MASTER GRANDE ÉCOLE

NEOMA BUSINESS SCHOOL

EMPOWERING MANAGEMENT

MEMOIRE

En vue de l'obtention du Diplôme Sup de Co de Reims

MASTER GRANDE ECOLE – NEOMA BUSINESS SCHOOL

CYCLE MASTER

Est-il juste de penser que le Bitcoin favorise les actes frauduleux ?

MEMOIRE ACADEMIQUE

PAR: Cécile LAURENT

JURY : Mme Anne SIHEM – **TUTEUR**

Décembre 2015

Table des matières

REMERCIEMENTS

Pour la réalisation de ce mémoire, je tiens à remercier tout particulièrement :

- Les différents intervenants qui ont accepté de prendre du temps pour m'aider et m'éclairer dans mon travail de recherche :

Monsieur Brard C., mineur de bitcoin

Monsieur Cauderlier A., Bitcoin et blockchain entrepreneur

Monsieur De Jong I., expert à la Direction Générale Infrastructure de marché et paiements (Banque Centrale Européenne)

Monsieur Favier J., auteur de « La Voie du Bitcoin »

Monsieur Raymaekers W., Head of Banking market (SWIFT)

Monsieur Stervinou A., Chef du Service de la Surveillance des moyens de paiements scripturaux (Banque de France)

- Elie Bousselin, pour m'avoir fortement inspiré dans le sujet de ce mémoire.

- Corentin Boyer, pour les explications complémentaires en informatiques et les premières critiques.

- Mes parents ainsi Macha du Bourblanc, pour les relectures et les corrections orthographiques et syntaxiques.

- Ma tutrice, Madame Anne Sihem, pour son aide et pour le temps consacré à la correction de ce mémoire.

INTRODUCTION

Lundi 30 août 2015, coup de tonnerre dans le domaine bancaire : une des plus prestigieuses banques britanniques, la Barclays, annonce qu'elle s'apprête à accepter les échanges en Bitcoin, et ce avant la fin de l'année civile en cours[1]. Si cette décision n'est pas encore totalement mise en place à l'heure actuelle, plusieurs accords et contrats ont d'ores et déjà été signés entre le géant britannique et une dizaine de start-ups, qui évoluent dans le domaine du Bitcoin et de sa technologie[2].

Si la banque tient parole, même en 2016 seulement, elle serait alors une des toutes premières institutions bancaires majeures du monde à accepter des transactions réalisées en bitcoins. En effet jusqu'ici seule une poignée de commerces et d'entreprises, certes de plus en plus nombreux, acceptait ce moyen de paiement. La majorité d'entre eux en revanche connaissent de grandes difficultés à avoir accès à des services bancaires de base pour les soutenir dans le fonctionnement de leurs activités. En effet, le monde bancaire traditionnel et l'univers du système du Bitcoin ne pourraient apparaître comme plus opposés l'un à l'autre.

Le système bancaire actuel est le résultat du développement du réseau bancaire dans les pays occidentalisés depuis de nombreuses années, voire depuis plusieurs siècles. Organisé, encadré, centralisé, c'est un système bien construit et fort hiérarchisé qui fonctionne grâce à quelques personnes au sommet qui ont la main sur toute la pyramide du système. A l'inverse, le système du Bitcoin a été pensé et développé pour

[1] http://www.dailymail.co.uk/news/article-3216246/Barclays-UK-high-street-bank-accept-bitcoin.html

[2] http://www.bizjournals.com/newyork/news/2015/10/13/barclays-signs-two-blockchain-deals-among-slew-of.html

être un système de pair-à-pair, décentralisé, dans lequel chaque participant est garant de la sécurité et du bon fonctionnement de l'ensemble du réseau grâce à une responsabilité partagée. Le système du Bitcoin jouit ainsi dans le monde de la finance et des institutions bancaires d'une plutôt mauvaise réputation et d'une très grande méfiance, quel que soit le pays. Ainsi Taïwan et la Russie ont déclaré illégale l'utilisation du Bitcoin sur leur territoire, alors que plusieurs autres pays, dont la France notamment, ont émis de sérieuses alertes sur les risques associés à son utilisation par l'intermédiaire de leurs banques centrales.

Les chiffres de son expansion et du développement du réseau sont cependant assez éloquents. Si à peine 5000 transactions étaient réalisées en bitcoin par jour en 2011, leur nombre étaient de 50 000 mi-2012 pour atteindre le sommet de 200 000 transactions quotidiennes au cours de l'année 2015. Comment alors expliquer ces chiffres ? Si le système du Bitcoin est si peu fiable et si risqué, à tel point que certains états choisissent de l'interdire complètement, comment expliquer ce développement si rapide et important ?

Face à ce paradoxe, il m'a semblé pertinent de m'interroger sur la réalité du système du Bitcoin. A quoi sert le Bitcoin ? Quel usage en est réellement fait ? Qui peut ou pourrait y trouver un intérêt ? Pourquoi son utilisation présente-t-elle autant de risques pour les utilisateurs d'après les professionnels du système bancaire ? Autant de questions qu'il m'importait d'étudier, et de comparer avec ce qui est dit et répété de ce système, le plus souvent manière négative, et qui semble finalement assez peu correspondre à la réalité.

Afin de mener à bien cette étude, la première partie d'état de l'art dépeint tout d'abord un état de lieu de cette nouvelle monnaie qui beaucoup parler d'elle. Son fonctionnement, son protocole sous-jacent, ainsi que ses diverses opportunités et limites – réelles ou supposées- y seront notamment détaillés. A la suite de cette première partie trois hypothèses de recherche ont été développées, qui seront vérifiées grâce à un travail de recherche sur le terrain, développé dans la seconde partie de ce mémoire.

ETAT DE L'ART

I) Présentation du système monétaire et bancaire actuel

Si le système du Bitcoin est considéré comme innovateur et déclenche beaucoup de controverses et de discussion, c'est qu'il ne reprend en rien les grandes lignes du fonctionnement du système monétaire et bancaire traditionnel que nous connaissons depuis plusieurs années. Cette monnaie, qui est en même temps un système de paiement à part entière, a un mode de fonctionnement totalement étranger à tout ce que nous avons pu connaître jusqu'à aujourd'hui.

1) Le système monétaire actuel et le quasi-monopole de la monnaie scripturale dans les transactions quotidiennes

a) Le système monétaire actuel

Est appelé « système monétaire » l'ensemble de règles et d'institutions qui organise la monnaie au sein d'un espace monétaire. La plupart du temps cette tâche est de la responsabilité des Etats, et représente ainsi la politique économique intérieur des pays. Certains systèmes peuvent cependant être supranationaux, à l'exemple de la zone euro au sein de l'Union Européenne.

Un système monétaire est composé de plusieurs éléments essentiels. Le premier est un système de monnaie de compte - monnaie avec laquelle sont tenues les comptabilités dans l'unité de compte en question, par exemple l'euro et les centimes d'euro au sein de la zone euro. Le deuxième élément est un système de moyen de paiement. Ce dernier regroupe par exemple aujourd'hui non seulement les monnaies fiduciaires (pièces et billets), mais également ce qu'on appelle la monnaie scripturale, ou monnaie bancaire.

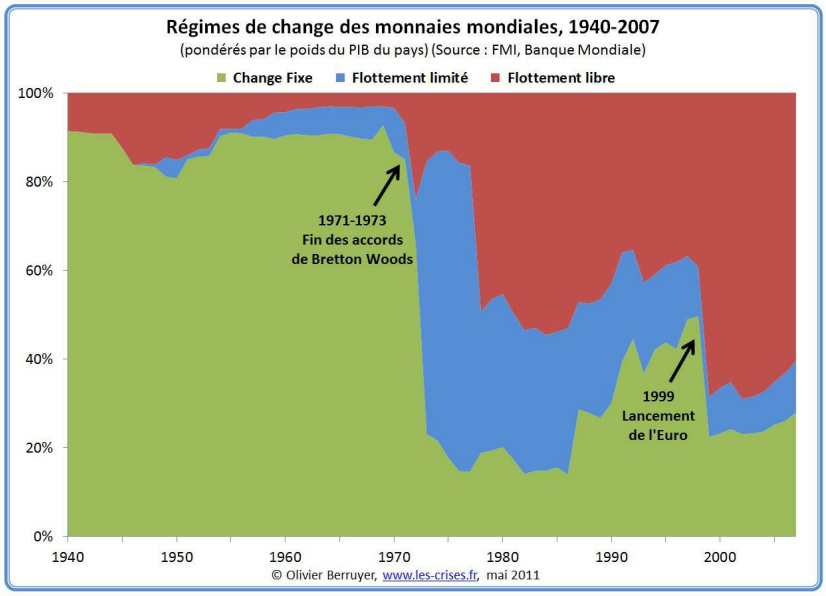
Enfin les mécanismes de change, fixes ou flottants, sont un troisième élément définissant un système monétaire.

Les mécanismes de change, ou systèmes de change, des monnaies permettent de définir le cours des différentes monnaies et d'assurer leur stabilité. Depuis les accords de la Jamaïque en 1976, qui ont fixé les nouvelles règles du système monétaire international, les monnaies convertibles ne sont plus définies par rapport à un étalon, l'or, ou par une parité fixe, le plus souvent le dollar américain, lui-même défini par un poids d'or. Le cours des monnaies est désormais déterminé par la confrontation de l'offre et de la demande sur le marché des changes. Ces accords représentent donc la fin du régime des parités fixes au niveau international, ainsi que la fin du statut officiel de l'or dans le système monétaire international. Il y a désormais un flottement international des monnaies selon les transactions réalisées sur le marché des changes. [3]

Il faut toutefois noter que ce système de changes flottants ne s'applique pas à l'ensemble des pays de la planète, mais plus particulièrement aux pays à économie de marché. D'autres systèmes de change existent encore, en particulier les currency boards, ou caisses d'émission, dans lesquels le cours des monnaies est fixé en fonction des réserves détenues dans la monnaie d'ancrage, à l'exemple de Honk-Kong ou de l'Argentine, dont les monnaies sont ancrées sur le dollar américain ; et les régimes intermédiaires (régime d'arrimage souple), dans lesquels le cours de la monnaie évolue dans une fourchette, ou selon un panier de devises de référence, à l'exemple de la Chine dont le yuan est ancré depuis 2005 sur un panier de devises (dollar, euro, yen …).
En 2008, le FMI recensait 48 pays avec un régime de change fixe (arrimage ferme) et 60 pays avec un régime intermédiaire (arrimage souple) et 79 pays avec un régime de change flottant. Le nombre de ces derniers ne cesse d'augmenter depuis plusieurs années. [4]

[3] http://www.cvce.eu/education/unit-content/-/unit/7124614a-42f3-4ced-add8-a5fb3428f21c/94fb0a95-09b1-4ee1-b0ff-c24e661506f1 Consulté le 11/10/2015

[4] http://www.leaders.com.tn/article/11619-regimes-de-change-et-guerre-des-monnaies-qu-en-est-il-du-dinar-tunisien Consulté le 11/10/2015

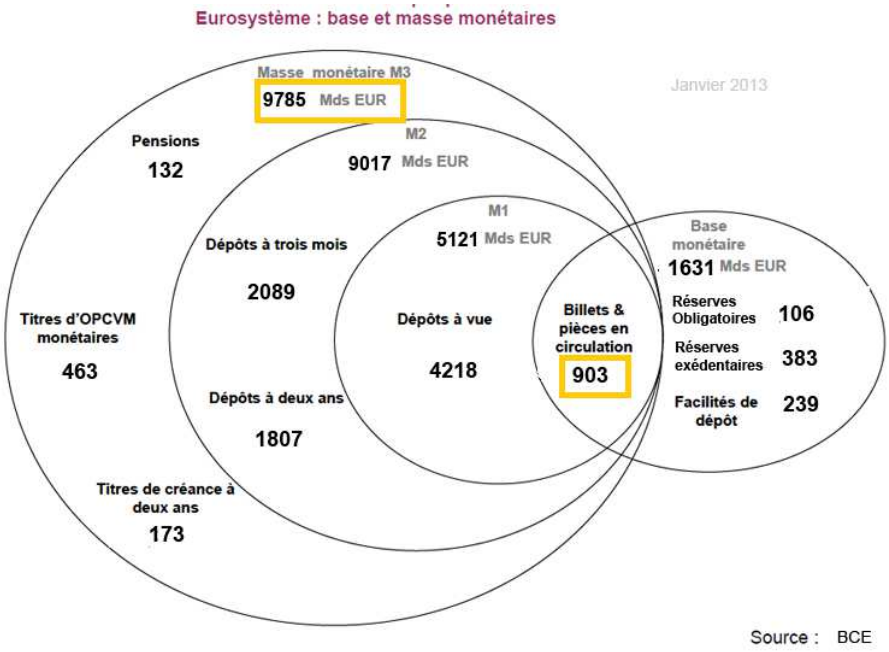


b) La croissance continue de la monnaie scripturale et son quasi-monopole aujourd'hui

La monnaie scripturale est la possession de monnaie matérialisée par une écriture bancaire, ou une écriture de compte. Ainsi lorsqu'un client effectue un dépôt bancaire, de pièces ou de billets, la banque ne garde pas cette monnaie dans un coffre fermé au nom du client. L'argent va être utilisé et va circuler au cours de différentes transactions. La banque émet donc une reconnaissance de dette en faveur du client, et crée ainsi de la monnaie scripturale. La balance du compte en banque du client en question est donc la totalité de la dette de la banque en sa faveur (ou l'inverse si le compte est débiteur).

Depuis environ 30 ans, la masse monétaire scripturale a connu une croissance exponentielle pour plusieurs raisons. Tout d'abord l'interdiction progressive des paiements en liquide de grosses sommes, pour des raisons de sécurité, ainsi notamment que l'apparition du chéquier, de la carte bancaire, et du paiement en ligne. La monnaie scripturale représente aujourd'hui environ 90% de la masse monétaire totale, comme le montre le graphique ci-dessous. De plus, du fait de la croissance toujours plus grande des paiements dématérialisés, en particulier par téléphone ou grâce à des portes-

monnaies électroniques, on peut donc s'attendre à un quasi monopole de la monnaie scripturale dans les années à venir. [5]



(903/9785 = 0.0923 La monnaie fiduciaire représente donc seulement un peu moins de 10% de la masse monétaire totale (M3).)

Dans cet environnement, la circulation de la monnaie se fait donc en très grande partie au moyen de virements d'un compte bancaire à un autre entre acteurs économiques. Ces virements s'effectuent grâce aux différents moyens de paiements du système : par carte bancaire, virements bancaires, ou par chèque.

Cette montée en puissance de la monnaie scripturale est bien entendu liée à l'ère du numérique et à l'utilisation croissante de l'informatique dans les activités monétaires, bancaires, et financières. Ainsi les banques ont longtemps tenu les écritures de compte dans des registres avant de changer pour un système entièrement informatisé depuis plusieurs années. Cependant, cette importance de la monnaie scripturale n'est pas seulement un effet secondaire de l'importance du numérique dans les diverses

[5] http://www.piecedemonnaie.fr/lexique/monnaie-scripturale/ Consulté le 15/10/2015

activités, mais est également un choix de la part des institutions. Elle est effet gage de sécurité et aide au contrôle et à la surveillance du bon fonctionnement du système. En France par exemple, le transport de sommes supérieures ou égales à 10 000 € (ou équivalent en devise) en pièces ou billets par une personne physique est illégal. Le paiement en liquide d'aussi grosses sommes est interdit et doit s'effectuer via les comptes bancaires des acteurs économiques, ce qui permet une traçabilité et un suivi des mouvements de fonds importants, afin par exemple de lutter contre le blanchiment d'argent provenant de trafics illicites, et notamment de stupéfiants. [6]

2) Présentation et fonctionnement du système bancaire traditionnel

a) La Banque Centrale, organe centralisateur de l'ensemble du système bancaire

Le système bancaire moderne est articulé autour de deux composants essentiels : la Banque Centrale et les banques commerciales.

La Banque Centrale est l'institution chargée d'appliquer la politique monétaire d'un pays (ou d'un ensemble de pays dans le cas de la zone euro par exemple).

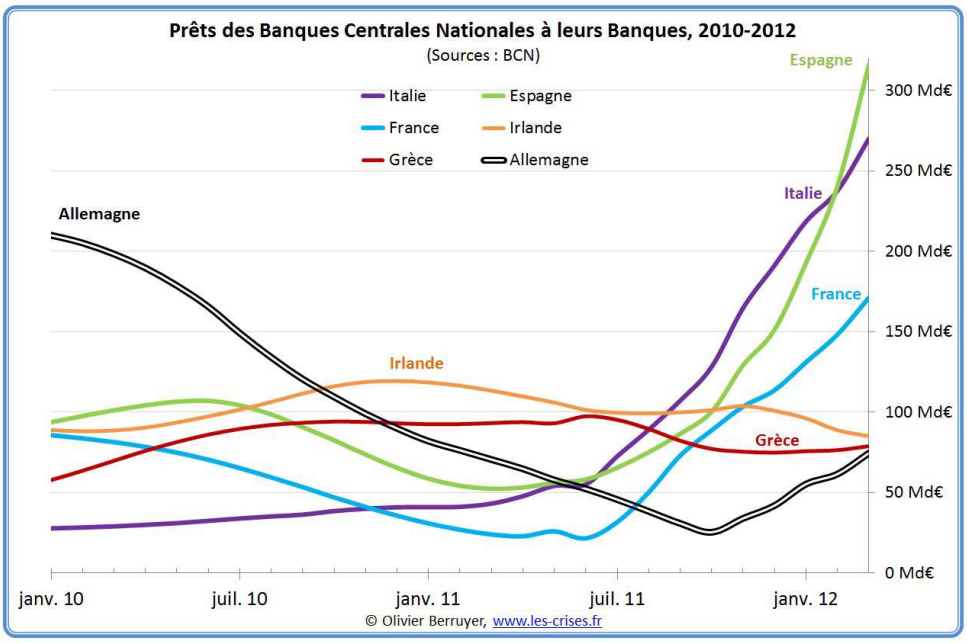
Une Banque Centrale a 4 grands rôles principaux. Elle fixe tout d'abord, au jour le jour, les différents taux directeurs. Ces taux directeurs permettent d'influer sur l'activité économique du pays ou de la zone, et sont au nombre de trois : le taux de rémunération des dépôts (dépôts placés par les divers établissement financiers, dont les banques commerciales, auprès de la Banque Centrale) ; le taux d'escompte, ou taux de prêt marginal, qui est le taux auquel la Banque Centrale prête des liquidités aux banques commerciales qui en ont besoin ; et enfin le taux de refinancement, qui est la taux auquel les établissements financiers peuvent emprunter auprès de la Banque Centrale. Ce dernier taux est le plus important, puisqu'il a une grande influence sur l'activité

[6] http://www.douane.gouv.fr/articles/a10796-obligation-declarative-des-sommes-titres-et-valeurs Consulté le 13/10/2015

économique. En effet, les banques commerciales répercutent ce taux sur leurs propres taux accordés à leurs clients, ce qui influe sur les apports ou retraits de liquidité.

