est le cas notamment pour les représentants de personnes morales. Cela pose un défi de taille ! Dans la mesure où les crypto-monnaies seraient intégrées dans un schéma bancaire traditionnel, comment identifier les détenteurs de bitcoins par exemple ?

Imaginons que les crypto-monnaies soient considérées comme des outils d'investissements financiers, dans quelle catégorie les classer ? comment les intégrer dans la réglementation MIFID[48]?

D'autre part, concernant les DAOs, comment déterminer la responsabilité d'une telle organisation, dont les activités seraient illicites, sans administrateur ou du moins identifiable ? On aurait tendance à vouloir porter cette responsabilité aux créateurs du logiciel, pour autant qu'ils ne soient pas anonymes. Et, quand bien même nous les trouverions, comment arrêter les méfaits commis par une organisation qui agit de manière autonome et indépendante ?

Vu cette autosuffisance, il me semble que la régulation devrait intervenir avant la mise en force des « smart contracts ». Mais, comment anticiper, préjuger d'une éventuelle sortie du cadre juridique ? - Cela me fait penser à la fiction de Philip K. Dick : Minority Report (1956). Fiction dans laquelle, dans un monde futuriste, les policiers pouvaient, grâce aux dons de préscience de trois mutants, intervenir et empêcher les crimes avant qu'ils ne soient commis… - Concrètement, j'imagine la création d'une nouvelle fonction : Auditeur de « smart contracts ». Sorte de contrôleur qui vérifie que ce logiciel

[48] URL: https://www.fsma.be/fr/regles-de-conduite-mifid/

reprend bien les instructions initialement prévues, est configuré correctement et cadre avec l'environnement légal.

Vu le potentiel de la blockchain, appliquer des règles juridiques traditionnelles à cette technologie de rupture me paraît incohérent voire impossible. Cela en limiterait le potentiel ou la portée. Un nouveau cadre juridique globalisé est à créer pour cet environnement sachant que nous ne savons pas aujourd'hui où cette technologie nous mènera et quelle ampleur son champ d'application prendra !

La volonté pieuse de la blockchain Bitcoin était d'échapper à toute régulation, à toute dépendance étatique, dans son enthousiasme libertarien. Les autres blockchains (je pense notamment à Ethereum et son champ applicatif lié au monde de l'entreprise) ont un intérêt certain à cadrer légalement (mais surtout justement) leurs activités pour pouvoir inciter davantage à la création d'un écosystème fourni autour du protocole et aider à son adoption de masse. La régulation trop rigoureuse de cette technologie entrainerait ses utilisateurs et créateurs dans un cercle vicieux visant à la rendre encore plus libertaire afin de s'émanciper de ces contraintes règlementaires. Ce cadre légal doit être progressif, flexible et évoluer en même temps que la blockchain se développe. Il en va de même pour l'Intelligence Artificielle.

Les décisions prises aujourd'hui définiront le futur de la blockchain et par extrapolation la manière dont la société en général s'émancipera…

Selon Jérôme Giusti, Avocat fondateur du cabinet "11.100.34. Avocats Associés", spécialiste en droit des nouvelles technologies, on peut imaginer trois domaines juridiques impactables par la blockchain :

- ⇒ Le droit de la preuve, qui peut être complètement modifié
- ⇒ Tout ce qui relève de la notarisation et du tiers de confiance. Cela peut impacter le formalisme juridique, notamment tout ce qui est contractuel, puisque le droit impose aujourd'hui, dans bien des cas, des contrats écrits, signés, avec des clauses qui doivent être démontrées par écrit ;
- ⇒ Tout ce qui relève de l'exécution automatique de clauses contractuelles[49].