Le second rôle de la Banque Centrale est donc d'assurer le refinancement des banques commerciales lorsque celles-ci en ont besoin. Lorsque les banques commerciales n'ont plus assez de liquidités, elles se tournent alors vers le marché monétaire (la Banque Centrale, ou parfois des institutions financières privées) pour se refinancer. En échange de liquidités, la Banque Centrale prend alors « en pension » des actifs de la banque commerciale (bons du Trésor et créance privée de qualité). En lui fournissant des liquidités, la Banque Centrale lui fait donc crédit et crée ainsi de la monnaie. Cette monnaie disparaît dès qu'elle est remboursée à la Banque Centrale (fin de la prise en pension).

Elle joue également le rôle essentiel de prêteur en dernier recours cas de crise systémique. Si une crise de liquidité a lieu sur le marché monétaire - lorsque les acteurs économiques ne disposent pas des liquidités nécessaires pour faire face à leurs engagements envers les banques commerciales - la Banque Centrale se doit de créer la monnaie nécessaire au bon fonctionnement du système bancaire. Un exemple peut-être la crise des subprimes aux Etats-Unis en 2007. Pour éviter que tout le système financier américain ne s'effondre, la FED a injecté à partir de 2007 plus de 1000 milliards de dollars sous différentes formes pour refinancer les banques commerciales.



Enfin, la Banque Centrale a le rôle de veiller sur la monnaie, les crédits, et le bon fonctionnement général de l'ensemble du système bancaire à l'aide de différents outils, tels que le ratio de solvabilité ou encore les réserves obligatoires pour les banques commerciales, qui garantissent la sécurité et préviennent les possibles dérives. [7]

La Banque Centrale est donc au cœur même du système bancaire. Elle peut être décrite comme la banque des banques. Dans les faits, chaque banque commerciale possède un compte auprès de la Banque Centrale pour y déposer ses réserves obligatoires. Depuis 2012, le taux de réserves obligatoires au sein de la zone euro est de 1% des dépôts que possède la banque commerciale. Ces réserves obligatoires sont donc des liquidités déposées auprès de la Banque Centrales, constituées des dépôts, titres de créance, et instruments du marché monétaire dont les échéances sont inférieures à deux ans. Elles servent à compenser les chèques et les paiements électroniques des clients.

b) Le réseau des banques commerciales et leurs activités de proximité

Les banques commerciales ont pour leur part 3 rôles principaux. Le premier est de collecter et prêter les dépôts des ménages, des entreprises, et des administrations. Ces dépôts sont en grande majorité constitués des revenus et de l'épargne des ménages, ainsi que des rentrées d'argent et des placements des entreprises en excédent temporaire de liquidités. Lorsque cette masse de monnaie est collectée, les banques l'utilisent alors pour prêter cet argent, soit directement à d'autres de leurs clients en leur faisant crédit, soit par l'intermédiaire des marchés monétaires ou financiers pour emprunter ou acquérir des actifs par exemple.

Le second rôle principal des banques commerciales est de servir d'intermédiaire financier. Lorsqu'une entreprise ou même l'Etat souhaite se refinancer, il émet alors des titres (action ou obligation) qu'il vend aux autres acteurs économiques par l'intermédiaire des banques commerciales. Depuis plusieurs années déjà, la part de ce

[7] http://www.m-lasserre.com/educpop/dossiermonnaie/4lesystemebancaire.ht Consulté le 15/10/2015

rôle d'intermédiaire financier ne cesse d'augmenter dans l'activité globale des banques commerciales, au détriment de leur rôle traditionnel de collecte et de prêt auprès des ménages, entreprises, et des administrations.

Enfin, le dernier rôle majeur joué par les banques commerciales est de créer de la monnaie scripturale. Il existe deux manières différentes pour les banques d'accorder un crédit à un de leurs clients. Soit elles prêtent de l'argent qui a déjà été déposé chez elles, et dans ce cas il ne s'agit que de faire circuler la monnaie ; soit elles accordent le crédit en faisant confiance à l'emprunteur, sans dépôt préalable. Elles prêtent donc de l'argent qui n'existe pas encore par une simple écriture sur le compte du client, contre promesse de la restitution de cette somme à échéance fixée. Durant toute la durée de ce prêt, la monnaie existe et circule entre une multitude d'acteurs économiques, avant d'être détruite lorsque le crédit sera remboursé. Il y a donc une véritable création monétaire, et spécifiquement de monnaie scripturale.
Dans les faits, les dépôts ne servent pas, ou très peu, à financer les crédits. Ils sont majoritairement utilisés pour réaliser des placements financiers. La création monétaire, sous forme de monnaie scripturale, résulte donc de l'accord de crédit des banques à leurs clients.

Le système bancaire moderne est donc un système centralisé, dans lequel la Banque Centrale met en œuvre l'ensemble de la politique monétaire grâce aux divers outils dont elle dispose et à l'ensemble des banques commerciales qu'elle supervise.
Dans ce système, chaque transaction monétaire effectuée par un acteur économique passe par un tiers bancaire, que ce soit une banque commerciale ou la Banque Centrale elle-même. 90% de la monnaie étant sous forme scripturale, seules les banques ont aujourd'hui la capacité de réaliser les changements d'écriture qui résultent des transactions réalisées par les divers moyens de paiement possible.

II) Présentation du système du Bitcoin et de son fonctionnement

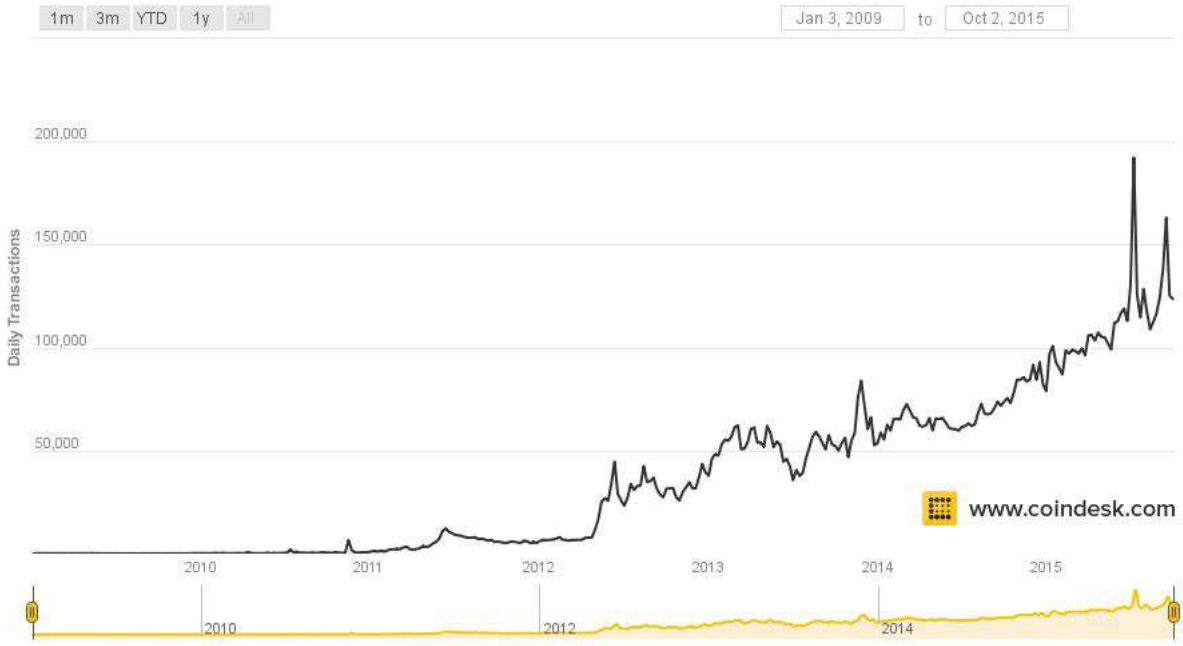
Créé en 2009 par Satoshi Nakamoto, le Bitcoin est le premier système de paiement numérique entièrement décentralisé, c'est-à-dire permettant des échanges directement de pair à pair, sans passer par un tiers. Une des spécificités importante du Bitcoin est d'être à la fois une monnaie et en même temps un système de paiement à part entière. Ainsi le terme Bitcoin, avec une majuscule, fait référence à la fois au concept et au système de paiement de manière générale. Le terme bitcoin, sans majuscule, réfère quant à lui à l'unité monétaire utilisée par ce système de paiement, également exprimée par BTC.

Dans la lignée de la monnaie scripturale, le Bitcoin est une monnaie entièrement dématérialisée qui s'échange uniquement par le biais de transactions numériques. Il n'existe pas de pièces ou de billets en bitcoin, et les échanges ne se font que grâce au logiciel Bitcoin prévu à cet effet.

Si ce n'est pas la toute première monnaie entièrement virtuelle à être créée – le Linden Dollar, dans l'univers virtuel de Second Life par exemple, permet à ses utilisateurs d'acheter des biens et des services – elle prend toutefois une autre dimension. Si, comme bien d'autres, elle permet d'échanger des biens et des services, cette monnaie est également souvent décrite comme une devise, à savoir qu'elle se veut indépendante de toute autre monnaie de référence telle que le dollar américain ou l'euro, et est définie dans sa propre unité de compte. Ainsi chaque bitcoin (BTC) est sous divisé en 100 millions de petites unités, appelées des satoshis (1 satoshi = 0.00000001 bitcoin). De plus, il n'y a pas de taux d'échange fixe entre le Bitcoin et les autres devises de référence. Ainsi que le pointent souvent les médias, le Bitcoin s'échange au gré de l'offre et de la demande du marché, ce qui peut parfois amener à une forte volatilité de ces taux d'échange.

1) Vue d'ensemble du système du Bitcoin

Le Bitcoin existe depuis 2009 mais a connu jusqu'au milieu de l'année 2012 des débuts plutôt lents. Il s'échangeait alors entre 5 et 10 dollars, et le nombre de transactions réalisées par jour n'atteignait pas 10 000.



Au cours de l'année 2013, le système a été victime de plusieurs piratages informatiques et le nombre de transactions réalisées a plus d'une fois chuté. Toutefois, à la fin de l'année, le nombre global de transactions par jour était de l'ordre de 50 000, et le bitcoin s'échangeait alors contre un peu plus de 1000 dollars. Simultanément, le très populaire moteur de recherche chinois Baidu annonçait qu'il acceptait à présent les paiements en bitcoin, et plusieurs audiences tenues au sein du Congrès américain sur le sujet du Bitcoin lui ont été plutôt favorables.

La Banque Centrale de la République populaire de Chine a cependant interdit en décembre 2013 aux institutions financières chinoises d'utiliser le bitcoin. Cette décision a eu pour effet de faire chuter le cours du Bitcoin et de limiter les transactions. Aujourd'hui encore, certains services offerts par Baidu ne sont pas payables en bitcoin par exemple.

Fin 2014, à la suite de la chute d'une des plates-formes d'échange majeure, Mt.Gox, le bitcoin s'échangeait contre 383 dollars.

Plusieurs Etats commencent à réfléchir à diverses formes de régulation pour essayer de contrôler un tant soit peu les échanges et les transactions réalisés au sein du système du Bitcoin. Il est entre autre question de considérer le Bitcoin comme un actif imposable et de réguler les échanges réalisés en Bitcoin. Il est de plus question de soumettre les plates-formes d'échange aux lois contre le blanchiment d'argent et aux exigences demandées dans le cadre de la lutte anti-terroriste.

Quelques chiffres permettent de se rendre un peu mieux compte de la réalité de cette monnaie numérique :

- Si le Bitcoin est la crypto monnaie la plus célèbre, ce n'est en revanche pas la seule à exister. A la fin de l'année 2014, un total de 483 crypto monnaies différentes était ainsi recensé. Le Bitcoin à lui-seul capitalisait alors 92% du chiffre d'affaire réalisé par l'ensemble de ces monnaies.
- Toujours fin 2014, il y avait environ 6,5 millions de portes-monnaies électroniques de créé, contre seulement 1,3 million en septembre 2013.
- Enfin, environ 76 000 commerces et entreprises à travers le monde acceptent désormais les paiements en Bitcoin, que ce soit de grandes entreprises internationales à l'exemple de Dell, ou bien des commerces locaux, comme des fleuristes. Le tout premier achat en Bitcoin fut d'ailleurs réalisé en mai 2010 par un américain, Laszlo Hanyecz, qui à l'époque a déboursé 10 000 BTC pour acheter deux pizzas (ce qui correspondrait aujourd'hui à la modique somme de 3 345 000 dollars environ).

2) Les différents concepts présents au cœur du système

Le système du Bitcoin repose tout entier sur un modèle mathématique très complexe, où tout - depuis la création monétaire jusqu'à la vérification des transactions réalisées - fonctionne grâce à des algorithmes générés par les ordinateurs des utilisateurs.

3 concepts majeurs sont fondamentaux pour comprendre le fonctionnement et les spécificités du Bitcoin : la cryptographie, la chaîne de bloc, et l'activité de minage.

a) La cryptographie, ou la méthode sous-jacente de la technologie du Bitcoin

Le Bitcoin a été décrit par ses utilisateurs comme la toute première implémentation du concept de crypto monnaie. Les crypto monnaies sont des monnaies qui utilisent le système de la cryptographie pour valider les transactions et générer la monnaie. Ce sont donc des monnaies numériques et décentralisées, qui fonctionnent de pair à pair.

Dans l'esprit de la cryptologie, la cryptographie permet d'envoyer des messages en les protégeant par des clés, générées à l'aide d'algorithmes mathématiques. Seules les personnes détenant les clés spécifiques au message envoyé peuvent le décoder et y avoir accès.

Dans les faits, chaque utilisateur de Bitcoin possède un porte-monnaie numérique, appelé « wallet », et auquel est attribué une adresse sous forme de clé publique (comparable au principe du RIB dans le système bancaire), qui a pour rôle d'être diffusée. Est également attribuée une clé privée, qui est gardée secrète. Ces deux clés servent lors de transactions à coder et décoder les messages, garantissant ainsi la confidentialité des informations échangées. Ainsi lors de l'envoi d'un message, l'expéditeur utilise la clé publique du destinataire pour coder le message. Seul le destinataire, à l'aide de la clé privée correspondante, pourra alors le décoder. A l'inverse, l'expéditeur peut également utiliser sa clé privé pour coder le message, et le destinataire utilisera alors la clé publique correspondante pour le décoder. Ce système de signature numérique permet donc d'authentifier l'auteur du message et son destinataire, ainsi que d'en protéger la confidentialité.

Tout le fonctionnement du Bitcoin repose sur ce système de cryptographie à clés publiques et privées. Un exemple permet de comprendre ce fonctionnement assez facilement. Imaginons un utilisateur A qui souhaite envoyer 5 BTC à un utilisateur B.

La transaction prend alors la forme d'un fichier, créé par le porte-monnaie de l'utilisateur A, et publié sur le réseau. Ce fichier contient plusieurs éléments. Tout d'abord les deux clés nécessaires permettant d'identifier les utilisateurs A et B concernés par la transaction, selon que le message sera signé ou chiffré ; le contenu de la transaction elle-même, à savoir les 5 BTC ; et enfin les références des transactions précédentes de l'utilisateur A, qui permettent ainsi de s'assurer qu'il est effectivement en position de ces 5 BTC. Enfin, l'ensemble de ce fichier est signé ou chiffré grâce à la clé choisie de l'utilisateur A[8]. De cette manière l'authenticité du message ainsi que les identités des utilisateurs seront préservés.

b) La chaîne de bloc - ou blockchain - l'aspect essentiel de toute la technologie du système

Le point le plus étonnant et particulier du système de Bitcoin est que ce réseau fonctionne de manière totalement autonome. Tout repose entièrement sur ses utilisateurs et leurs ordinateurs mis à disposition du système.

Le principe essentiel de Bitcoin est de tenir à jour sur un très grand nombre d'ordinateurs - appelés des nœuds, répartis à travers le réseau – un ensemble de registres publics et infalsifiables de toutes les transactions réalisées depuis que le système existe. Ces registres sont synchronisés à travers le réseau, et fonctionnent selon le modèle du pair à pair.[9]

---

[8] Lorsque le message est signé, le fichier est crypté avec la clé privée de l'utilisateur A et sera déchiffré par l'utilisateur B avec la clé publique de l'utilisateur A (qui est donc connue). Cette méthode permet de s'assurer de l'identité de l'envoyeur.
A l'inverse lorsqu'un message est chiffré, le fichier est crypté avec la clé publique du destinataire B, et ce dernier pourra le déchiffrer grâce à sa clé privée. Cette méthode permet en revanche de s'assurer que seul le destinataire B pourra déchiffrer le message envoyé.

[9] Le modèle du pair à pair permet à plusieurs ordinateurs de communiquer entre eux à travers le réseau Bitcoin. Grâce à l'architecture particulière des systèmes pair à pair, les données transférées sont échangées directement entre les ordinateurs concernés, sans transiter par un serveur central. Tous les ordinateurs jouent donc à la fois le rôle de serveur et de clients. Sont spécifiquement appelés des « nœuds » tous les ordinateurs qui sont connectés à un réseau fonctionnant selon le modèle du pair à pair.

L'avantage de ces multiples registres est de garantir la véracité de l'ensemble. En effet, comme les copies sont multiples, il y a peu d'incitation ou de gain à fausser le registre d'un ordinateur particulier. La sécurité du réseau n'est donc pas basée sur un ensemble de codes par exemple que détiendrait une autorité centrale, mais sur un système distribué qui rend les fraudes ou les attaques très complexes à réaliser, et, de manière générale, peu lucratives.
Cet ensemble de registres tenus sur le réseau Bitcoin forment l'équivalent d'un grand livre comptable, partagé entre tous les utilisateurs du réseau et donc entièrement public.

Pour aller plus loin dans la compréhension du fonctionnement du Bitcoin, 2 concepts majeurs sont nécessaires : la chaîne de bloc et le minage. Ces deux concepts sont étroitement reliés l'un à l'autre et forment la spécificité même du système du Bitcoin.