Pour conclure sur les enjeux juridiques, je dirais qu'il est encore tôt pour émettre des règles établies et imposer un cadre juridique strict. L'usage de la blockchain est encore limité. Cette technologie devra être règlementée lorsque l'usage sera assez répandu. Les secteurs technologiques et juridiques doivent selon moi progresser conjointement afin d'être cohérents tout au long du processus d'acceptation et

[49] Blockchain France Associés (Mai 2016). La Blockchain décryptée. Les clefs d'une révolution

d'implémentation. Il ne doit pas s'agir de « tuer la blockchain dans l'œuf ». Selon Giusti, il s'agit aussi d'un enjeu générationnel : « Les gens qui sortent des écoles d'avocat et des facultés de droit n'ont pas encore assimilé la technologie dans leur pratique, et c'est un vrai problème. A l'inverse les jeunes diplômés en licence commencent, pour certains, à avoir cette compétence. La nouvelle génération semble donc aller dans le bon sens à ce niveau-là. Cela nécessite en tout cas une vraie volonté de la part des juristes d'intégrer des compétences qu'ils n'ont pas, en le faisant soit personnellement, soit en intégrant dans leur cabinet ou leur équipe des profils techniques comme nous l'avons fait chez nous, et de se poser la question de savoir comment leur métier va évoluer dans les 20 ans à venir. »

Une initiative a été lancée par l'Etat de New York : la « BitLicense » (B. Lawsky, 2015). Cette licence a pour but de réguler l'utilisation des crypto-monnaies dans cet Etat en enregistrant les données de ces utilisateurs durant dix ans ! le problème est que cela impacte ceux qui doivent obtenir cette licence (entreprises concernées par les crypto-monnaies) mais aussi ceux qui n'en n'ont pas besoin (détenteurs de crypto-monnaies). Le texte de loi est tellement vaste qu'il est finalement inapplicable dans la pratique ! L'industrie Bitcoin s'inquiète d'ailleurs du langage très vaste, large portée et extraterritorial utilisé dans ce texte. Peu de temps après avoir créé la « BitLicense » Benjamin Lawsky s'est retiré du gouvernement pour créer une entreprise de conseil aux sociétés bitcoin qui sont dans un processus de demande de « BitLicense ». Il a construit un mur autour du bitcoin et son écosystème naissant puis s'est installé à la porte en faisant payer les gens qui souhaitaient y entrer ! Illustration du capitalisme de connivence !

Cela confirme que technique et jurisprudence doivent évoluer en parallèle… Et soulève la dimension éthique de l'utilisation du bitcoin.

7.4 Les enjeux éthiques

Une des plus importantes barrières à l'adoption générale de la technologie blockchain est clairement son lien avec le Darknet pour le blanchiment d'argent, le trafic de drogue, d'armes ou encore d'êtres humains. La médiatisation autour de la plateforme Silk Road a notamment terni – légitimement - la perception publique du Bitcoin.

Au sortir de la crise mondiale de 2008, la crédibilité des institutions financières et du système monétaire dans son ensemble ont été remis en cause. La toute-puissance de ces « gangsters de la

finance » était mise au jour et les populations ont sérieusement commencé à chercher des alternatives. Dans les années 1990, certaines initiatives avaient déjà été lancées mais sans aboutir. Je pense à Hashcash (A. Back, 1997), Bit Gold (N. Szabo, 1998). En 2008, le bitcoin fut créé par le mystérieux Satoshi Nakamoto, et s'inscrit dans cette mouvance des « cyberpunks » libertariens dont le souhait était de s'affranchir de tout contrôle étatique et financier. Leur souhait était de rendre le pouvoir au peuple notamment par la création d'une cybermonnaie non traçable et donc totalement anonyme.

On pourrait, a priori, juger cette volonté comme éthiquement juste ! Malheureusement, le bitcoin connait son heure de gloire avec l'avènement de la plateforme Silk Road (R. Ulbricht, 2011). En effet, le seul moyen de régler ses achats sur ce marché libre, dont l'interface est simplifiée, c'est la crypto-monnaie Bitcoin. La navigation y est sécurisée par le navigateur Tor. L'utilisation du bitcoin est donc devenue un levier pour le blanchiment d'argent, le financement du terrorisme et d'Etats voyous. En finançant leurs activités frauduleuses via le bitcoin, puis en les convertissant en devises réelles via des sociétés offshores, les malfrats peuvent injecter ces fonds dans l'économie réelle.

De ce pont de vue, nous sommes loin d'un usage éthique et juste du bitcoin sachant qu'il impacte de nombreuses victimes de ces trafics. Je pense aux victimes de la drogue, des armes, les enfants soldats, etc.