Les mineurs, qui effectuent une activité de minage, sont les vérificateurs des transactions effectuées sur le réseau. Ils enregistrent les transactions dans ce qui est appelée « la chaîne de bloc ». On dit qu'ils « trouvent des blocs ».
Concrètement, l'objectif des mineurs est de rassembler dans des blocs les transactions qui circulent sur le réseau. Chaque bloc est formé d'environ 300 transactions. Une fois que ces blocs sont vérifiés (ou « trouvés »), c'est-à-dire que les transactions ont été déclarées comme valides par les mineurs, ces blocs rejoignent les blocs précédents déjà vérifiés. Cet ensemble de blocs forme la chaîne de bloc, qui est inscrite sur les différents registres du réseau.
Valider un bloc de transactions signifie que les mineurs remontent la chaîne des blocs - et donc, d'adresse en adresse, toutes les transactions passées - pour vérifier d'où proviennent les bitcoins impliqués dans les transactions présentes. Cela permet premièrement de vérifier que l'expéditeur possède bien les bitcoins qui vont être échangés, et également de vérifier qu'aucun bitcoin n'est apparu sans raison et de cette façon d'empêcher les fraudes.
Ce système de chaîne de bloc permet donc une traçabilité complète des transactions et des bitcoins, et empêche toute possibilité de contrefaçons. C'est pourquoi le système du

Bitcoin peut entièrement se passer d'une entité qui jouerait le rôle d'une banque centrale.

De manière plus précise, chaque bloc contient donc trois éléments essentiels : plusieurs transactions, un identifiant généré automatiquement par un algorithme en fonction des transactions qu'il contient, ainsi que l'identifiant du bloc qui le précède. Les blocs s'ajoutent donc dans la chaîne de manière chronologique – ce qui justifie l'appellation de « chaîne » - un nouveau bloc ne pouvant pas être ajouté si on ne connaît pas l'identifiant du précédent. L'historique des transactions du réseau est ainsi préservé. Dès qu'un mineur trouve un bloc l'information est diffusée par le logiciel Bitcoin aux autres nœuds du réseau pour que chacun l'ajoute à son propre registre de la chaîne de bloc. Cet échange d'informations en temps réel sur Internet permet de synchroniser les différentes copies de la chaîne de bloc conservées par les nœuds.

Il peut arriver que plusieurs mineurs trouvent des blocs en même temps, en utilisant des transactions différentes. Sont alors éditées plusieurs versions de la chaîne de bloc sur les différents registres. Avec le temps cependant les nœuds du réseau finissent par se mettre automatiquement d'accord. N'est toujours gardée que la version la plus longue de la chaîne de bloc, qui devient alors la chaîne de bloc officielle. Les versions qui ne sont pas retenues constituent alors des blocs orphelins. Le fait de toujours choisir la version la plus longue de la chaîne de bloc est ce qui sécurise le système du Bitcoin. Il devient en effet beaucoup plus difficile pour un mineur de frauder en essayant d'ajouter des blocs de transactions frauduleuses. Il lui faudrait miner beaucoup plus vite que tous les autres mineurs, et donc rassembler une puissance du réseau considérable pour que sa version soit choisie comme la version officielle, ce qui est aujourd'hui de l'ordre de l'impossible.

c) Le minage, activité indispensable au bon fonctionnement de l'ensemble du réseau

Le minage, pour sa part, est une activité qui nécessite une forte utilisation du matériel informatique pour exécuter un algorithme issu de la cryptographie, afin de confirmer les blocs de transactions et d'assurer la sécurité du réseau. L'exécution de ces

algorithmes est très coûteuse en matériel et également en énergie. C'est pourquoi il arrive que les mineurs se regroupent entre eux, ils forment alors un pool, pour se répartir le travail et donc les coûts matériels et énergétiques surtout de cette activité. Un mineur peut cependant miner seul.

« Miner » signifie donc exécuter un certain algorithme - le SHA-256 - de nombreuses fois jusqu'à ce qu'il trouve un résultat qui prouve qu'il a bien trouvé un bloc, selon certains critères propres au système du Bitcoin. Le plus souvent le mineur doit exécuter cet algorithme plusieurs milliards de fois par seconde pendant plusieurs minutes avant de trouver un bloc.

Lorsqu'on l'exécute, le SHA-256 produit une chaîne de caractères plus ou moins aléatoires que l'on appelle un « hash ». Un exemple de hash pourrait être : g912fg1cdd3f842g18688cbbc22c9c9fa76eg192gd403dg511b880g6842.

Trouver un bloc revient à trouver le hash qui commence par un certain nombre de zéros. Pour ce faire, les mineurs exécutent l'algorithme en y ajoutant un incrément, qu'ils augmentent à chaque tour, jusqu'à ce qu'ils trouvent le bon hash.

Un exemple permet de mieux comprendre ce fonctionnement :

Tout d'abord prenons une chaîne de caractère au hasard, par exemple « 1234567890 Bitcoins ».

En appliquant l'algorithme SHA-256 à cette chaîne de caractère, on obtient comme résultat le hash suivant : 506f841085373238d1f8bc82e234e8b3baddb7b4b6315db3e1750dec6c310d99. Or, ce hash ne commence pas par zéro.

On réapplique donc l'algorithme à la chaîne de caractère, en y ajoutant cette fois-ci un incrément : « 12345678910 Bitcoins-1 », « 12345678910 Bitcoins-2 », etc, jusqu'à trouver un hash qui commence par un zéro.

Le premier hash commençant par zéro est obtenu avec le neuvième incrément, « 12345678910 Bitcoins-9 », qui donne effectivement comme résultat : 0b82f4fd32f4de56aec4f43d7e46c3b45c6ac45ecd71cb0351716b372e3e9a21. [10]

[10] http://www.monnaie-bitcoin.com/minage-bitcoins Consulté le 5/09/2015

Dans cet exemple, 9 essais ont été nécessaires pour trouver un hash qui commence par un zéro. Dans la réalité, des milliards d'essais sont nécessaires pour que les mineurs trouvent un hash qui commence par le bon nombre de zéros.

Une fois que le bon hash a été trouvé, le mineur l'envoie à tous les nœuds du réseau qui vérifient ce résultat et l'ajoute à leur chaîne de bloc.

L'activité de minage nécessite du matériel permettant une très forte puissance de calcul. Tout d'abord car c'est une activité très concurrentielle. Les mineurs ont donc tout intérêt à s'équiper le mieux possible pour miner le plus rapidement possible avant les autres. Ensuite, car l'algorithme SHA-256 nécessite énormément de ressources informatiques. Il est aujourd'hui par exemple impossible de miner avec un simple PC. A titre de comparaison, les outils avec lesquels les mineurs travaillent aujourd'hui peuvent en moyenne déployer une puissance autour de 400 000 MH/s (quatre cent mille millions de hash par seconde), et pourrons bientôt atteindre les 1 500 000 MH/s, alors qu'un ordinateur ordinaire atteint en moyenne une puissance de 100 MH/s.
De ce fait, la puissance informatique allouée au réseau Bitcoin ne cesse d'augmenter jusqu'à culminer aujourd'hui à son plus haut point : l'algorithme SHA-256 est exécuté plus de 2 millions de milliards de fois par seconde par le réseau Bitcoin.

Cette forte puissance informatique nécessaire est garante de la sécurité du réseau Bitcoin. En effet, pour pouvoir insérer des transactions frauduleuses dans la chaîne de bloc, un mineur frauduleux devrait pouvoir rassembler plus de la moitié de la puissance totale du réseau. Ce fait est connu sous le nom de la règle des 51%. Il lui faudrait donc disposer de 51% de la puissance du réseau, ce qui est pour ainsi dire impossible.

Comme le minage est une activité qui demande du temps et surtout beaucoup d'énergie et d'investissement, les mineurs reçoivent une rémunération de la part du réseau. Pour cela ils doivent fournir la preuve de leur travail et des ressources utilisées, c'est-à-dire l'identifiant du bloc qu'ils viennent de miner, le numéro de l'incrément, ainsi que le hash trouvé. Ce point est très important dans le système de Bitcoin, car si les mineurs n'étaient pas rémunérés ils n'auraient pas d'incitation à autant investir dans

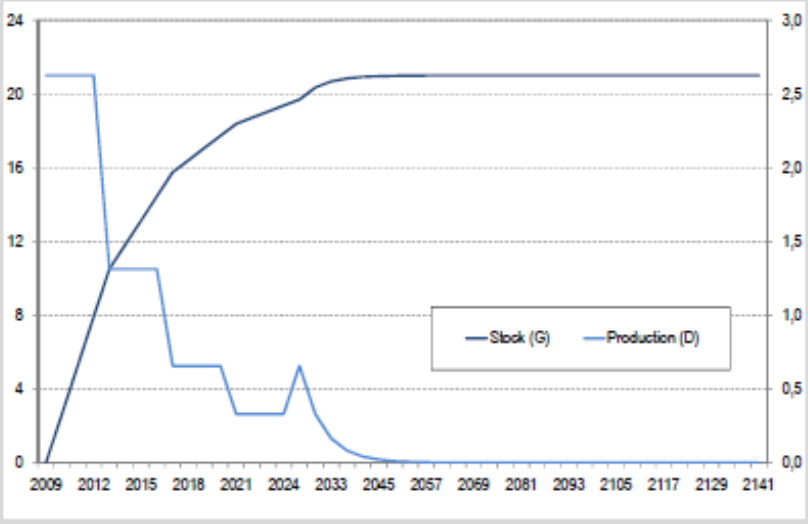
de telles puissances de calcul, afin d'assurer le bon fonctionnement et la sécurité du réseau.

La rémunération des mineurs se fait en fractions de bitcoins nouvellement créés, et représente la seule manière possible de créer de nouveaux bitcoins. Cette création de monnaie est transparente, puisque chacun peut savoir combien de nouveaux bitcoins ont été créés en fonction des blocs validés, et assure le bon fonctionnement du réseau. Grâce à ce système, le réseau Bitcoin peut donc se passer d'une entité qui jouerait le rôle d'une banque centrale.

Un point essentiel à noter est que la récompense, ou rémunération, des mineurs n'est pas fixe. Plus le nombre de blocs validés augmente, plus la rémunération des activités de minage diminue. Elle est divisée par deux tous les 210 000 blocs trouvés, et cela pour une raison simple : la somme totale des bitcoins est limitée. Le système est en effet programmé pour que sa masse monétaire totale ne dépasse pas 21 millions d'unité à terme. Lors de sa création en 2009, le rythme de création des nouveaux bitcoins était de 1 bitcoin toutes les 25 minutes. Ce rythme a été environ divisé par deux depuis 2013. La création de bitcoins s'arrêtera donc lorsque les 21 millions programmés auront été créés, ce qui devrait se produire en 2040. Fin 2014, déjà 12 millions de bitcoins avaient déjà été mis en circulation.

Lorsque la création de bitcoins aura cessé, les mineurs seront alors récompensés par une commission prise sur les transactions qu'ils vérifient. Ils auront ainsi toujours une incitation à travailler pour le bon fonctionnement et la sécurité du réseau.

Graphique 51 : Stock et production annuelle de bitcoins
(en millions et en millions par an)



Sources : AMF, Blockchain.info.

III) Différents points de réflexion sur le Bitcoin

Le Bitcoin est un sujet un peu déconcertant au premier abord. Etant vaguement connu, le plus souvent de manière négative, il est facile d'être très surpris lorsqu'on se penche un peu plus en détails sur le sujet. Cette innovation technologique a en effet de nombreuses qualités et ouvre à un certain nombre d'opportunités qui ne sont que trop rarement connues.

1) Le système du Bitcoin et son utilisation présentent des limites morales aussi bien que techniques

a) La possibilité de réaliser des actes frauduleux

Ce qui est le plus ancré dans les connaissances générales, et ce qui ressort le plus souvent, est que le Bitcoin est une monnaie virtuelle, donc non contrôlable par un gouvernement, qui de plus est anonyme, donc fortement utilisée pour toutes les transactions illégales que l'on pourrait imaginer. Cette idée à la peau dure s'est installée dans les esprits à partir d'octobre 2013, date de la première fermeture du site Silk Road par le FBI, plateforme illégale, leader de la vente de drogue en ligne, et qui utilisait le bitcoin comme monnaie d'échange.

Il est en effet vrai que les utilisateurs du réseau Bitcoin peuvent posséder une ou plusieurs adresses (les portes-monnaies électroniques), qui ne sont assimilées qu'à des pseudonymes. Aucune information d'identification nécessaire en dehors du réseau, tel que le nom ou l'adresse par exemple, n'est nécessaire ni demandée sur le réseau. Si les transactions réalisées sont donc publiques, il est donc en revanche difficile de pouvoir connaitre la véritable identité des personnes, propriétaires et bénéficiaires de ces transactions, sur le réseau.
Cet anonymat, associé au manque de régulation sur les monnaies numériques, rend donc cette monnaie fortement attractive pour les utilisateurs, et notamment pour tous ceux qui

chercheraient à réaliser des transactions hors du domaine de la légalité. Le cas de Silk Road, qui utilisait exclusivement le bitcoin, est révélateur. Silk Road était le numéro 1 du marché noir de la vente en ligne de drogue. Le site représentait à la date de sa fermeture prés de 70% du marché de vente de drogue sur Internet. Il permettait également de se fournir en armes, ou encore de s'offrir les services de professionnels de piratage de comptes Facebook ou Tweeter, ou de faux-papiers. L'utilisation du bitcoin offrait aux personnes intéressées un anonymat au cours de leurs transactions sur ce site. Selon le FBI, près de 9 millions de bitcoins ont transité sur Silk Road, pour un total de plus d'1,2 milliards de dollars.

De la même manière, deux autres points sont montrés du doigt lorsque le Bitcoin est évoqué : l'évasion fiscale et le blanchiment d'argent. En effet, comme il a déjà été noté, un certain manque de réglementation et de législation entoure le développement et l'utilisation du Bitcoin. Il est donc permis de craindre de tels trafics monétaires, fortement facilités par la protection offerte par cet anonymat.

b) Un manque de protection des utilisateurs contre le vol ou la perte

Un deuxième point négatif du système du Bitcoin est son manque total de protection vis-à-vis des utilisateurs du réseau. Comme il a été expliqué plus haut, le système du Bitcoin fonctionne entièrement à l'aide de fichiers électroniques. Les bitcoins sont eux-mêmes des fichiers électroniques, stockés dans d'autres fichiers électroniques (les portes-monnaies, ou wallets), et qui sont échangés à l'aide de clés électroniques. De plus, comme aucune entité centrale n'est présente pour coordonner ou surveiller le bon fonctionnement du système, rien n'est prévu et ne peut être activé en cas de perte de bitcoins ou de faille du système. Il suffit simplement à un utilisateur de perdre par exemple ses clés électroniques pour ne plus avoir accès au porte-monnaie contenant ses bitcoins. Aucun recours n'est possible dans ce cas, et les bitcoins sont tout simplement perdus à la fois pour l'utilisateur mais aussi pour l'ensemble du réseau. Il en est de même en cas de suppression malencontreuse de bitcoins. Aucun recours n'est non plus possible après une transaction. Toute transaction est en effet irréversible, quelque soit les circonstances de son exécution, et le système n'est en aucun cas garant de la fiabilité

des vendeurs, encore plus difficile à retrouver en cas de fraude du fait de l'anonymat des adresses Bitcoin.

Enfin, il existe de vrais risques de vols de bitcoins ou encore de déni de service, contre lesquels rien non plus n'est prévu pour assurer les utilisateurs. L'exemple le plus probant est le cas de Mt.Gox, qui était la plateforme d'échange de bitcoins la plus importante en volume. Elle s'est brusquement effondrée en février 2014, supposément du fait d'un piratage informatique qui lui aurait coûté prés de 750 000 bitcoins – ce qui représentait alors 350 millions de dollars. Le site avait suspendu les transactions début février et stoppé toute possibilité de retrait pour les utilisateurs, évoquant un bug informatique. Par la suite le contenu du site a tout simplement disparu, laissant simplement les utilisateurs avec des pertes plus ou moins importantes.

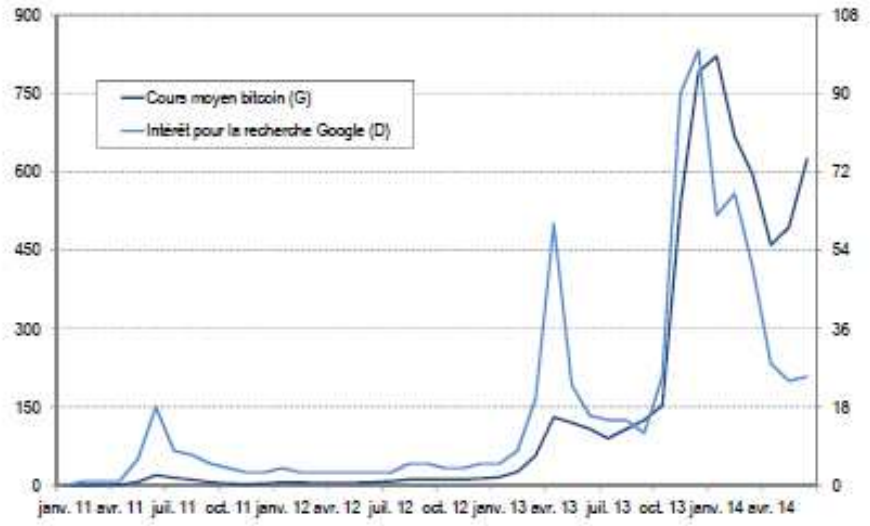
Tous ces risques sont avérés et sont de véritables limites du système de Bitcoin, qui peuvent fortement porter au scepticisme. Cela est d'autant plus vrai que le Bitcoin souffre également d'autres points faibles, qui découlent cette fois de ses caractéristiques propres.

c) Une forte volatilité du cours du bitcoin

Une des plus importante critique faite au Bitcoin est son extrême volatilité, qui est supérieure à celle des devises traditionnelles ou à celle de l'or. Le Bitcoin en effet n'est rattaché à aucune monnaie de référence telle que le dollar américain ou l'euro par exemple, qui sont le plus souvent utilisées comme monnaies de référence. Ainsi, en l'absence d'une autorité régulatrice qui surveillerait le cours de la monnaie, le Bitcoin ne s'échange donc qu'au gré de l'offre et de la demande, et surtout au gré de la spéculation. De plus, les monnaies virtuelles sont entièrement dépendantes de la technologie et des infrastructures informatiques pour pouvoir être créées et fonctionner, ce qui n'est pas sans influer sur le succès de ces monnaies. Dans les faits, une forte corrélation existe entre le cours du Bitcoin depuis le début de l'année 2011 et l'intérêt porté au Bitcoin sur les moteurs de recherche. Il apparaît ainsi que l'appréciation de la valeur du Bitcoin est donc due à des forts effets de réseaux et aux comportements

moutonniers des utilisateurs, qui augmentent donc rapidement la demande de bitcoin. Il y aurait donc une prophétie auto-réalisatrice d'appréciation de la monnaie.

Graphique 50 : Bitcoin : un e-phénomène
(contre dollars et indice Google)



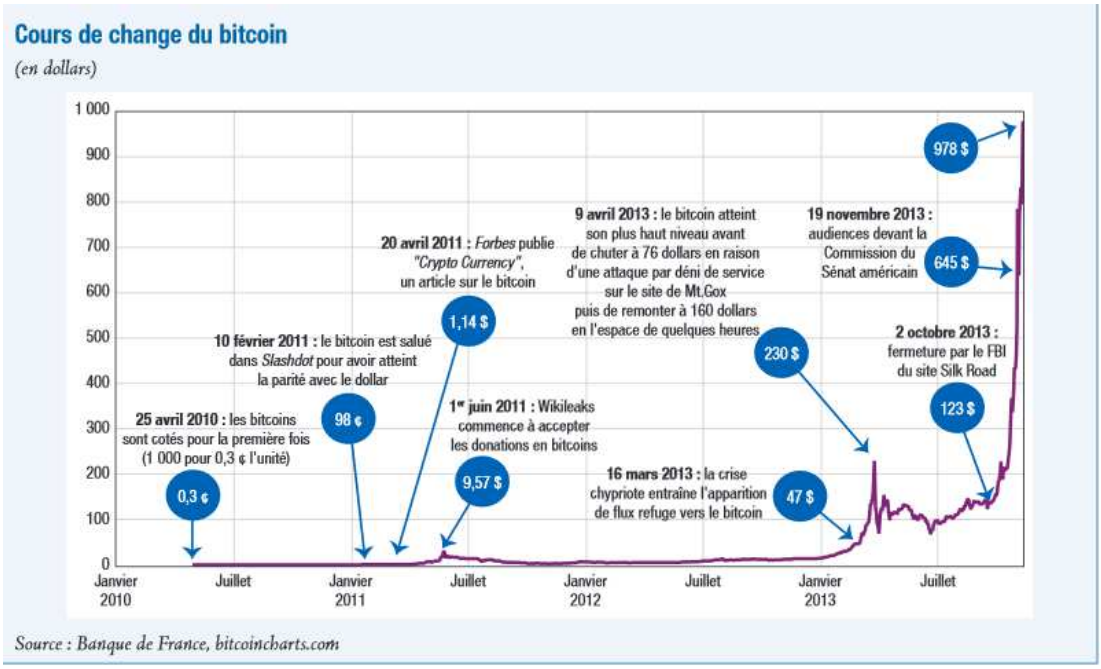
Sources : AMF, Blockchain.info, Google trends. Note : Données de juin 2014 partielles.

Le système du Bitcoin prévoit de plus une création de monnaie non seulement à vitesse descendante - plus les bitcoins créés sont nombreux plus les prochains seront difficiles à obtenir - mais également une création limitée, qui cessera lorsque les 21 millions d'unités prévues auront été créées. A titre d'exemple, en 2009, les bitcoins étaient créés au rythme de 50 nouveaux bitcoins toutes les 10 minutes. En 2013, seuls 25 bitcoins sont créés dans ce même laps de temps. Il est alors fortement tentant de comparer le Bitcoin à de l'or numérique : comme l'or, il est difficile à trouver et sa valeur repose en grande partie sur sa rareté. Il est donc facilement imaginable d'anticiper une hausse incessante de sa valeur, ce qui incite beaucoup à le considérer comme un investissement spéculatif.

Plus qu'une monnaie d'échange le Bitcoin est en effet aujourd'hui de plus en plus utilisé comme un instrument de spéculation. Prés de 55% des bitcoins par exemple ne sont pas en circulation au sein du réseau, mais jouent le rôle d'investissement. De cette utilisation de la monnaie découle donc une importante fluctuation de son cours. En 2013 par exemple, le cours du Bitcoin a varié de 13$ début janvier pour atteindre 166$ à

la mi-août. Au milieu de l'année 2014, les 12,5 millions de bitcoins créés totalisaient une valeur d'environ 7,5 milliards de dollars, soit prés de 600 dollars par unité.

Cette forte volatilité a de multiples conséquences, la première étant d'amoindrir la confiance portée à cette monnaie comme monnaie d'échange. Que faire en effet en cas de perte due aux fluctuations de la monnaie ? Aucune assurance n'est prévue par le système, vers qui peut donc se tourner le vendeur qui perd la valeur du montant de sa transaction ?



2) De nombreux points forts et avantages du système gagneraient cependant à être plus connus

Il serait en effet très incorrect de limiter l'intérêt du Bitcoin à ces points faibles. Si certaines critiques sont légitimement recevables, il ne faudrait pas qu'elles cachent les aspects positifs et innovateurs du système.

a) Un coût de transaction beaucoup plus faible voire quasi nul, ainsi que la possibilité de réaliser des micropaiements

Le point fort essentiel du système de Bitcoin est d'être un réseau décentralisé, qui n'a donc pas d'entité régulatrice pour en contrôler le bon fonctionnement, et qui se passe également d'une tierce entité pour faire le lien entre vendeur et acheteur lors des transactions, rôle que joue dans les deux cas les banques centrales dans le système bancaire actuel.
Ce fonctionnement autonome et de pair à pair - c'est-à-dire directement d'acheteur à vendeur, sans passer par un intermédiaire – constitue sa force principale.

Le premier point essentiel est que les transactions sont de fait plus rapides, et beaucoup moins chères. Il n'y a en effet plus ou presque plus de frais liés aux transactions, qui peuvent atteindre jusqu'à 10% de la valeur de la transaction dans le système bancaire actuel, comme c'est par exemple le cas de la banque Goldman Sachs. Ces frais peuvent atteindre des sommes très importantes qui ne bénéficient pas du tout au consommateur. Chaque année en France, le système des cartes bancaires rapportent 2,7 milliards d'euros, les frais liés aux virements et aux prélèvements 0,7 milliard d'euros, et la gestion des sommes déposées sur les comptes courants prés de 4,7 milliards d'euros. Ces coûts élevés sont une charge importante pour les consommateurs. La grande avancée de cette monnaie est donc de réduire drastiquement les frais, qui ne représentent guère plus que 1% des transactions.
Cette baisse des coûts est également un véritable avantage pour les commerçants, pour qui le système des cartes bancaires représente aussi un coût. En acceptant les paiements en bitcoins cela leur permet de développer leurs commerces ou leurs entreprises tout en réduisant une partie des frais liés à ce développement.

Une autre particularité du Bitcoin est qu'il permet les micro paiements, ce qui est aussi de grand intérêt pour les utilisateurs, ainsi que les commerces et les entreprises. Le bitcoin peut en effet être fractionné jusqu'à 8 décimales, ce qui représente donc des paiements de très faibles sommes, ce qui n'est pas possible avec les devises traditionnelles. Les frais fixes liés aux transactions sont en effet trop importants pour

réaliser des transactions si petites. [11]Le Bitcoin permet donc de réaliser des transactions non possibles jusqu'à maintenant. Un des meilleurs exemples est celui des journaux en ligne, qui font parfois payer la lecture de leurs articles. Or il se peut que les utilisateurs soient intéressés par un ou deux articles en particulier, mais pas par l'ensemble des publications auxquelles l'abonnement permet l'accès. Ils ne s'abonnent donc pas et ne peuvent accéder à ces articles. Le micro paiement permettrait donc de ne payer que l'accès à ce ou ces articles en particuliers.

Enfin cette baisse des coûts des transactions financières offerte par le système du Bitcoin, et notamment des frais sur les transferts d'argent, représente également un véritable avantage entre autre pour les immigrants, qui envoient régulièrement de l'argent à leur famille restée dans leur pays d'origine.

La faible bancarisation de certaines régions du monde a beaucoup profité ces dernières années à certaines plateformes d'échange, particulièrement Money Gram ou encore Western Union par exemple. Ainsi en Afrique, les marges prises par ces plateformes vont de 8 à 12% de la somme envoyée en moyenne, ce qui est un lourd prix à payer pour ces habitants qui font partie des plus pauvres de la planète. Lorsqu'en 2009 la Banque Mondiale a lancé son « objectif 5x5 »[12], qui visait à réduire les coûts des envois de fonds partout dans le monde à 5% maximum, un calcul montrait qu'en cas de réussite, cela permettrait aux migrants africains d'économiser 4 milliards de dollars par an, ce qui est loin d'être négligeable.[13]

Face à ces lourdes marges, le système du Bitcoin propose en revanche des frais beaucoup moins onéreux que les plateformes traditionnelles, oscillant entre 1 et 3%

[11] http://www.lesechos.fr/idees-debats/cercle/cercle-90826-bitcoin-bien-plus-quune-simple-monnaie-dechange-ou-une-valeur-refuge-1001763.php Consulté le 09/10/2015

[12] http://blogs.worldbank.org/voices/fr/objectif-smart-agir-intelligemment-pour-reduire-le-cout-des-envois-de-fonds Consulté le 09/10/2015

[13] Si aujourd'hui le coût global moyen des envois de fonds n'est toujours pas de 5% comme prévu mais de 7,7%, cet effort a tout de même permis à l'ensemble des migrants de la planète et à leur famille d'économiser au total plus de 60 milliards de dollar.

seulement, ce qui en fait une alternative très intéressante et facile d'accès pour ces populations. [14]

b) Le Bitcoin peut être source de bénéfices sociaux, notamment pour les populations en situation d'oppression ou n'ayant pas accès à des services financiers

Un second point essentiel à souligner est l'opportunité d'accès aux services financiers de base qu'offre le Bitcoin à tous ceux qui n'en bénéficiaient pas auparavant. Les populations des régions les plus excentrées de la planète ne peuvent en effet pas toujours bénéficier d'un accès à ces services financiers qu'il faut aller chercher presque exclusivement dans les villes, dans les structures bancaires et financières habilitées à cela, et qui ont de plus un certain coût. L'intérêt du Bitcoin dans ce contexte est de proposer un accès à tous ces services qui ne nécessite qu'une connexion internet (à défaut d'ordinateur, un téléphone portable pourrait donc même suffire).
Ce point est vraiment essentiel. Sans annoncer pour autant que le Bitcoin réussira à résoudre le problème de la pauvreté mondiale, il est cependant important de remarquer qu'une ouverture à des services financiers accessibles est en effet une clé et un levier essentiel dans le développement local de ces régions et de leurs populations. N'ayant pas d'objectif de rentabilité ni de coûts, le système de Bitcoin représente donc ici une véritable avancée que n'a pu jusqu'ici offrir le système bancaire traditionnel.

Un autre véritable bénéfice pour les populations lésées est celui de l'anonymat des transactions financières offert par le Bitcoin, qui apporte cette fois une confidentialité des mouvements de capitaux et une liberté bienvenues.
En effet dans les pays gouvernés par un régime strict, qui souhaiterait que son adhésion et son soutien financier au mouvement d'opposition soit connus par exemple ? Qui souhaiterait qu'un gouvernement puisse suivre à la trace les mouvements de capitaux et les transactions réalisées par les groupes opprimés et peut-être en fuite ?

[14]http://www.huffingtonpost.fr/othmane-zrikem/bitcoin-solution-transferts-dargent-afrique_b_4389534.html Consulté le 09/10/2015

De la même manière, un strict contrôle du capital financier peut être exercé par les gouvernements de certains pays. Le système du Bitcoin permet à l'inverse d'assurer qu'aucune manipulation et qu'aucun contrôle ne puisse être exercé sur les capitaux ou les transactions. Deux exemples récents illustrent ce rôle de monnaie refuge du Bitcoin :

Le premier exemple est celui de l'Argentine, pays dans lequel l'utilisation du Bitcoin ne cesse de croître depuis la crise de 2012. Durant cette période, et encore aujourd'hui, le gouvernement a restreint les mouvements de capitaux, imposé des limites aux possibilités de changer le peso (monnaie argentine officielle) en d'autres monnaies, et exercé un fort contrôle des prix. L'utilisation du Bitcoin a alors permis de faire face à cet état qui manipule sa monnaie et restreint les libertés économiques. Il a permis pour nombre d'argentins de sauvegarder leur épargne.

Le second exemple de taille est la crise chypriote. En mars 2013, l'état chypriote a annoncé qu'une taxe serait appliquée sur l'ensemble des dépôts bancaires des habitants du pays pour aider à renflouer le pays. Finalement, seuls les comptes d'un montant supérieur à 100 000 euros devait être sollicités, mais à hauteur de 30% et plus. Face à cette décision, qui s'apparente de fait beaucoup plus à du vol qu'à une taxe, les épargnants des autres pays en grande difficulté ont eu peur que leur propre gouvernement prenne la même décision. Ainsi en Espagne durant cette période, les applications permettant d'acheter des bitcoins ont connu des niveaux record de téléchargements.

c) La technologie du Bitcoin a permis de résoudre deux grands problèmes informatiques bien connus : la double dépense, et le « problème des généraux byzantins »

La première réponse apportée est celle à un problème bien connu de tout système de paiement, celui de la double dépense. En effet, une des préoccupations communes au système bancaire traditionnel et au système de Bitcoin est de s'assurer que la même unité monétaire, 1 dollar ou 1 bitcoin par exemple, ne sera pas dépensé deux fois par la même personne au cours de deux transactions différentes.

De manière simple, que ce soit au sein du système bancaire traditionnel ou au sein du système de Bitcoin, la masse monétaire stockée est conservée sous forme numérique. Ce sont donc pour ainsi dire des fichiers. Lors d'une transaction ces fichiers sont envoyés d'une adresse à une autre. Mais comment vérifier qu'ils n'ont pas été gardés par l'expéditeur, et que ce dernier ne les utilisera pas de nouveau au cours d'une autre transaction ? Dans le système bancaire actuel les banques jouent le rôle d'intermédiaire au cours des transactions pour vérifier que les utilisateurs sont bien en possession de l'argent qu'ils dépensent et pour suivre ces dépenses. [15]

Le système de Bitcoin en revanche fonctionne de pair à pair, il n'y a donc aucun intermédiaire pour contrôler et réguler le réseau. Comment dès lors éviter ce risque majeur ? Le Bitcoin est la première monnaie alternative à avoir apporté une réponse satisfaisante à cette question, sous la forme de la chaîne de bloc. En effet, grâce au minage et aux différents registres, chaque transaction depuis le tout début du fonctionnement du réseau a été enregistrée et est conservée dans ces registres. De plus, chaque bitcoin créé et mis en circulation sur le réseau est identifié à travers toutes les transactions dans lesquelles il a été impliqué. Il est ainsi possible de suivre « à la trace » tous les mouvements successifs de chacun des 12,5 millions de bitcoins actuellement créés. Il n'est donc pas possible pour un utilisateur d'utiliser plusieurs fois le même bitcoin, les transactions ne seraient pas validées par les mineurs.

Le second apport central de la technologie du Bitcoin est de résoudre le fameux « problème des généraux byzantins », qui soulève la question de la fiabilité d'une transmission donnée et de la fiabilité, ou non, des interlocuteurs. La finalité du problème est de savoir dans quelle mesure et comment puis-je transmettre une information à un interlocuteur que je ne connais pas, et comment être sûr que cette information sera correctement transmise ? [16]

L'énoncé du problème est simple : des généraux byzantins campent autour d'une ville ennemie qu'ils souhaitent attaquer. Ils ne peuvent communiquer entre eux que par

[15] http://www.finance-watch.org/informer/blog/1003?lang=fr Consulté le 22/10/2015

[16] http://www.lesechos.fr/02/06/2014/LesEchos/21699-052-ECH_une-histoire-de-generaux-byzantins.htm?texte=leslie%20lamport# Consulté le 22/10/2015

messagers interposés. La victoire dépendra de la réussite à établir ou non un plan de bataille commun. Cependant certains des généraux peuvent être des traîtres, qui essaieront donc de saboter toute élaboration de plan.
La réponse à ce problème se trouve sous la forme d'un algorithme mathématique qui prend en compte à la fois les différentes informations nécessaires, le transport de ces informations d'un point à un autre, mais également les potentiels problèmes de défaillances du système, qu'elles soient d'origine matérielle, accidentelle, ou encore malveillantes.
Le système innovant du Bitcoin est le tout premier à avoir trouvé une solution pour transférer une propriété digitale sur Internet à un interlocuteur, qui peut être inconnu, tout en garantissant la sécurité de ce transfert, c'est-à-dire que le transfert aura bien lieu, que le contenu ne peut pas être volé ou victime d'une attaque, et que personne ne peut revenir dessus.