Le Bitcoin est une aubaine pour les mafias. En effet, il combine les avantages de l'argent liquide et du paiement en ligne et favorise l'évasion fiscale.

Au-delà de l'usage frauduleux du bitcoin, je suis convaincu que l'infrastructure sous-jacente : la blockchain, en tant qu'outil technologique, propose une multitude d'applications intéressantes.

Cependant, quelle place occupera le Bitcoin dans notre économie capitaliste de production ?

Nous vivons une ère, certes capitaliste, mais de rentabilité industrielle. Le bitcoin se positionne comme un levier pour une économie capitaliste mais de spéculation. Cette devise numérique est très instable dû à son jeune âge. Cela la rend attractive pour ceux qui cherchent le profit à tout prix.

Une monnaie joue un rôle fondamentalement collectif, en tant qu'instrument de cohésion sociale, ou pour reprendre Mauss, elle est « un fait social total »[50]. Les individus qui acceptent son utilisation

[50] Faure, P. H. (2016). Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique.

adhèrent aux normes de la société et marquent leur appartenance à une communauté. La monnaie les met en relation. Dans cette configuration de monnaie comme « créature de la loi » (Knapp, 1905)[51], c'est l'Etat qui cadre son utilisation. La monnaie remplit une fonction d'unité de compte qui régit les échanges entre individus.

C'est dans cette logique que la théorie classique énonce que la monnaie est dite exogène –les autorités sont capables de contrôler la masse monétaire en circulation et par voie de conséquence l'inflation grâce aux instruments dont ils disposent. Pour le Bitcoin, les règles d'émission d'unités monétaires sont différentes. C'est le code qui joue ce rôle de régulateur et détermine qu'en 2140 la masse monétaire bitcoin atteindra son maximum. Mais, cette méthode est considérée comme sommaire et inappropriée par les keynésiens.

L'économie postkeynésienne renverse le point de vue classique et défend une conception endogène de la monnaie – les banques de second rang ne peuvent créer de la monnaie que par l'octroi de crédits. C'est-à-dire que c'est l'évolution de l'activité qui régule l'évolution de la masse monétaire en fonction des besoins des agents économiques. La monnaie occupe donc un rôle de créateur de richesses en raison du décalage entre la production et l'encaissement du produit des ventes.

Ce caractère exogène ou endogène de la monnaie occupe une place cruciale dans le choix d'un système monétaire. Dans le cas d'une monnaie endogène, le lien à un métal précieux (l'or par exemple) dont la quantité est par nature limitée risque d'amener à un manque de ressources à terme qui pourrait mettre l'activité en péril. C'est notamment une des limites qu'a rencontré l'accord de Bretton Woods (première version) avec l'introduction de l'étalon-or et qui a causé son éclatement à la fin des trente glorieuses. Si l'on établit un parallèle avec le Bitcoin, dont le caractère totalement privé évoque l'abolition du monopole des banques centrales dans l'émission de billets et le passage à la concurrence entre les monnaies privées, on peut dire qu'il réintroduit cette menace déflationniste. En effet, puisque la crypto-monnaie a un cap fixé à 21 millions d'unités, elle connaît une déflation constante. Cette crypto-monnaie se prêtant davantage à l'épargne qu'à la dépense et même à la spéculation, elle ne peut constituer une réponse aux défis actuels. De ce point de vue, elle n'a aucune justification.

Cependant, le bitcoin peut-il réellement être considéré comme une monnaie ?

[51] Ibid

Le bitcoin s'apparente plus à une valeur boursière plutôt qu'une monnaie. Les banques centrales et de second rang n'auraient donc pas de rôle à jouer !

On pourrait aussi se demander, le Bitcoin est-il juste ?

L'ADN du bitcoin est caractérisé par deux paramètres : l'anonymat de ses utilisateurs et la décentralisation du contrôle des transactions. Dans ce protocole, la protection exacerbée des données privées pose certaines problématiques, notamment sur le volet fiscal. L'anonymat des transactions ne permet une taxation juste et menace potentiellement la justice sociale. En effet, le bitcoin échappant aux autorités fiscales, il possède un attrait certain pour les fraudeurs. De plus, la déclaration d'éventuelles plus-values réalisées grâce à la crypto-monnaie se ferait sur base du bon vouloir du détenteur. Si nous poussons le raisonnement plus loin, cela aura une implication dans la redistribution des richesses et aussi dans le calcul des ressources générées par des entités territoriales comme par exemple le calcul du PIB (Produit Intérieur Brut).

A ce stade de développement du Bitcoin, de nombreux Etats, dont la Belgique, ne souhaitent pas se positionner sur une législation. Cette position prématurée causerait sans doute une certaine évasion fiscale vers d'autres états moins regardants si la législation était jugée trop ferme.

Le fonctionnement du bitcoin rend aussi ses utilisateurs inégaux entre eux. En effet, les mineurs sont privilégiés face aux utilisateurs « classiques » dans l'accès à la monnaie puisqu'ils sont rémunérés pour le minage. Ils ont donc un avantage sur les autres. Evidemment, tout le monde peut potentiellement devenir mineur, mais, la complexité du système requiert des compétences informatiques et une puissance de calcul qui ne sont pas accessibles à tous. C'est ainsi que « générer des Bitcoins seul est quasiment impossible. Il est indispensable de rejoindre des pools de mineurs pour cela. En outre, les premiers mineurs ont un avantage sur les suivants puisque le niveau de rémunération en bitcoins va décroissant alors que le niveau de complexité de calcul lui va croissant.

Un autre enjeu, lorsque l'on parle de blockchain, est écologique. En effet, la consommation énergétique entrainée par la force de calcul déployée dans le processus de vérification du « proof-of-work » est énorme ! Une étude menée par des chercheurs suisses a montré qu'en 2015, le minage sur Bitcoin avait consommé autant d'énergie que 620.000 ménages.

Cependant, le système Ethereum du « proof-of-stake » règle cette problématique, puisque la force de calcul n'est plus nécessairement distribuée via tous les nœuds.

Lorsque je pense aux potentielles applications de la blockchain, et plus particulièrement à l'effet de levier que pourrait avoir cette technologie d'un point de vue éthique, je pense à l'exploitation des enfants encore présente dans certaines industries. J'imagine, à l'instar des services que proposent Provenance.org pour la traçabilité des produits alimentaires, une blockchain publique permettant de tracer et rendre transparent les processus de production de certaines industries d'extraction ou textiles. Ceci dans le but d'éviter ou du moins limiter l'exploitation de populations isolées ou de mineurs d'âge.

Cette vision peut paraître utopique, certes. Nous sommes dans une phase de développement de la technologie blockchain qui est couplée à un phénomène de « hype ». La technologie suscite un engouement certain et une médiatisation accrue. Il n'est ainsi pas toujours aisé de faire la différence entre les opportunités qu'amène la blockchain et l'utilisation malhonnête de la crypto-monnaie Bitcoin.

Ce qui m'intéresse c'est la capacité de la blockchain à changer notre organisation. Internet avait déjà considérablement réduit les couts d'accès aux informations et développé l'auto-organisation humaine grâce à la réduction des distances de communication. La blockchain amène une couche supplémentaire au-dessus de celle d'Internet, une nouvelle baisse des couts de communication et de transaction en y ajoutant une meilleure sécurité. La blockchain amène une nouvelle approche des communs, nous fait entrer dans la logique coopérative et collaborative lui conférant ainsi une dimension plus éthique. Cette autre forme de gouvernance est permise par le caractère décentralisé et distribué du registre open source.

VIII La blockchain comme base de construction d'un système des communs

L'engouement pour la blockchain est considérable depuis quelques années. Premièrement parce qu'il représente une révolution technologique qui ouvre des applications réduisant les couts structurels. Deuxièmement, elle ouvre la voie à un nouveau type de gouvernance générale. A l'image d'Internet en son temps, cette technologie disruptive est susceptible de transformer en profondeur notre organisation sociale et notamment en matière de production économique. Cela vient de sa capacité à créer un consensus entre des agents économiques qui à priori n'ont aucune raison de se faire confiance.