3) La difficulté de la mise en place d'une nécessaire réglementation du système, tout en préservant les bénéfices possibles pour le système bancaire actuel

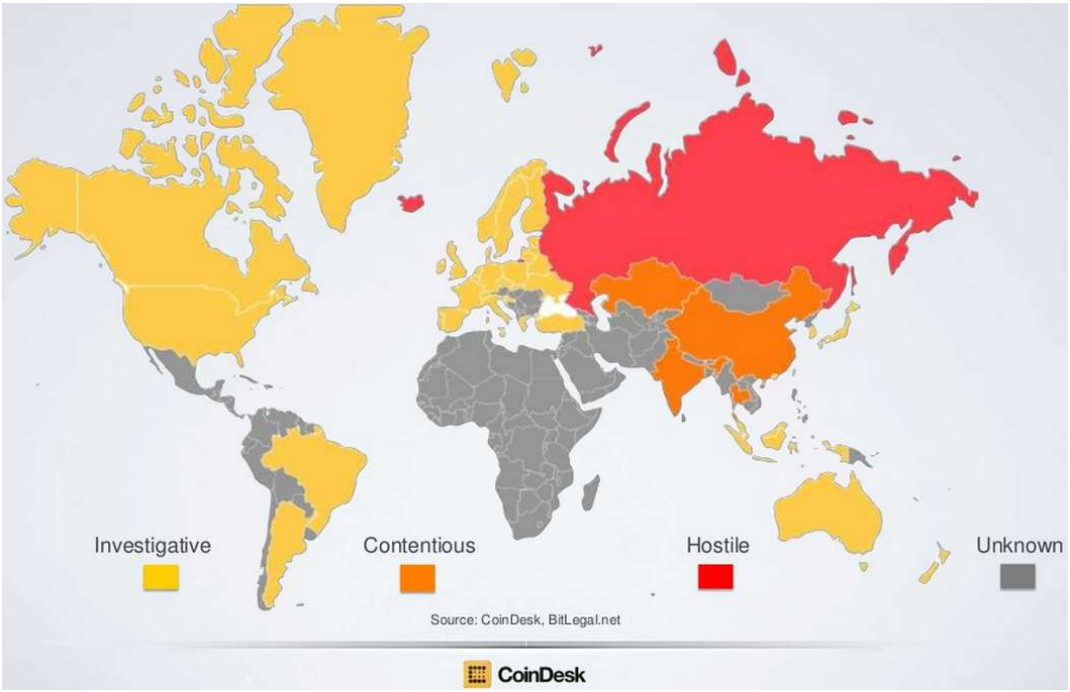
« Bitcoin is either feared because of ignorance or distrusted because of its history. But there is nothing inherently dangerous about Bitcoin. In fact, I think it is a superior medium of exchange than many of the traditional methods of payment we now rely on out of necessity." Joe Cutler *(*"Bitcoin: how to regulate a virtual currency?", *International Financial Law Review*, Sep2013)

Les monnaies virtuelles, et le Bitcoin tout particulièrement, jouant un rôle de plus en plus important dans les transactions réalisées au quotidien à travers le monde, les deux grands défis à relever aujourd'hui sont ceux de la réglementation de ces monnaies, et d'un possible lien avec le système bancaire traditionnel. Il n'est en effet pas envisageable d'imaginer que ces monnaies disparaitront d'elles-mêmes un jour, et il ne serait pas non plus du tout sérieux ni raisonnable de ne pas s'intéresser à ces nouveaux acteurs qui occupent une place de plus en plus importante dans le paysage financier.

a) Réflexion sur une future réglementation

Le premier enjeu majeur est de définir une réglementation et un contrôle, non pas tant des monnaies virtuelles en tant que telle, mais de l'utilisation qui en est faite, ce qui n'est pas si simple. La première grande difficulté de cette tâche vient de la nécessaire utilisation d'internet, qu'il est donc difficile de contrôler. De plus, dans les cas de transactions illégales, ces dernières sont le plus souvent réalisées sur le dark net – l'ensemble des pages internet non référencées sur les navigateurs de recherche – qui représente 80% d'internet, et échappe à tout contrôle. La seconde difficulté provient du système pair à pair du réseau Bitcoin. En effet un tel système peut difficilement être régulé car il résulte de l'accord des utilisateurs entre eux, et ne nécessite aucune entité centrale pour fonctionner. Il apparaitrait donc que seule une action sur les acteurs tiers du système, comme les plates-formes d'échange de monnaie par exemple, peut être envisagée. Il faut cependant noter que cette solution ne permet pas de réglementer l'utilisation effectivement faite de cette monnaie sur internet. En cas de fraude, seule une intervention des forces de l'ordre pourrait alors stopper les activités illicites.

Cette question de la réglementation du Bitcoin a une importance internationale du fait de l'utilisation d'internet. Si les différents états, notamment des pays du G20, ne parviennent pas rapidement à une réflexion commune et à une entente minimale sur ce sujet, le risque est de voir apparaître une non-coordination des juridictions et un arbitrage réglementaire. Or il est difficile pour les différents pays de la planète d'avancer ensemble sur ce sujet. Certaines juridictions ont déjà commencé à réglementer voire à interdire le Bitcoin et son utilisation, quand d'autres commencent à peine à y réfléchir. Définir au plus vite les autorités compétentes pour agir dans ce domaine ainsi que les textes de lois serait pourtant essentiel pour limiter les risques de fraude liés à l'utilisation du Bitcoin.



La question de la réglementation du Bitcoin est complexe et vaste. Que faut-il exactement réguler ? Les transactions ? Les caractéristiques de la monnaie (son anonymat, son émission automatique …) ? Ou faut-il agir en amont, en palliant les faiblesses du système ? Si les avis divergent, une opinion est cependant unanimement partagée: il ne faut surtout pas complètement interdire son utilisation. Le risque d'une interdiction complète de la monnaie et de son utilisation pourrait en effet avoir comme première conséquence de promouvoir fortement son attrait et son développement souterrain. En outre simplement interdire le Bitcoin ne résoudrait en rien la question présente. En effet une multitude de monnaies rivales similaires au Bitcoin se sont déjà développées (Litecoin, Worldcoin, Mastercoin par exemple), et de nouvelles technologies apparaissent sans cesse dans ce domaine. Les futures législations devront donc se positionner au-delà d'une simple interdiction d'une monnaie en particulier pour s'étendre sur un terrain global.

De plus, dans quelle mesure peut-on réguler le Bitcoin sans lui faire perdre son objectif premier ? Les utilisateurs du Bitcoin évoquent le plus souvent deux facteurs clés pour justifier leur adhésion au système : l'idéologie proposée par cette monnaie – contourner le système bancaire actuel et ses multiples intermédiaires –, et la recherche

de frais de transactions faibles. Le défi est dés lors d'instaurer une régulation qui permette de contrôler les défaillances possibles du système tout en conservant et protégeant ses divers avantages. Malgré les nombreuses critiques qui peuvent lui être adressées, force est de constater que le système du Bitcoin propose un bénéfice majeur : celui de réaliser des transactions rapides, y compris des micros transactions, à moindre coût, sans bureaucratie ni frais de transaction excessifs. Quelle orientation alors prendre pour relever cette double contrainte ?

Une des propositions les plus plébiscitées est de s'attaquer au défi posé par l'anonymat proposé par le système, tout en permettant le développement des « trust-less transfers » (transactions sécurisées de pair à pair sans pour autant avoir de multiples garanties sur la confiance que l'on peut accorder aux différents acteurs impliqués. Cf « le problème des généraux byzantins »). De cette manière, les législateurs permettraient d'encourager l'utilisation des nouvelles technologies avec un fort impact social. Cela favoriserait en effet la concurrence dans le domaine de l'offre des services financiers – qui serait particulièrement bienvenue dans le secteur des cartes de crédit et des virements bancaires, aujourd'hui monopole des institutions bancaires traditionnelles - et ainsi le bien-être des utilisateurs.
La plus grande source d'inquiétude pour les législateurs semble donc être l'anonymat des acteurs des transactions. Identifier ces acteurs permettrait de contrôler les fraudes fiscales, les risques de blanchiment d'argent, et améliorerait la protection des utilisateurs. L'Etat aurait entre autre un rôle à jouer pour donner des lignes directrices et des conseils de prévention à tous ceux qui souhaiteraient utiliser ces monnaies sur les risques associés et les précautions à prendre.

3 axes principaux semblent donc se démarquer pour orienter les régulations à venir :

- Encourager l'usage des nouvelles technologies qui permettent d'améliorer la concurrence au sein du secteur des moyens de paiements ;
- Rendre obligatoire l'identification des acteurs des transactions réalisées en monnaies virtuelles ;
- Assurer une protection minimale aux utilisateurs.

Toutefois une question majeure reste encore en suspens. Réfléchir à une future régulation du Bitcoin est une bonne chose, mais comment réguler ce qui n'est pas encore défini ? Cette première étape n'est pas des plus aisées.

Le statut juridique et réglementaire des monnaies virtuelles n'a pas encore été clairement défini aujourd'hui et pose de nombreuses questions. Le Bitcoin n'est ni une monnaie légale, ni un moyen de paiement couvert par la Directive des services de paiement au niveau européen. Il n'est pas non plus considéré comme un moyen de paiement par le Code monétaire et financier français, car la monnaie n'est pas émise contre remise de fonds. Plusieurs propositions sont donc possibles pour qualifier le Bitcoin. Il peut être considéré comme produit bancaire, comme marchandise, ou encore par exemple comme mesure financière servant de support à des contrats financiers. Les interrogations sur ce sujet sont aujourd'hui nombreuses, mais tant qu'un cadre légal ne sera pas posé pour encadrer cette monnaie, aucune protection ne sera possible pour la réguler en tant que moyen de paiement.

De la même manière, comme le Bitcoin n'est juridiquement pas qualifié, il ne peut être pris en compte de manière comptable que comme un actif physique, et non comme un actif financier, ou comme monnaie/trésorerie. Il n'est de plus pas évident de réussir à valoriser une trésorerie détenue en monnaie virtuelle, ou bien un produit ayant pour sous-jacent une monnaie virtuelle. [17]

b) De possibles bénéfices pour le système bancaire ?

Si le système bancaire traditionnel et les monnaies virtuelles, à l'image du Bitcoin, semblent complètement s'opposer voire se rivaliser, il n'est pas certain qu'un possible rapprochement n'est pas lieu dans un futur plus ou moins proche. D'un certain point de vue, il pourrait même apparaître que les banques et le Bitcoin ont mutuellement besoin de leurs points forts respectifs. Le système du Bitcoin a créé une nouvelle manière de transférer des fonds et de réaliser des paiements sans intermédiaire et à moindre coûts. Dans le même temps, l'industrie bancaire a vu le nombre de ses régulations ainsi que le

[17] ***Cartographie 2014 des risques et tendances sur les marchés financiers et pour l'épargne***, par l'Autorité des Marchés Financiers (AMF), Juillet 2014

contrôle politique sur ses activités fortement augmenter, notamment depuis la crise de 2007. Ces changements ont eu entre autre pour effet d'augmenter les coûts du secteur, ainsi que les durées d'exécution des transactions, rendant en outre cette industrie de moins en moins profitable. Un éventuel partenariat ou rapprochement entre le système du Bitcoin et le secteur bancaire traditionnel pourrait alors être bénéfique à la fois aux entreprises et à leurs clients/utilisateurs.

Tout d'abord, grâce aux innovations technologiques apportées par le Bitcoin, le système bancaire traditionnel bénéficierait d'une approche innovante et rajeunie d'être en relation avec ses clients et les autres banques. De plus ces mêmes innovations technologiques offrent des coûts de transfert de fonds beaucoup plus faibles, ce qui n'est pas sans intérêt au regard des coûts actuels du secteur. A titre d'exemple, la gestion de l'argent liquide et la gestion des chèques bancaires coûtent respectivement chaque année 2,6 milliards d'euros et 2,4 milliards d'euros aux banques.[18] Face à ces forts désavantages concurrentiels, cette adaptation pourrait rapidement devenir bien plus une nécessité qu'un simple avantage pour les banques, au risque de voir une partie importante de leurs fonds se convertir en Bitcoin.[19]

Le système du Bitcoin pour sa part pourrait largement bénéficier de la légitimité des banques ainsi que de leur structure en accord avec les législations en place. De nombreuses entreprises ou intermédiaires du système du Bitcoin (les plateformes d'échange à l'entrée par exemple) n'ont en effet ni les ressources ni les connaissances exactes pour se conformer aux diverses lois et régulations en vigueur, en particulier les lois contre la fraude et le blanchiment d'argent par exemple, ce qui les empêche soit d'être en conformité avec la loi, soit de continuer à se développer. Dans ce contexte les banques pourraient être un atout pour ces acteurs, en les aidant à comprendre et endosser leurs responsabilités, et ainsi se développer plus encore auprès de nouveaux utilisateurs.

---

[18] Herlin P. (2013), « La révolution dans les monnaies : contourner les banques et les Etats », in ***La Révolution du Bitcoin et des monnaies complémentaires : Une solution pour échapper au système bancaire et à l'euro*** *?*

[19] Thomas Z., "Why Bitcoin could be the key to banking's future?", ***International Financial Law Review***, Jun2014

Une fois qu'ils auront atteint le système bancaire ou les acteurs du système du Bitcoin, tous ces bénéfices se transmettraient par ricochet aux clients et aux utilisateurs, ce qui améliorerait grandement la santé générale du marché. De plus, cela serait également bénéfique pour les gouvernements, pour qui il deviendrait beaucoup plus aisé de réguler les monnaies virtuelles.

Deux limites cependant sont à poser qui pourraient être un frein à de tels changements. Tout d'abord, imaginer un tel rapprochement avec le système bancaire relève du paradoxe pour le système du Bitcoin. Ce système en effet a justement été imaginé et mis en place dans l'idée finale de contourner les banques et leur système, de ne plus avoir besoin d'elles et de pouvoir être totalement autonome vis-à-vis de leur contrôle et/ou supervision. Cependant, afin de gagner une légitimité suffisante pour pouvoir continuer à se développer, le Bitcoin aurait besoin de se rapprocher de ce même système qu'il fuyait auparavant. Il semble donc difficile aujourd'hui d'imaginer ce qu'il en adviendra.

De plus, si un tel partenariat pourrait en effet être bénéfique aux deux systèmes, il n'a toujours pas été mis en place du fait justement de l'incertitude légale et régulatoire qui entoure le Bitcoin. Les banques sont trop frileuses pour le moment pour accepter de manière générale un rapprochement de la sorte.

Formulation des hypothèses :

Après avoir étudié les différentes composantes du système du Bitcoin ainsi que ses diverses applications possibles, notre étude portera sur la vérification de la véracité des connaissances populaires du Bitcoin, qui lui font le plus souvent mauvaise presse. Cela se fera plus particulièrement au travers de trois axes d'étude spécifiques :

- Le Bitcoin aurait aujourd'hui une réputation qui n'est pas justifiée, due à certains usages trop connus de cette monnaie pour des transactions illicites ;

- Le Bitcoin offre de nombreuses opportunités et améliorations face au système bancaire et financier actuel ;

- La réglementation et l'intégration du Bitcoin dans le système financier pourraient être les défis à relever dans les années à venir.

METHODOLOGIE

I) Démarche réflexive de départ

Ma démarche de réflexion pour ce mémoire a débuté en avril 2014, à la lecture d'un article du Courrier International, *Le Bitcoin expliqué à ma mère*[20], dans lequel l'auteur dépeint rapidement le fonctionnement de cette nouvelle monnaie électronique à la lumière des récents évènements du à la fermeture du site de Silk Road en octobre 2013 par le FBI. Ce site, qui a depuis été de nouveau ouvert anonymement, était très connu pour être une des plus grandes plates-formes de vente en ligne de tous types de produits illicites, notamment de la drogue et des armes, ainsi que des services tels le piratage de comptes. La spécificité première de ce site était entre autre d'utiliser exclusivement le Bitcoin pour régler ses achats du fait, comme l'expliquait simplement l'article, du caractère anonyme des transactions réalisées.
La lecture de cet article se terminait ensuite simplement par quelques chiffres et informations générales sur le Bitcoin, qui mettaient en lumière son développement croissant incessant depuis quelques années et notifiaient entre autre la mise en service de distributeurs de Bitcoin dans les plus grandes métropoles du monde, en particulier Paris, Vancouver, ou encore Berlin.

Ne connaissant alors pas, ou très peu, le Bitcoin je suis restée en suspens à la fin de cette lecture. Il me restait en tête que cette monnaie virtuelle était anonyme, qu'elle représentait donc un boulevard grand ouvert sur internet pour toutes sortes de transactions illicites pour les acteurs mal attentionnés, et que personne n'y pouvait rien puisqu'aucune entité ou autorité n'était en charge de cette monnaie. Et cependant son

[20] http://www.courrierinternational.com/article/2014/04/03/le-bitcoin-explique-a-ma-mere Consulté le 30/10/2015

utilisation et sa renommée ne faisait que de grandir au point de l'en rendre accessible à tous, publiquement, dans les centres-villes des plus grande métropoles du monde.

Si cette monnaie ne servait qu'aux trafics illégaux, le monde entier devenait-il contrebandier en s'intéressant ainsi de plus en plus au phénomène ? Les gouvernements supportaient-ils alors le développement de cet outil de trafic en autorisant l'installation des distributeurs dans leurs villes ? De plus, comme cette monnaie n'est indexée sur aucune monnaie ou matériau digne d'en garantir la confiance, quel intérêt pourrait avoir qui que ce soit à l'utiliser ? Pourquoi alors le nombre de ses utilisateurs ne cessait-il d'augmenter ?

Quelques recherches rapides sur internet m'ont confirmé à maintes reprises que le Bitcoin, lorsqu'il est connu, ne l'est presque exclusivement qu'au prisme de l'affaire de Silk Road, et jouit donc d'une très mauvaise réputation qui le condamne tout entier. Mais je n'ai pas réussi à trouver une once d'information sur l'intérêt que pouvait représenter cette monnaie pour des acteurs économiques sans intention particulièrement mauvaise. Intriguée par le sujet, j'ai donc décidée d'y consacrer ce travail de recherche, poussée par la curiosité.

II) Les méthodes utilisées pour mener à bien cette recherche

1) Articles académiques et publications officielles

La première source d'information traitant du sujet en profondeur a été les articles académiques, lors du travail pour le document intermédiaire du mémoire et par la suite. La littérature académique, à la différence des articles de journaux d'information, apporte un éclairage beaucoup plus complet sur le Bitcoin, notamment sur le fonctionnement du système. De plus, si Silk Road est parfois cité à titre d'exemple, l'attention principale de ces articles n'est pas portée sur cette affaire et ce côté sombre du Bitcoin, à la différence des journaux d'information. J'y ai donc découvert le fonctionnement complet du système, avec ses technicités particulières, les risques

potentiels, ainsi que l'utilisation possible et toutes les nouvelles opportunités qu'offre cette monnaie.

Dans un deuxième temps je me suis intéressée à divers rapports officiels portant sur le sujet. Ces publications - publiées par la Banque de France, l'Autorité des Marchés Financiers, ou encore la Banque Centrale Européenne au cours des deux ou trois dernières années – m'ont apporté un éclairage tout à fait nouveau. En effet, publiées à la suite de recherches et d'études spécialisées, elles reflètent le niveau de connaissance concrète et d'actions actuelles de la part du système bancaire et financier vis-à-vis du Bitcoin. Les risques présentés ne sont plus de simples hypothèses théoriques mais une réalité qu'il convient de prendre en compte.

2) Investigation sur le terrain

Pour vérifier mes hypothèses de recherche j'ai fait le choix d'orienter ma recherche terrain vers une étude qualitative, plutôt qu'une étude quantitative. En effet, le sujet du Bitcoin est peu connu du grand public, et demande de plus une certaine compréhension de ses spécificités techniques. Faire appel à des professionnels au travers d'une étude qualitative m'a donc semblé être la méthode la plus pertinente. Il s'agissait d'analyser dans le détail la réalité du Bitcoin, au-delà des théories et des possibilités que peut offrir la monnaie, et surtout son impact réel aujourd'hui et dans les années à venir sur le système bancaire, monétaire, et financier. Il me fallait donc comparer ce que j'avais pu lire dans les différents articles étudiés et la réalité de l'utilisation du Bitcoin.

A l'aide d'un guide d'entretien, j'ai donc réalisé des entretiens semi directifs. Mon questionnaire type, élaboré à l'avance pour regrouper au mieux les interrogations liées à mes hypothèses, me permettaient d'orienter mes questions et mes remarques sur les sujets qui m'intéressaient. Cependant les questions étaient majoritairement ouvertes et complémentaires les unes par rapport aux autres. Cela me permettait ainsi de laisser parler librement mon interlocuteur sur le sujet, couvrant ainsi parfois des points que je n'avais pas prévu d'aborder, et me permettant de rebondir sur ses propos afin d'affiner ou de demander plus de précisions sur certains points.

Enfin je me suis naturellement tournée vers le secteur des professionnels pour réaliser ces entretiens. Le sujet étant technique et peu connu, il me fallait directement aller frapper aux portes des grands pôles de recherches afin d'entrer en contact avec des spécialistes du sujet. Je me suis donc orientée vers la Banque de France et la Banque Centrale Européenne, qui ont toutes deux publiées plusieurs rapports et articles sur ce sujet à la suite de recherches, et qui ont apporté un point de vue d'analyse technique et opérationnelle sur le sujet. J'ai également contacté un des auteurs des divers articles académiques que j'ai pu étudier, ce qui m'a permis d'avoir un avis académique sur mes recherches. J'ai enfin pris contact avec un entrepreneur ayant travaillé dans le secteur du Bitcoin pour les entreprises, ainsi qu'un ancien mineur qui ont tous deux apporté un éclairage très différent de celui du secteur bancaire.

J'ai élaboré mon guide d'entretien en trois parties, chacune ciblant une hypothèse de recherche particulière, afin d'aborder ces trois axes de la manière la plus complète possible.
Ce questionnaire a dans les faits été un guide, me permettant de garder un fil rouge cohérent, mais les entretiens n'ont jamais véritablement répondu à toutes les questions précisément. Elles étaient plus un prétexte pour engager la discussion sur un sujet en particulier, et mon interlocuteur répondait ainsi le plus souvent à plusieurs questions à la fois en parlant librement au fil de ses pensées.

GUIDE D'ENTRETIEN

1) <u>La réalité du Bitcoin aujourd'hui confrontée à sa médiocre réputation :</u>

- Qui utilise le Bitcoin aujourd'hui ?
- Quelles sont les transactions les plus couramment réalisées en Bitcoin ?
- Quels sont les risques que présente réellement le Bitcoin ?
- L'idée que le Bitcoin favorise les transactions illégales (blanchiment d'argent, marché noir, fraude fiscale) grâce à l'anonymat est-elle justifiée ?

- L'affaire de Silk Road est-elle représentative de l'environnement du Bitcoin ?
- Quels sont les freins les plus importants au développement du Bitcoin ?
- Peut-on penser que l'utilisation du Bitcoin va continuer à croître et à toujours plus se développer ?

2) Les opportunités et avantages du Bitcoin, notamment pour le système bancaire :

- Peut-on considérer le Bitcoin comme une réelle monnaie alternative au système bancaire actuel ?
- Le Bitcoin est-il vraiment un moyen de contourner le système bancaire actuel ?
- Son développement peut-il à la longue être néfaste pour le système bancaire ? Pourquoi ?
- Le Bitcoin apporte-t-il un complément ou avantage par rapport au système bancaire actuel ? Quel est-il ?
- Comment peut-on expliquer l'attrait croissant du Bitcoin pour les utilisateurs ?
- Peut-on réellement envisager une convergence de ces deux systèmes dans les années à venir ? De quelle manière ?
- Une convergence ou une coordination des deux systèmes serait-elle souhaitable voire bénéfique ? Pourquoi ?
- Les deux systèmes peuvent-ils sinon fonctionner en parallèle ?

3) Les défis de la réglementation et de l'intégration du Bitcoin dans le système financier :

- Sur quels aspects du Bitcoin est-il essentiel de légiférer ? Comment mettre de telles législations en place ?
- Est-il réellement possible d'encadrer le système du Bitcoin malgré les difficultés liées à Internet ?
- En quoi la technologie du Bitcoin (cryptographie et chaine de blocs) pourrait-elle être bénéfique au système bancaire actuel ?

- Un nouveau système bancaire utilisant la technologie de la cryptographie est-il vraiment une possibilité pour les années à venir ?
- Quels seraient les défis à relever pour mettre en place ce nouveau système bancaire ?
- Quels en seraient les bénéfices à la fois pour les banques et pour les utilisateurs ?
- Quels en seraient les inconvénients ?
- Qu'adviendrait-il alors du Bitcoin et des autres monnaies cryptographiques ?

III) Les difficultés rencontrées

1) La difficulté du sujet

La première difficulté que j'ai rencontrée dans ce travail a été celle de travailler sur un sujet récent et peu connu. Le Bitcoin a été créé en 2009 et n'a réellement commencé à être connu qu'à partir de 2012 ou 2013. La littérature académique sur le sujet est donc encore peu abondante, et peu variée. Il m'a été difficile de trouver le nombre demandé minimum d'articles académiques, mais surtout de livres. Très peu d'ouvrages sont encore consacrés à ce sujet, la plupart ne l'évoquent qu'au cours d'un chapitre ou de quelques paragraphes. La recherche d'informations nouvelles a donc été minutieuse. Elle consistait la plupart du temps à cibler la petite information spécifique à un article parmi ses multiples pages, qui apportait un point supplémentaire à l'ensemble des connaissances déjà accumulées.

2) Les difficultés dans les prises de contact

La deuxième difficulté majeure rencontrée s'est présentée lors de la recherche terrain et de la prise de contacts avec les professionnels. Le sujet nécessitant une étude qualitative j'ai donc contacté des personnes compétentes sur le sujet.

La première tâche fut d'arriver à obtenir les noms et/ou coordonnées des personnes pouvant être en mesure de m'aider, notamment à travers les dédales de services et des différents bureaux de certaines institutions.

De plus, certaines personnes ont clairement fait preuve de réticences à l'idée d'être citées ou de parler au nom d'une institution au sein de ce mémoire. C'est pourquoi les personnes interrogées seront citées au début de la seconde partie de ce mémoire, mais ne sont pas explicitement citées dans le corps du texte.

Enfin, les personnes compétentes sur ce sujet travaillant souvent à des postes importants au sein du système bancaire ou ailleurs, il a été difficile de garder contact avec eux jusqu'à la fin de ma recherche (mail de notification d'absence prolongée, rendez-vous téléphoniques annulés etc).

3) Ecueil de la répétition

Tout au long de la rédaction de ce mémoire il m'a enfin été difficile de ne pas tomber dans le piège de la répétition. En effet, certaines informations recueillies dans l'analyse des articles académiques pouvaient parfois apporter un élément de réponse à une de mes hypothèses. Il m'a ainsi été quelques fois difficile de bien dissocier l'analyse de l'état de l'art et le résultat de ma recherche sur le terrain.

RESULTATS ET VALIDATION DES HYPOTHESES

Différents interlocuteurs m'ont permis de poursuivre mon raisonnement autour de mes hypothèses de recherche en acceptant de répondre à mes questions. Comme tous ne souhaitent pas être explicitement cités par la suite pour des raisons de confidentialité, voici dés à présent le nom et les fonctions des personnes qui ont accepté de m'aider et qui sont à la source de toute cette seconde partie.

- BRARD C., mineur de bitcoin
- CAUDERLIER A., Bitcoin et blockchain entrepreneur
- De JONG I., expert à la Direction Générale Infrastructure de marché et paiements (Banque Centrale Européenne)
- FAVIER J., auteur de « La Voie du Bitcoin »
- RAYMAEKERS W., Head of Banking market (SWIFT)
- STERVINOU A., Chef du Service de la Surveillance des moyens de paiements scripturaux (Banque de France)

I. Avancée de la recherche à la suite des entretiens

1) La médiocre réputation populaire du Bitcoin n'est ni justifiée ni légitime

Malgré sa sombre réputation, le Bitcoin n'est pas dans les faits un formidable accélérateur de trafics illégaux en tout genre. Tout d'abord quelques chiffres permettent de remettre ces idées en perspective. En termes de trafics illégaux, les transactions réalisées sur Internet en Bitcoin ne représentent environ que 1 % du total des transactions de produits illicites dans le monde, ce qui est bien peu[21]. De la même manière, il est difficile de réellement affirmer que le Bitcoin joue un rôle actif dans le financement du terrorisme. L'EI par exemple, dont il a été avancé que l'organisation se finançait en partie grâce au Bitcoin, ne possède que 5 bitcoins dans son porte-monnaie électronique[22], ce qui représente environ 1000 dollars. Face aux 800 millions de dollars par an de revenus pétroliers de l'organisation, cette contribution est donc tout à fait dérisoire.

Un point essentiel à mettre en valeur est que le Bitcoin a un certain nombre de similitudes avec l'argent cash. En effet, lorsque deux individus réalisent une transaction avec du cash, il n'y a pas d'intermédiaire entre eux pour assurer la garantie de la transaction, et aucune trace de la transaction n'est gardée dans un livre de compte par exemple. De plus, si ces deux individus ne connaissent pas leurs identités réciproques, la transaction est alors complètement anonyme. Il est en outre intéressant de remarquer que le Bitcoin ne crée pas de nouveaux marchés. Son utilisation favorise ou facilite peut-être certains types de transactions sur des marchés spécifiques, mais ces marchés n'ont pas été mis en place grâce au Bitcoin. Ils existaient bien avant, même sur Internet. Ainsi, de la même manière que le cash, le Bitcoin peut être utilisé pour de bonnes ou de

[21] https://le-coin-coin.fr/1972-terrorisme-blanchiment-trafic-le-bitcoin-se-defend/ Consulté le 13/11/2015

[22] https://blockchain.info/address/13Pcmh4dKJE8Aqrhq4ZZwmM1sbKFcMQEEV Consulté le 13/11/2015

mauvaises transactions. La grande majorité des transactions illicites qui ont lieu chaque jour sont réalisées en cash, des valises le plus souvent pleines de billets de 100$ ou plus circulent dans de nombreux pays. Le cash n'a pas pour autant une mauvaise réputation ni ne rencontre de volonté de l'interdire entièrement. Cela dépend de l'utilisation qui en est faite. Il en va de la même manière pour le Bitcoin. Quelques chiffres permettent rapidement d'illustrer ce point : la capitalisation totale du Bitcoin aujourd'hui est d'environ 5 milliards de dollars. Le marché de la drogue dans le monde aujourd'hui représente environ 2000 milliards de dollars. Donc même si l'ensemble de la masse monétaire du Bitcoin était consacrée au commerce de la drogue, cela resterait dérisoire – 0,25% - au regard de la grandeur du marché.

Une différence majeure en revanche est que, à la différence du cash, le Bitcoin est transparent, et finalement peu anonyme. En effet, comme il a été expliqué dans la 1ère partie, toutes les transactions réalisées sur le réseau Bitcoin depuis le tout premier bloc sont consignées sur la chaîne de bloc. La traçabilité est donc complète et possible à tous moment. De plus, les transactions Bitcoin sont réalisées entre deux clés (ou adresses) publiques, et ne sont donc pas totalement anonymes. Il existe différentes techniques, s'appuyant par exemple sur les adresses IP ou sur l'historique des transactions, permettant de briser cet anonymat relatif qui sont connues des informaticiens et agences de sécurité nationale des différents pays, à l'image de la bien connue NSA aux Etats-Unis.
Enfin, la chaîne de bloc conservant la trace de toutes les transactions jamais réalisées, l'identification des utilisateurs peut donc être rétroactive. Une transaction frauduleuse réalisée par exemple en 2011 sur Silk Road pourra donc être identifiée et punie bien longtemps après avoir été réalisée, par exemple en 2020.

Ainsi, si une fois couplé à d'autres technologies existantes - telles que le réseau anonyme Tor par exemple - le Bitcoin peut faciliter certaines transactions, il n'est pas exact d'affirmer qu'il favorise d'emblée les actes frauduleux. Il apparaît en effet que s'il n'est pas « pire » que le cash, il représente peut-être même moins d'avantages de part la traçabilité complète de toutes ses transactions et des adresses associées. Certains

spécialistes de la question affirment même que c'est le moyen d'échange le plus ouvert et transparent qui n'ait jamais existé.

2) La projection de multiples opportunités est à grandement modérer

Prouesse technologique reconnue, le système du Bitcoin possède de nombreuses améliorations et innovations qui font défaut au système bancaire traditionnel : des transactions à moindre coût, la possibilité de réaliser des micro-transactions, la liberté économique pour les populations opprimées, l'accès à des services bancaires de base pour les personnes qui en sont aujourd'hui privées, l'accès à une monnaie où aucune manipulation n'est possible etc.

Cependant dans un grand nombre de cas, il apparaît que ces multiples possibilités doivent être considérées avec précaution, ou tout du moins avec un certain recul. Selon A. Stervinou, chef du Service de la Surveillance des moyens de paiements scripturaux au sein de la Banque de France, ces innovations sont très théoriques et ne se retrouvent que très faiblement dans la réalité.

Tout d'abord il ne faut pas oublier qu'utiliser le système de Bitcoin nécessite une certaine technologie et un certain équipement qui ne sont pas à la portée de tout le monde. Pour les populations de la brousse africaine trop éloignées des grandes villes pour avoir accès aux établissements financiers les plus proches, palier ce manque grâce au Bitcoin signifierait d'avoir accès à un réseau Internet, avec une connexion de préférence 3G ou même 4G, ainsi qu'un smartphone ou un ordinateur portable. Il est difficilement imaginable d'imaginer une telle situation. Utiliser le Bitcoin nécessite en effet, du moins aujourd'hui, d'être déjà intégré économiquement.

De la même manière, lors d'une transaction financière entre pays, par exemple dans le cas des immigrants, le système répond-il véritablement aux besoins actuels des différentes parties prenantes de la transaction? La réponse aujourd'hui semble être non. Il est vrai que ces transferts d'argent à l'international à moindre frais sont un énorme avantage pour les personnes vivant dans les pays développés. Mais qu'en est-il des

personnes ou des petites entreprises qui les reçoivent ? Auront-elles elles aussi accès à l'équipement et à la technologie nécessaire pour recevoir, convertir et enfin utiliser cette transaction en Bitcoin dans les villages ruraux d'Afrique ou au cœur de la campagne vietnamienne par exemple ? Souhaitent-elles de plus réellement recevoir de la monnaie digitale au lieu d'un virement traditionnel sur un compte bancaire, ou même de la monnaie papier ? Pour le moment du moins, le système du Bitcoin n'a pas encore réussi à prendre en compte ces aspects pratiques du côté des receveurs à l'inverse du système bancaire traditionnel qui tire sa force de son énorme réseau. Même dans les endroits les plus reculés de certains continents, il est possible d'utiliser les présences locales d'un petit magasin ou d'une agence de poste pour faire le lien entre les institutions bancaires et les populations. Ce n'est pas encore le cas pour le Bitcoin.

Le second point à nuancer est celui de la garantie de sécurité que pourrait offrir le Bitcoin face à un gouvernement qui contrôlerait le capital financier et manipulerait les transactions financières. Cela peut évidemment paraître idéal de trouver une monnaie refuge pour placer ses capitaux loin de toute tentative de manipulation. Cependant le Bitcoin ne possède pas les qualités nécessaires afin de pouvoir jouer ce rôle. Les phénomènes qui ont pu être observés lors de la crise grecque ou argentine sont plus épidermiques et ponctuels que preuves réelles de l'émergence d'une nouvelle valeur.

Deux qualités principales sont en effet attendues d'une valeur refuge : un risque minimal, afin d'être garant de la valeur d'origine, et une bonne liquidité. Or le Bitcoin est encore aujourd'hui une valeur hautement spéculative, et peut même difficilement pour certain être considéré comme une monnaie du fait qu'aucun système de confiance n'en soit garant. Au-delà de sa volatilité bien connue il semble que ce système soit extrêmement fragile, même dans les cas a priori les plus sûrs à l'exemple de la plateforme d'échange Mt.Gox. Comment accorder confiance à un système dont même la tête de pont peut parvenir à couler en quelques jours? Le Bitcoin paraît donc encore loin de pouvoir rassurer dans ses capacités, malgré l'idée de liberté, quelque peut illusoire sûrement, qu'il offre à certains.

Enfin, si le Bitcoin, pour de bonnes ou de mauvaises raisons, devient une valeur refuge pour certains, qu'adviendra-t-il par la suite lorsqu'ils souhaiteront récupérer leur monnaie investie ? Aucune institution ou aucun système ne garantit pour le moment le système de Bitcoin. Ainsi, si les personnes ayant investi dans le système ne trouvent pas de nouveaux utilisateurs pour racheter leurs bitcoins, elles auront perdu dans le processus l'ensemble de la valeur qu'elles espéraient protéger. Il est donc d'un certain point de vue possible de comparer le système de Bitcoin à un système de Ponzi – système où les clients sont rémunérés par l'apport des investisseurs entrants – montage financier frauduleux qui s'écroule à partir du moment où les apports des investisseurs entrants ne suffisent plus à rémunérer les clients. Et il n'est pas aujourd'hui évident d'affirmer que le Bitcoin existera toujours, à l'image de dizaines de monnaies alternatives, comme les monnaies locales, déjà créées dans le passé et qui ont toutes fini par passer.

Le dernier point à nuancer est celui de la sécurité que pourrait offrir le Bitcoin aux populations ou à certains groupes de personnes opprimés par les régimes politiques en place, et qui chercheraient la confidentialité de leurs mouvements bancaires. Aucune certitude sur ce point ne peut démontrer qu'il est illusoire et purement théorique, mais avec un peu de recul il semblerait étonnant qu'un gouvernement d'oppression ne regarde que les mouvements bancaires. Si une surveillance est faite, elle sera complète et largement déployée, à l'image des autorités chinoises par exemple qui exercent une surveillance et une régulation sur le secteur des télécoms.
Le Bitcoin peut-il vraiment aider dans certains cas ? Peut-être, mais il n'est pas certain qu'il y ait beaucoup à y gagner.

3) Les balbutiements des réglementations étatiques

a) Les réglementations pour protéger les utilisateurs

La possible future législation du système du Bitcoin, intégré ou en dehors du système bancaire traditionnel, est un point plus compliqué à traiter. Tout d'abord une

première question se pose, à savoir pourquoi développer tant d'efforts - d'audiences, de rapports, d'auditions et autres - pour un sujet qui, de l'avis même de ceux qui déploient ces efforts, ne fera pas long feu ? En effet pour un grand nombre de professionnels du secteur bancaire le Bitcoin n'est qu'un phénomène, presque une mode, qui finira par disparaître dans quelques temps. La réponse rapide des professionnels concernés est que, puisque ce sujet est si brulant et présent dans les médias, il est important d'alerter le public sur les possibles risques qu'il présente. Cette hausse de l'attention portée par les autorités sur ce sujet à travers le monde serait donc due à la hausse de l'attention portée par les médias sur le Bitcoin. Les « pro-Bitcoin » feraient miroiter un nouvel actif financier doré, facile d'utilisation, présentant de nombreux avantage, et promis à un brillant avenir, au détriment d'une réalité beaucoup plus risquée. Il est d'ailleurs souvent recommandé dans les nombreux documents, édités soit par la Banque de France ou par la Banque Centre européenne par exemple, de ne pas investir « plus d'argent qu'on ne peut en perdre », ce qui est assez éloquent sur les positions du système bancaire à ce sujet. De la même manière, Tracfin[23] déclare avoir estimé premièrement que le Bitcoin représente un risque particulier en ce qui concerne le blanchiment d'argent et le financement du terrorisme (LCB-FT), et ensuite que le Bitcoin ne remplit pas les conditions nécessaires pour jouer le rôle d'un support d'investissement crédible. Son utilisation est donc hautement risquée, notamment pour ses utilisateurs eux-mêmes.