La blockchain permet de certifier des informations, ce qui jusqu'à présent nécessitait le passage par un tiers de confiance et aboutissait à une concentration des richesses à ce niveau. Ces relations désintermédiée de pair-à-pair créent un nouveau paradigme économique : l'économie collaborative. Les différents services que j'ai présentés dans ce travail contribuent à une « horizontalisation » du monde et des organisations modernes.

J'ai eu l'occasion de lire l'ouvrage de Jeremy Rifkin, La nouvelle Société du Cout Marginal Zéro[52]. Cet ouvrage m'avait beaucoup intéressé même si ma pensée était bien moins utopique et plus nuancée que celle de J. Rifkin.

Je rejoins l'économiste quand il définit les contours d'un nouveau système économique, l'économie de partage. Je nuance par contre son propos quand il prévoit l'éclipse du capitalisme.

La logique des communs collaboratifs s'installe peu à peu mais reste tout de même en marge. Le capitalisme ne disparaît pas, il sera transféré. L'agent catalyseur c'est le cout marginal égal à zéro : c'est-à-dire que le cout de production d'une unité supplémentaire qui tend en effet vers zéro grâce aux nouvelles technologies, dont la blockchain au travers des différentes applications précitées. Mais aussi grâce à l'utilisation d'énergies renouvelables.

Cette vision est permise grâce au développement de l'Internet des Objets et la disponibilité grandissante des ressources open source. Certaines industries sont déjà frappées par les effets de l'économie collaborative comme par exemple l'industrie musicale, l'édition, les transports. L'IoT remet également en cause la distribution de l'énergie traditionnelle mais surtout verte et autoproduite par les panneaux solaires ou les éoliennes. Sans compter les impacts sur les changements climatiques.

La production d'une unité supplémentaire suppose la production d'une « première » unité, c'est pourquoi il me semble néanmoins que du capital soit bien nécessaire initialement dans le processus de production. J'entends bien que l'utilisation de plateformes – IaaS, Paas, SaaS -, le pair-à-pair incite à faire tendre ce cout vers zéro mais je reste convaincu que le capitalisme occupera encore une place prépondérante dans les années à venir. L'exemple de la plateforme Azure (Windows), PaaS, n'est-il pas un exemple significatif ? Elle utilise la blockchain comme infrastructure mais facture ses services à ses clients comme acteur de cet écosystème.

[52] Rifkin, J. (2014). La nouvelle société du coût marginal zéro: L'internet des objets, l'émergence des communaux collaboratifs et l'éclipse du capitalisme.

Lorsque je pense aux voitures autonomes, au partage de véhicules via Autolib ou BlaBlaCar, il m'apparaît que la notion de propriété ne porte plus le même « prestige » pour les jeunes générations. L'accès semble importer davantage que la propriété en elle-même.

Je ne crois pas à la fin du capitalisme mais plutôt que le capitalisme entre dans une nouvelle phase que j'aurais envie d'appeler : le capitalisme distribué. A l'image des technologies qui en dessinent l'avenir…

IX Conclusion

En conclusion, la blockchain est une technologie révolutionnaire et qui ne se cantonne pas au Bitcoin. On connaît les liens qui se sont établis entre la crypto-monnaie et les trafics en tout genre sur le Darknet et la plateforme Silkroad notamment. On reconnaît aussi les possibilités de blanchiment d'argent qu'elle ouvre et les enjeux éthiques que ces mécanismes représentent. Je ne souhaite pas les occulter mais je préférerai retenir que la blockchain représente une opportunité pour permettre à l'Internet des Objets de prendre son envol.

La blockchain est un « enabler » pour une « liquéfaction »[53] du monde moderne et une « horizontalisation »[54] des organisations. L'écosystème et les initiatives autour de la blockchain sont florissants.

La technologie du registre distribué connait actuellement un engouement considérable et elle se place en bonne position dans le « pic des espérances exagérées du « Hype Cycle » de Gartner [55]. C'est un signe d'effet de mode et de démultiplication des initiatives, mais également d'immaturité du domaine et d'apprentissage par l'expérimentation. »[56]

[53] Waelbroeck, P. (2017). Les enjeux économiques de la blockchain. In *Annales des Mines-Réalités industrielles* (No. 3, pp. 10). FFE.