Cela étant dit, aucune régulation n'est à ce jour possible sur le système du Bitcoin en lui-même, de par sa nature décentralisée, et surtout de par son existence sur Internet seulement. En effet les monnaies virtuelles n'entrent pas dans le champ d'exercice de la supervision et de la surveillance des autorités compétentes en la matière dans le système monétaire et financier traditionnel. De par le fonctionnement de ces monnaies, il n'est ni possible de réguler leur émission, qui est de toute façon conçue pour pouvoir échapper à tout contrôle de la sorte, ni possible de réguler l'utilisation qui en est faite.

[23] TRACFIN – « Traitement du renseignement et action contre les circuits financiers clandestins » - est un organisme du ministère de l'Economie et des Finances français, spécialement chargé de la lutte contre le blanchiment d'argent.

Un point cependant reste légalement et réellement accessible aux législateurs : ce sont les plates-formes d'échange, ou toute autre porte d'entrée dans le système du Bitcoin. En effet ces plates-formes d'échange sont utilisées pour convertir le Bitcoin en monnaie légale et inversement. Elles offrent donc un service de paiement, et sont de ce fait sujettes aux législations correspondantes, avec un intérêt prononcé pour les activités de lutte contre le blanchiment d'argent et le financement du terrorisme. En effet les activités illicites réalisées dans cette optique n'ont d'intérêts que si le résultat peut, en fin de course, être converti en monnaie légale.

De manière plus spécifique, ces plates-formes exercent une activité de réception, de virement, et de tenue de compte de fonds de monnaies qui ont cours légal. C'est pourquoi elles sont considérées comme des prestataires de service de paiement. Ces plates-formes d'échange sont ainsi soumises dans l'Union Européenne à la Directive sur les moyens de paiements, et nécessitent, en France notamment, l'obtention d'un agrément d'établissement de paiement pour pouvoir exercer leur activité. L'obtention de cet agrément et la supervision des activités est aujourd'hui placée en France sous le contrôle de l'Autorité de contrôle prudentiel et de résolution (l'ACPR, organe de supervision français de la banque et de l'assurance). La Banque de France exerce de plus une surveillance de la sécurité opérationnelle de ces plates-formes afin de limiter les risques de fraude possible lors de l'achat ou de la vente de bitcoins. De la même manière, l'obtention de l'agrément nécessaire aux Etats-Unis implique l'application des règles juridiques en matière de LCB-FT.

Un exemple particulier de régulation est celui de la « BitLicense », qui a pris effet en août 2015 aux Etats-Unis dans l'état de New-York. Cette licence d'exploitation est une première dans le monde. Délivrée par le New York State Department Financial Services (NYSDFS), elle concerne toutes les entreprises ayant une activité de transmission, de stockage, de contrôle, achat et de vente, de service, ou encore d'émission de monnaie virtuelle. Dans les faits, elle rend obligatoire pour ces entreprises (« cryptocurrency banks ») de vérifier l'identité de leurs clients et, le cas échéant, de demander plus d'informations pour les clients à hauts risques, pour ceux qui ont un fort volume d'échange, ou bien ceux dont les comptes contiennent des rapports d'activités suspects. Selon Benjamin M. Lawsk, le directeur du NYSDFS, cette

BitLicense aurait pour objectif premier d'aider à protéger les utilisateurs et d'arrêter le plus tôt possible toute suspicion d'activités illégales[24].
Depuis sa mise en application en août dernier, plusieurs « cryptocurrency banks » ont annoncé qu'elles arrêteraient leurs activités dans l'état de New-York du fait de cette nouvelle régulation. Le New York Business Journal a ainsi parlé du « Grand exode du Bitcoin » (« Great Bitcoin Exodus »)[25].

Cet exemple de régulation, qui est à ce jour la seule en place au monde à être aussi complète, est une très bonne illustration de la position du système bancaire et financier sur le sujet.

Enfin un dernier point reste à souligner : aucune loi ou régulation ne peut aujourd'hui surveiller et contrôler l'utilisation qui est réellement faite des monnaies virtuelles sur Internet. Seule une intervention des forces de l'ordre peut, lorsque nécessaire, mettre un terme ou punir a posteriori l'utilisation de manière illégale de ces monnaies. C'est pourquoi Europol a ainsi demandé que plus de possibilités soit données à la police pour identifier les utilisateurs frauduleux de ce système, en particulier pour lutter contre le blanchiment d'argent.

b) Définition juridique du Bitcoin et réflexion sur la taxation

Le second point difficile à définir pour le moment est la définition juridique du Bitcoin. Quel statut lui donner ? Le Bitcoin échappe encore en effet à toute qualification, qu'elle soit monétaire ou bancaire. Et à partir de ce statut, comment l'intégrer dans le système traditionnel ? A l'heure actuelle les transactions réalisées en Bitcoin, et plus généralement en monnaie virtuelle, ne sont pas reconnues et échappent donc à toute taxation.

[24] http://www.engadget.com/2014/07/18/new-york-cryptocurrency-regulations/ Consulté le 15/11/2015

[25] http://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html Consulté le 15/11/2015

Aucun accord n'a pour le moment été trouvé sur ce point, chaque pays opérant de son côté. Plusieurs grandes tendances se dessinent tout de même avec de nombreuses spécificités propres à chacun. Selon les pays, le Bitcoin sera considéré soit comme un service financier, comme au Danemark par exemple, soit comme une matière première, à l'exemple de la Finlande. Il pourra également avoir un statut de chose ou de marchandise, comme c'est le cas au Japon, aux Etats-Unis ou encore en France (défini spécifiquement comme un bien meuble), ou encore être défini par ce qu'il n'est pas, c'est-à-dire ni un moyen de paiement ni un instrument financier, comme l'ont défini pour le moment les Pays-Bas et la Slovénie. Enfin dans d'autres cas encore, il n'aura tout simplement pas de statut. De ces définitions, ou début de réflexion sur une future qualification du Bitcoin, découlent pour certains pays un début de régulation sur la question de l'inclusion financière du Bitcoin dans le système traditionnel.

De manière simplifiée et succincte, quatre grandes catégories de pays se distinguent :

- Tout d'abord certains pays ont purement et simplement interdit l'usage du Bitcoin sur le territoire en le déclarant illégal, à l'image de la Thaïlande, de Taïwan, ou de la Russie pour les plus connus.
- D'autres pays, comme l'Italie, l'Irlande, la Grèce ou encore la Pologne n'ont pas encore décidé d'une qualification juridique pour les monnaies virtuelles. La situation est donc encore une situation de fait, ces transactions existent, sont connues, mais ne sont pas encore prises en compte et inclues dans le système monétaire et financier traditionnel.
- De leur côté, le Japon, les Etats-Unis, le Royaume-Uni, l'Espagne et la Finlande ont quant à eux décidé de soumettre à l'impôt les gains réalisés grâce aux transactions en monnaie virtuelle.
- Dans le même esprit, la Slovénie, le Danemark, les Pays-Bas ou encore L'Allemagne ont plutôt orienté leurs réflexions sur la fiscalité et en particulier sur la taxation des plus-values réalisées lors de la vente de bitcoins.

Il est à noter que si les qualifications du Bitcoin différent, toutes les Banques Centrales de ces pays - sans exception notable - ont émis des alertes, à plus ou moins grande échelle, sur les risques associés à son utilisation.

Le tableau ci-dessous rassemble les premières qualifications données au Bitcoin et les régulations appropriées proposées par les pays.[26]

Juridictions	Qualification juridique du bitcoin	Traitement proposé
Union européenne	Respect du 1er et du 3e critère de la directive sur les moyens de paiement électronique (*electronic storage, acceptance as a mean of payment*) mais pas du 2e (*issuance upon receipt of funds*)	Avertissement de l'EBA sur les dangers associés aux transactions (achat, détention ou trading de monnaies virtuelles), aucune protection des consommateurs et gains réalisés potentiellement taxables fiscalement. Les institutions de paiement n'ont pas le droit d'émettre de la monnaie électronique.

[26] Storrer P. (2014), « Notion de monnaie électronique : monnaies virtuelles », in ***Droit de la monnaie électronique***, RB Edition, 2014

Allemagne	Unité de compte privé (*binding financial instrument, private mean of payment withing private trading exchanges*) (août 2013).	Communication de la BaFin : pas d'obligation de licence bancaire mais régulation du trading de bitcoins. Pas encore de position fiscale. Exigence d'une autorisation préalable en cas d'utilisation commerciale, d'activités de trading pour compte propre ou de *brokerage* ou de système plateforme multilatérale.
Chypre	-	Déclaration de la Banque Centrale sur les risques associés aux monnaies virtuelles (déc. 2013)
Danemark	Pas une monnaie mais un service électronique.	La FSA a déclaré qu'elle ne régulerait pas l'utilisation du bitcoin, car hors du champ de la régulation financière (déc. 2013). Les gains de ce service électronique seraient taxables mais pas encore de position officielle.
Espagne	Pas une monnaie ayant cours légal. Considéré comme des biens digitaux.0	En tant que « bien digital », le bitcoin est assujetti à la TVA.
Estonie	-	Transactions suivies par la Banque Centrale.
Finlande	Matière première	Pas de loi mais taxation des gains réalisés lors de la conversion de monnaies virtuelles en monnaies ayant cours légal et assujettissement du *mining* au titre de l'impôt sur le revenu.
France	Bien meuble incorporel (Trésor). Pas une monnaie. Pas un moyen de paiement.	Avertissement de la Banque de France sur les risques associés (déc. 2013). Position de l'ACPR (jan. 2014)[80] : Opération de conversion de monnaies virtuelles contre une monnaie ayant cours légal relève de la fourniture de services de paiement donc agrément obligatoire de prestataire de service de paiement délivré par l'ACPR[81].
Grèce	-	Pour autant, le bitcoin est accepté par certaine sociétés de paiement.
Irlande	-	Uniquement monitoring par l'administration fiscale.
Italie	-	-
Malte	-	*Hedge fund* maltais investi en bitcoin.
Pays-Bas	Pas une monnaie électronique. Pas un produit financier.	Question de la taxation des plus-values à régler. Décembre 2013 : alerte de la banque centrale sur les risques associés.
Pologne	-	-
Portugal	Bitcoin : modèle de paiement en monnaie virtuelle bidirectionnel. bitcoin : -	Communication de la banque centrale en novembre 2013 sur les risques du bitcoin, qui ne serait pas une monnaie sure.
Royaume-Uni	« *Single purpose voucher* » selon l'administration fiscale.	En tant que tel, assujetti à la TVA.
Slovénie	Pas un moyen de paiement. Pas un instrument financier.	Opinion du Ministère des Finances émis en décembre 2013, sans pour autant définir de statut. Question de la taxation à régler.

Chine	Interdiction des institutions financières (déc. 2013) et des sociétés de paiement (avr. 2014) de traiter des bitcoins. Autorisation du *trading* en ligne.	
États-Unis	Actif (*property*) et non devise.	Actif soumis à l'impôt : plus-values imposées comme les gains sur le capital et revenus tirés de l'activité de minage au-delà de 600 USD soumis à l'impôt sur le revenu (IRS, mar. 2014). La négociation/conversion d'une monnaie virtuelle contre une monnaie légale étant assimilable à un service de transmission de fonds, obligation d'agrément en tant que *Money Service Business* (FinCEN, mar. 2013).
Japon	Statut de marchandise ou de chose (mais pas une monnaie).	Soumis à l'impôt (mar. 2014)
Russie	Illégal.	
Singapour	Pas une valeur mobilière.	Régulation des intermédiaires en monnaie virtuels (mar. 2014) afin de limiter les risques (blanchiment, financement du terrorisme, etc.) : devoir de vérification de l'identité des contreparties des transactions et de signalisation toute transaction suspecte au *Suspicious Transaction Reporting Office*.
Taïwan	Illégal.	
Thaïlande	Illégal.	Interdiction des monnaies virtuelles

Source : http://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives.html?docId=workspace%3A%2F%2FSpacesStore%2Fb87033f5-ecbf-41f1-8236-ee44c91df3c7

II. Réorientation de la réflexion et des recherches

Au cours de mes recherches et des discussions avec mes interlocuteurs, je me suis rendue compte que le véritable sujet de réflexion pour les années à venir était beaucoup moins le Bitcoin et sa réglementation en tant que monnaie, que le Bitcoin en tant que système avec son protocole d'échange décentralisé. Cette innovation technologique, qui ne m'apparaissait auparavant que comme l'outil qui permettait la circulation de cette monnaie, et en fait pour un grand nombre de chercheurs et de développeurs le véritable point d'intérêt du système, qui pourrait être promis à un grand avenir dans les années qui viennent. C'est pourquoi j'ai décidé d'y consacrer la seconde partie de mes recherches.

1) Le grand intérêt pour le protocole du Bitcoin plus que pour la monnaie elle-même

En novembre 2013 déjà, dans une lettre adressée au Sénat américain dans le cadre des auditions organisées sur les monnaies virtuelles, l'ancien président de la Fed Ben Bernanke reconnaissait que cette dernière n'avait pas l'autorité nécessaire pour superviser les monnaies virtuelles. Mais, plus important, il déclarait également que ces monnaies pouvaient être une promesse d'avenir, notamment si ces innovations permettent de promouvoir un système de paiement plus rapide, plus sécurisé, et plus efficace[27].

Aujourd'hui encore, ces nouvelles technologies si prometteuses pour l'avenir font beaucoup parler d'elles et suscitent beaucoup de débats et de recherches, tout particulièrement l'une d'entre elle : la blockchain, ou chaîne de blocs. Plus que le Bitcoin en tant que monnaie, c'est ainsi le système du Bitcoin, en tant que protocole, qui est aujourd'hui le centre de l'attention et qui interroge tant sur l'utilisation qui pourra en être faite dans les années à venir.

[27] http://www.businessinsider.com/ben-bernanke-on-bitcoin-2013-11?IR=T Consulté le 15/11/2015

Retirée du contexte du Bitcoin dans lequel elle a été présentée dans la première partie de ce mémoire, la blockchain reste une innovation technologique. De nombreuses applications sont possibles à partir de cette technologie, le système du Bitcoin étant l'une d'entre elles. De manière simplifiée, la blockchain est un registre de transactions sur Internet dont la validation n'est pas réalisée par une autorité centrale, mais par l'ensemble des participants du réseau grâce à l'utilisation de la cryptographie. Ces transactions aujourd'hui sont des fragments de bitcoins, sous la forme de fichiers électroniques, mais pourraient demain être des contrats entre les différentes parties prenantes, des œuvres sous le régime de la propriété intellectuelle etc.
Ces possibles développements d'avenir présentent aujourd'hui beaucoup d'intérêts pour un certain nombre d'acteurs.

Le système bancaire actuel n'est tout d'abord pas le dernier à s'y intéresser. En effet, en ne regardant que la technologie de la blockchain et en particulier le protocole de transport – et non l'usage qui en est actuellement fait avec l'application du système de Bitcoin – cette nouvelle technologie permet de désintermédier des transferts de données, ce qui peut représenter des gains de coûts considérables sur les contenus véhiculés. D'après A. Stervinou, chef du Service de la Surveillance des moyens de paiements scripturaux au sein de la Banque de France, il n'est ainsi pas exclu qu'à plus ou moins long terme de nouveaux protocoles jaillissent dans ce domaine au sein du système bancaire, par exemple dans l'envoi de contrats ou l'octroi de prêts bancaires.

De la même manière, selon I. de Jong, expert à la Direction Générale Infrastructure de marché et paiements de la Banque Centrale Européenne, il pourrait ainsi être intéressant d'utiliser ces nouvelles technologies en complément du fonctionnement du système bancaire actuel. Un tel protocole décentralisé permettrait en effet de réaliser des gains non négligeables en termes d'efficacité et de rapidité dans les échanges de données. De plus, le réseau d'utilisateurs ayant accès à cette technologie pourrait être beaucoup plus important comparé à un système centralisé, qui nécessite un accès et une proximité des différents acteurs à l'entité centrale pour chaque échange de données. Cela donnerait en outre à tous les utilisateurs et clients un accès direct au registre des transactions/données échangées, sans passer par une autorité centralisatrice

ni par la bureaucratie bancaire, ce qui représenterait de forts gains en termes de coûts et de temps.

Enfin, il faut tout de même noter qu'au-delà de cet accès direct pour les échanges de données, la technologie de la blockchain présente de nombreux avantages non négligeables pour le système bancaire. Ainsi grâce à elle, les transferts de fonds notamment - qui nécessitent en temps normal au minimum 48 heures entre le moment de l'envoi et la réception, et dont les frais peuvent finir par représenter des sommes très importantes – peuvent être réalisés en quelques secondes à peine, au grand maximum une dizaine de minutes le temps que la transaction soit validée par le réseau. Cela ne coûte rien, ne viole aucune loi, et les gains à en retirer sont considérables.

Toutefois, le système bancaire n'est pas le seul à percevoir les avantages proposés par cette innovation. Les différentes applications possibles pouvant être bâties sur ce type de protocole pourraient permettre l'émergence de nouveaux types de services financiers décentralisés, depuis les opérations de couverture de change en passant par les prêts financiers, l'émission d'actions, la signature de contrats etc. Cela signifierait tout simplement la possibilité de réaliser des prêts financiers sans l'intermédiaire d'une banque, de signer des contrats sans avocats ou notaires, ou encore d'émettre et d'échanger des actions sans courtiers. Tout cela serait exécuté et enregistré grâce à des centaines d'ordinateurs à travers le réseau, gages de la sécurité et de la fiabilité des ces contrats.

Cependant, au-delà des intérêts financiers à y trouver, la technologie de la blockchain pourrait également permettre une nouvelle définition d'internet. Dans un contexte où les boites mails individuelles sont souvent saturées de spams, où les numéros de cartes bancaires peuvent être piratés, et où chaque personne doit retenir au moins une dizaine de mots de passe pour accéder à ses différents comptes en ligne, le système de la blockchain pourrait devenir très attirant.