[54] Blockchain France Associés (Mai 2016). La Blockchain décryptée. Les clefs d'une révolution (pp 29)

[55] URL : www.gartner.com/technology/research/methodologies/hype-cycle.jsp

[56] Berbain, C. (2017). La blockchain : concept, technologies, acteurs et usages. In *Annales des Mines-Réalités industrielles* (No. 3, pp. 6-9). FFE

C’est une infrastructure ! Cela implique qu’elle ne saurait être bonne ou mauvaise en soi. C’est l’utilisation que l’on en fait qui est déterminante. Ne refusons pas un outil car il a été initialement utilisé pour de mauvais motifs.

Cette utilisation conduirait d’ailleurs à créer un nouveau paradigme économique : le capitalisme distribué. Je ne pense pas que nous assistions à l’éclipse du capitalisme mais plutôt à un mix d’économie capitaliste et collaborative. Prenons le cas de Facebook qui est un parfait produit du capitalisme d’extraction et en même temps un formidable outil d’émancipation et d’auto-organisation en pair-à-pair (comme par exemple lors du Printemps Arabe) !

Un défi à relever sera celui de la normalisation. L’acceptation par les industries et les populations me semble être un enjeu clé. La transversalité de la blockchain, qui permet de rompre avec la logique des silos, aidera à cette normalisation. J’attends d’ailleurs avec impatience le lancement de Metropilis – version grand public d’Ethereum – pour les novices. D’autre part, les contraintes techniques liées à la validation des blocs devront aussi être surmontées afin de permettre cette adoption massive. Finalement, l’impact environnemental de la méthode du « proof-of-work », très énergivore, sera aussi à régler…

Certains autres aspects sont encore à clarifier. Notamment définir clairement les responsabilités et le droit applicable aux blockchains. Je pense que cela se fera conjointement à l’évolution de la technologie et de l’acceptation globalisée de celle-ci. Brider la blockchain de manière anticipative n’aura qu’un effet négatif sur celle-ci. Ce sera le cas de l’Intelligence Artificielle également.

Comme le dit Lawrence Lessig, « code is law ». La confiance est accordée au système et plus à des intermédiaires. Nous vivons un moment clé pour la blockchain qui dessinera sans doute son futur technologique, social et économique…

X Bibliographie

Sources scientifiques

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. *URL : http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*.

Baldellon, O., & Équipe, A. S. A. P. (2010). Le problème du consensus byzantin en environnement asynchrone. *École Nationale Supérieure de Cachan, antenne de Bretagne*.

Berbain, C. (2017). La blockchain : concept, technologies, acteurs et usages. In *Annales des Mines-Réalités industrielles* (No. 3, pp. 6-9). FFE.

Blancafort, H., Recourcé, G., Couto, J., Sagot, B., Stern, R., & Teyssou, D. (2010). Traitement des inconnus: une approche systématique de l'incomplétude lexicale. *TALN 2010*.

Chiky, R., Defude, B., Hébrail, G., & Paris, G. E. (2006). Définition et diffusion de signatures sémantiques dans les systèmes pair-à-pair. In *EGC* (pp. 463-468).

Chrétien, R., & Delaune, S. (2014). Le bitcoin, une monnaie 100% numérique. *Interstices*.

DE VAUPLANE, H. U. B. E. R. T. L'ANALYSE JURIDIQUE DU BITCOIN.

Faure, P. H. (2016). Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique.

Kim, H. M., & Laskowski, M. (2016). Towards an ontology-driven blockchain design for supply chain provenance.

Laflaquière, J. (2005). Les « autres » applications des technologies peer-to-peer. *Multitudes*, (2), 59-68.

Larue, L. (2016). *Le Bitcoin : évaluation d'une innovation monétaire* (No. 2016127). Université catholique de Louvain, Institut de Recherches Economiques et Sociales (IRES).

Lavoie, M. (1982). Les post-keynésiens et la monnaie endogène. *L'Actualité économique*, *58*(1-2), 191-221.

Lohr, S. (2012). The age of big data. *New York Times*, *11*(2012).

Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems*, *25*(9), 1101.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies : Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* (pp. 239-278). Springer International Publishing.

Pilkington, M. (2015). Blockchain technology: principles and applications. *Browser Download This Paper*.

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

Rifkin, J. (2014). La nouvelle société du coût marginal zéro: Lřinternet des objets, lřémergence des communaux collaboratifs et lřéclipse du capitalisme.

Swan, M. (2015). Blockchain thinking: The brain as a dac (decentralized autonomous organization). In *Texas Bitcoin Conference* (pp. 27-29).

Swan, M. (2015). *Blockchain : Blueprint for a new economy*. " O'Reilly Media, Inc.".

Vergne, J., & Giguet, E. (1998). Regards théoriques sur le tagging. *Actes de Traitement Automatique des Langues Naturelles (TALN'98)*, 22-31.

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security* (pp. 112-125). Springer, Cham.

Waelbroeck, P. (2017). Les enjeux économiques de la blockchain. In *Annales des Mines-Réalités industrielles* (No. 3, pp. 10-19). FFE.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, *21*(1), 7-31.

Yermack, D. (2013). *Is Bitcoin a real currency? An economic appraisal* (No. w19747). National Bureau of Economic Research.

Revues non-scientifiques

Blockchain France Associés (Mai 2016). La Blockchain décryptée. Les clefs d'une révolution

Colwell B. (June 11, 2017). Ethereum Delirium: The Big List of Things You Should Know

Nakamoto, S. (2008). Bitcoin : A peer-to-peer electronic cash system.

Sites web

BlogChainCafé :

http://blogchaincafe.com/ethereum-vs-bitcoin-les-differences - 02 octobre 2017

http://blogchaincafe.com/la-limite-des-nombre-de-transactions - 29 août 2017

Cryptocompare : https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/ - 25 septembre 2017

Ethereum France : https://www.ethereum-france.com/slock-it-la-promesse-des-objets-connectes-surla-blockchain/ - 03 octobre 2017

L'usine Digitale : http://www.usine-digitale.fr/article/la-blockchain-pose-de-serieux-problemes-deconfiance-de-droit-et-de-securite.N401527 - 06 octobre 2017

Electronic Frontier Foundation : https://www.eff.org/fr/deeplinks/2014/10/beware-bitlicense-new-yorks-virtual-currency-regulations-invade-privacy-and-hamper - 02 octobre 2017

rts.ch. « Le bitcoin a consommé en 2015 autant d'énergie que 620'000 ménages ». http://www.rts.ch/info/sciences-tech/7674767-le-bitcoin-a-consomme-en-2015-autant-d-energie-que-620-000-menages.html - 6 octobre 2017

The BITCOIN.fr : http://www.thebitcoin.fr/legalite-utilisation-bitcoin-monde/ - 28 septembre 2017

Journal Le Figaro : http://www.lefigaro.fr/secteur/high-tech/2017/06/27/32001-20170627ARTFIG00256-de-grandes-entreprises-dont-saint-gobain-en-france-victimes-d-une-importante-cyberattaque.php - 17 septembre 2017

Journal l'Avenir : http://www.lavenir.net/cnt/dmf20170628_01024458/le-trafic-tnt-totalement-paralyse-par-la-cyberattaque - 17 Septembre 2017

Executive Summary

La blockchain est un défi pour les organisations modernes et la voie vers un nouveau paradigme économique. Sa première application en tant que crypto-monnaie : le Bitcoin, bien que malveillante, augurait déjà de ses principales caractéristiques. En effet, son caractère décentralisé et sécurisé qui élimine le besoin d'un tiers de confiance pour régir les transactions ouvre la voie vers des applications business d'un nouveau genre que nous détaillerons dans ce travail. Cette désintermédiation tend vers une horizontalisation des organisations et permet notamment à l'Internet des Objets de prendre une nouvelle dimension. Cependant, il sera crucial de ne pas négliger enjeux juridiques et éthiques dans l'utilisation des crypto-monnaies et de la blockchain. Consensus, traçabilité, liquéfaction des pouvoirs de décision, collectivisme ; tels sont les éléments qui mènent notre société vers une nouvelle organisation économique : le capitalisme distribué.