Pour certains défenseurs de la blockchain, une analogie pourrait être faite entre l'apparition de cette technologie aujourd'hui et l'apparition d'internet dans les années 1990. Personne n'y croyait vraiment, et cela a pourtant tout révolutionné. Toutefois certains pensent que l'expansion d'internet s'est faite de la mauvaise manière à cette époque : ils considèrent qu'aujourd'hui internet est dominé de manière malsaine par

quelques grandes entreprises. Ils estiment de plus que ce système informatique centralisé, dans lequel les données personnelles sont stockées afin de pouvoir ensuite mieux cibler les publicités envoyées, doit changer et laisser place à un nouveau paradigme. Le système de la blockchain pourrait être le prochain.

Un nouveau terme, le TradeNet, a fait son apparition en même temps que la découverte des usages possibles de la blockchain. Le terme TradeNet définit l'utilisation qui pourrait être faite d'internet pour échanger des actifs ou des données en ligne sans avoir besoin de passer par un tiers de confiance. Si aujourd'hui un seul système basé sur la technologie de la blockchain s'est véritablement développé - le système de Bitcoin - de nombreuses possibilités sont à prévoir, pouvant varier les unes par rapport aux autres selon les attentes et les ambitions des développeurs. Le TradeNet n'est encore aujourd'hui qu'un possible futur, mais qui pourrait rapidement se développer dans les décennies à venir. Pour les défenseurs de la blockchain, cette technologie ne représente pas moins que l'outil principal d'une révolution à venir.

Les plus modérés d'entre eux tout d'abord imaginent « simplement » un retournement du système financier global. Cela se traduirait par des coûts beaucoup plus faibles que ceux du système bancaire et financier actuel, une accélération du commerce grâce à la quasi instantanéité des échanges, et une perte de la nécessité et de la légitimité des banques comme tiers centralisateur, ainsi que du système des cartes de crédits par la même occasion.

D'autres en revanche attendent encore plus de l'application de cette technologie, en étendant l'impact de son utilisation à l'ensemble du domaine des télécommunications. Cela permettrait de restaurer une véritable confidentialité dans les communications ainsi qu'une autonomie dans les échanges, toujours dans l'idée de la suppression du tiers centralisateur.

Enfin, les plus convaincus de cette technologie n'en attendent pas moins qu'une véritable révolution avec la dissolution des gouvernements d'état en place, une connexion complète de la vie quotidienne à internet, et ainsi un nouveau fondement pour les sociétés civiles entièrement basé sur les mathématiques et l'utilisation de la cryptographie.

Le point principal du fonctionnement actuel d'internet que les défenseurs de la blockchain rejettent aujourd'hui est ce qui est appelé la « single source of truth », que l'on pourrait traduire en français par « source unique et fiable ». La « single source of truth » est un concept informatique qui consiste à faire en sorte de n'avoir qu'un seul point de référence dans un réseau informatique, une seule entité chargée de le gérer, qui est désignée par le créateur du réseau lors de son développement. Chaque réseau sur internet fonctionne donc grâce à cette entité, qui approuve ou non les informations transmises sur le réseau (« ceci est vrai », « cet utilisateur correspond bien à l'identité qu'il prétend avoir », « cette transaction a bien été effectuée » …). Il apparait donc que l'ensemble d'internet aujourd'hui dépend des entités qui gèrent ces réseaux, c'est-à-dire en grande majorité des plus grandes entreprises et des gouvernements.

Ainsi, grâce à son fonctionnement, l'intérêt majeur de la blockchain serait de permettre à l'ensemble du réseau de pouvoir fournir cette « single source of truth ». Ce mécanisme permettrait de conférer collectivement cette légitimité à chacun des utilisateurs.

L'application de la technologie de la blockchain à l'ensemble d'internet serait donc un immense retournement qui favoriserait l'émergence d'une nouvelle forme collective de comportements humains, et permettrait également de créer de nouveaux marchés sécurisés et décentralisés, qui pourraient étendre la portée et les capacités d'internet.

2) Faut-il déplacer le débat ?

Au cœur de toute cette réflexion de nombreux avis s'opposent selon les positions professionnelles de chacun, ses intérêts, ou son optimisme dans l'avancement des technologies. La blockchain va-t-elle se développer à grande échelle ? Peut-elle fonctionner sans l'application de Bitcoin ? Peut-on imaginer des blockchains privées adaptées à l'utilisation que l'on souhaite en faire ? De nombreuses questions sont posées et les discours à ce sujet sont multiples. Cependant, peut-être que l'important n'est pas là et que le débat mérite d'être déplacé.

Les réflexions actuelles portent en effet sur l'utilisation de la blockchain - protocole sous-jacent du Bitcoin - dans la société d'aujourd'hui. Or le monde du Bitcoin est celui d'internet avec d'autres règles, d'autres questions, et sans frontières. Déplacer le débat et ne plus réfléchir en termes de valeur mais, selon J. Favier, en termes d'utilité, permettrait alors de sortir de ce dialogue de sourds.

Les deux cultures qui s'affrontent dans ces réflexions sont tout à fait opposées et ne se comprennent pas. Celle du système bancaire traditionnel est centralisatrice et confidentielle, alors que celle de la blockchain est de fait de pair à pair et open data [28]. De la même manière les banques cherchent à sauver leurs institutions, alors que les défenseurs de la blockchain cherchent davantage à créer une autre économie, décentralisée et pair à pair, qu'à détruire le système présent.

Selon J. Favier, auteur de « La Voie du Bitcoin », il est important de ne pas perdre de vue que le véritable pays du Bitcoin est celui d'internet. Il serait donc absurde de vouloir l'intégrer à la totalité des transactions de la société actuelle. Payer par exemple un café en bitcoin serait ridicule et sans intérêt. Il est d'ailleurs intéressant de noter qu'en dehors de son utilité sur internet pour les jeux, en grande majorité, ainsi que la petite partie sombre bien connue de la drogue, du sexe et du crime, le Bitcoin n'a pas encore trouvé d'usage vraiment utile. Est-ce sa volatilité ? Un manque de confiance dans cette monnaie ? Pas de véritable utilité ? Toujours est-il que de nombreuses possibilités théoriques existent pour le Bitcoin, mais qui ne sont encore aujourd'hui que des idées sans réalités. Pourquoi alors autant s'y intéresser ?

Si sa valeur est si discutable et incertaine à l'heure actuelle, son utilité en revanche mérite un peu d'attention. Il ne suffirait en effet que d'une petite fraction de bitcoin pour envoyer un titre, une garantie, une hypothèque ou tout autre document tout en disposant d'une date certaine, d'une confidentialité, et d'un temps de transport de l'ordre d'une dizaine de secondes. Bitcoin pourrait donc bien plus servir demain à échanger des informations qu'à conserver ou échanger de la valeur.

[28] http://www.lesechos.fr/idees-debats/cercle/cercle-142818-de-la-blockchain-et-de-lancienne-societe-1173595.php Consulté le 21/11/15

On compte aujourd'hui environ 10 milliards d'objets connectés[29] sur la planète, 20 milliards en 2020, et 100 milliards à l'horizon 2050. C'est pour eux, et pour l'internet des objets[30], que le système de Bitcoin et son protocole sous-jacent, la blockchain, ouvrent des perspectives énormes. Ces objets font, ou feront, partie intégrante de notre quotidien, à l'exemple des frigidaires qui commandent seuls certains aliments qui ont été consommés, des téléphones qui indiquent nos données de santé, ou encore des pots de fleurs qui arrosent automatiquement les plantes lorsqu'elles en ont besoin. Or ces objets n'ont pas de personnalités juridiques qui leur permettent de contracter entre eux et qui assurent la légitimité de leurs contrats. Une authentification des transactions réalisées par un calcul sécurisé et effectué par l'ensemble du réseau semble donc être l'idéal pour eux. La blockchain semblerait alors être le meilleur support pour le développement de cet internet des objets.

Au-delà de cette question pratique – celle de la personnalité juridique de ces objets connectés et de la légitimité des contrats formés – J. Favier souligne encore l'importance de ne pas perdre de vue la différence entre le monde matériel et le monde d'internet auquel appartient le Bitcoin et la technologie de la blockchain. Les règles et les attentes n'y sont pas les mêmes, il ne convient donc pas d'opter pour le même comportement ou pour les mêmes régulations dans ces deux univers. En revanche « il est souhaitable que cet univers [*ndlr : celui d'internet et de la blockchain*] soit vivable et ne trouble point celui de notre vie matérielle. Il est urgent d'inventer des droits et des devoirs appropriés non seulement à la technique (pour ne pas interdire ce qu'on ne saurait empêcher), mais à la nature de cet espace [31] ». Ainsi, la blockchain fonctionnant

[29] Les objets connectés sont des objets de la vie réelle auxquels l'ajout d'une connexion internet permet d'apporter une valeur supplémentaire, que ce soit en termes de fonctionnalité, d'information, ou bien d'interaction avec leur environnement. Ils sont ainsi capables de contracter entre eux à l'aide d'un langage électronique (« si ceci … alors fait cela »).

[30] Le terme « internet des objets » fait référence à l'extension d'internet à des objets physiques. Ce sont les échanges d'informations et des données provenant des objets connectés vers le réseau internet.

[31] http://www.lesechos.fr/idees-debats/cercle/cercle-134553-le-bitcoin-et-les-limites-de-la-pensee-1134863.php Consulté le 21/11/15

grâce à l'application de l'algorithme mathématique SHA-256, il revient donc aux développeurs de trouver de quelle manière les mathématiques peuvent y faire régner l'ordre, loin de toutes les idées actuelles d'intégration de cet univers mathématique dans les structures traditionnelles existantes, qu'elles soient bancaires, étatiques ou autre.

Pour conclure, l'univers du Bitcoin et de la blockchain ainsi que l'univers de nos institutions traditionnelles ne pourraient être plus opposés dans leurs constructions et dans leur fonctionnement. Chercher à intégrer un univers à l'autre n'est ainsi peut-être pas la meilleure façon de suivre ces évolutions. En revanche, participer à la réflexion et à la construction de ces nouveaux systèmes pourrait être une manière pour les institutions traditionnelles de mieux comprendre ces évolutions et leur permettre de mieux « vivre en paix avec ce nouveau et transcendant voisin [32]».

[32] http://www.lesechos.fr/idees-debats/cercle/cercle-134553-le-bitcoin-et-les-limites-de-la-pensee-1134863.php Consulté le 21/11/15

CONCLUSION

Lors des premières recherches et de la rédaction de l'état de l'art, plusieurs constatations ont pu être faites sur le système du Bitcoin : tout d'abord le système est loin d'être parfait et présente certaines limites ; ce même système offre également une multitude d'opportunités et d'avantages, qui ne sont peut-être pas encore assez connues ; enfin au travers d'un début de réflexion sur la réglementation d'un tel système, le système bancaire traditionnel et le système du Bitcoin pourraient tous les deux bénéficier d'un rapprochement mutuel.

Face au premier constat, si les critiques envers le système concernant la volatilité de la monnaie et le manque de protection de ses utilisateurs peuvent s'avérer légitimes, il apparaît en revanche que sa mauvaise réputation ne serait pas justifiée. Le Bitcoin n'est dans les faits pas plus dangereux que le cash, et personne aujourd'hui ne songerait sainement à remettre en question l'existence même de l'argent cash. Aussi étrange que cela puisse paraître au vu des débats enflammés que provoque le Bitcoin sur internet, le système reste peu ou mal connu des individus lambda de la société, alors même qu'il connaît une croissance et un développement relativement spectaculaire depuis quelques années. Pour qui n'est pas un peu à l'aise avec le monde de l'informatique, le mot « bitcoin » n'évoque rien, ou au mieux une vague connaissance négativement connotée depuis que le cas de Silk Road a porté le système sous les projecteurs des médias.

Parallèlement à cette image négative qui s'est ainsi imposée à lui, la deuxième hypothèse développée stipulait que le système offre cependant de nombreux avantages et opportunités uniques, qui comblent certaines lacunes du système bancaire traditionnel. Si la théorie des ces idées est véritablement intéressante et pleine de promesses pour l'avenir, la réalité est en revanche beaucoup plus mitigée. Une des raisons principales pour cela est que le système du Bitcoin nécessite au préalable une intégration dans le système économique actuel, ne serait-ce que pour pouvoir accéder aux technologies nécessaires à son utilisation.

Enfin, la troisième et dernière hypothèse, qui avait pour but d'éclaircir la position des législateurs face ce système si négativement réputé, semble s'avérer simplement dépassée. Il se trouve en effet que si chaque pays décide de manière individuelle de sa politique en matière de Bitcoin et à des degrés différents, la véritable question ne se pose pas - ou tout du moins ne se pose plus - à ce niveau là. La question n'est plus en effet de savoir si c'est une bonne ou une mauvaise chose, elle n'est même plus tournée spécifiquement sur le Bitcoin en tant que monnaie. La technologie innovante et inédite de la blockchain a en effet pris le pas sur les premiers débats.

La question n'est donc plus de savoir s'il est souhaitable ou non de s'intéresser à cette innovation, mais semble plutôt être de savoir à quel degré s'y intéresser pour ne pas passer à côté de ce qui pourrait être une prochaine révolution.

BIBLIOGRAPHIE

- **OUVRAGES ET ARTICLES ACADEMIQUES**

Bank of England (2014 Q3), Ali R., of the Bank's Financial Market Infrastructure Directorate, Barrdear J., of the Bank's Monetary Assessment and Strategy Division, and Clews R. and Southgate J., of the Bank's Markets Directorate, **"**Innovations in payment technologies and the emergence of digital currencies".

Blundell-Wignall A., "The Bitcoin question: Currency versus Trust-less transfer of technology", ***OECD Working papers on Finance, Insurance et Private pensions***, 2014

Bollen R., "The legal status of online currencies: are bitcoins the future?", ***Journal of Banking and Finance Law and Practice,*** 2013

Brito J., Castillo A., "Bitcoin: a primer for policymakers" in ***Policy***, Mercatus Center, Summer 2013-2014

Chen Y.W, Vivek K.P., "The value of Bitcoin in enhancing the efficiency of an investor's portfolio", ***Journal of Financial Planning***, September 2014

Cusumano M., "The Bitcoin Ecosystem", ***Communications of the ACM***, October 2014

Daniali G., "E-money Laundering Prevention", ***New Marketing Research Journal***, 2014, Special Issue

Dodgson M., Gann D., Wladawsky-Berger I., Sultan N., George G., "Managing Digital Money", ***Academy of Management Journal***, 2015, Vol 58

Greebel E.L., Moriarty C., Callaway C., Xethalis G., "Recent key Bitcoin and virtual currency regulatory and law enforcement developments", ***Journal of Investment Compliance***, 2015, Vol. 16 Iss 1 pp. 13 - 18

Herlin P. (2013), « La révolution dans les monnaies : contourner les banques et les Etats », in ***La Révolution du Bitcoin et des monnaies complémentaires : Une solution pour échapper au système bancaire et à l'euro ?***, Editions Eyrolles et Atlantis, 2013, pp. 32-40.

Humphreys, Thomas A., Reigersman, Remmelt A., Goett, David J., "US: The challenges of virtual currency", ***International Financial Law Review***, Jun2014

Khan A., "Feature: Bitcoin – payment method or fraud prevention tool?", ***Computer Frand & Security***, May 2015

Lemineux P., « Who is Satoshi Nakamoto ? », ***Regulation***, Automne 2013

Levin R., O'Brien A., Osterman S., "Dread Pirate Roberts, Byzantine Generals, and federal Regulation of Bitcoin", ***Journal of taxation & regulation of financial institution,*** March/April 2014

Nellen A., "Taxation and Today's Digital Economy", ***Journal of Tax Practice & Procedur,*** Apr/May2015, Vol. 17 Issue 2

OECD Observer (2014), Blundell-Wignall A., **"**Bitcoin: more than a bit part?".

Raskin M., "Realm of teh coin: Bitcoin and civil procedure", ***Fordham Journal of Corporate & Financial Law***, 2015, Vol. 20 Issue 4

Raymaekers W., "Cryptocurrency Bitcoin: Disruption, challenges and opportunities", ***Journal of Payments Strategy & Systems***, Dec 2014, Volume 9 Number 1

Rogojanu A., Badea L., "The issues of competing currencies – Case Study – Bitcoin", ***Theoretical and Applied Economics***, 2014

Storrer P. (2014), « Notion de monnaie électronique : monnaies virtuelles », in ***Droit de la monnaie électronique***, RB Edition, 2014

Thomas Z., "Bitcoin tech could boost trade efficiency", ***International Financial Law Review***, August 2015

Thomas Z., "Bitcoin regulation: the latest development assessed", ***International Financial Law Review***, Dec 2013/Janv 2014

Thomas Z., "Americas: why can't we be friends*?"***, International Financial Law Review,*** April 2014

Thomas Z., "Why Bitcoin could be the key to banking's future?", ***International Financial Law Review***, Jun2014

Varriale G., **"**Bitcoin: how to regulate a virtual currency?", ***International Financial Law Review***, Sep2013

Varriale G., "What is the best way to regulate Bitcoin?", ***International Financial Law Review***, Oct2013, Vol. 32, Issue 7

Yahanpath N., Wilton Z., "Virtual money: betting on Bitcoin", ***University of Auckland Business Review,*** 2014, Volume 17 Number 1

- **RAPPORTS DES INSTITUTIONS**

Cartographie 2014 des risques et tendances sur les marchés financiers et pour l'épargne, par l'Autorité des Marchés Financiers (AMF), Juillet 2014

- **ARTICLES DE PRESSE**

- **Leaders**

« Régimes de change et « Guerre des monnaies »: Qu'en est-il du dinar tunisien? » par Ezzeddine Ben Hamida, le 19/06/2013

- **Les Echos**

« Bitcoin : bien plus qu'une simple monnaie d'échange ou une valeur refuge », par Stanislas Marion, le 11/02/2014

« Une histoire de généraux byzantins », par Y.V, le 02/06/2014

« Le Bitcoin et les « limites » de la pensée », par Jacques Favier, le 06/07/2015

« De la blockchain et de l'ancienne société », par Jacques Favier, le 09/11/2015

- **Le Huffington Post**

« Bitcoin comme solution aux transferts d'argent en Afrique ? », par Othmane Zrikem, le 05/12/2013

- **Courrier International**

« Le Bitcoin expliqué à ma mère », par Kevin Maney, le 11/04/2014

- **New York Business Journal**

"The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem", par Michael Del Castillo, le 12/08/2015

"Barclays signs two blockchain deals among slew of other contracts at Techstars accelerator", par Michael Del Castillo, le 13/10/2015

- **The Daily Mail**

"Barclays set to become first UK high street bank to accept bitcoin as it starts taking charity donations in the virtual currency", par Tim MacFarlan, le 30/08/2015

- **SITES INTERNET**

- **Blogs**

Blog World Bank (http://blogs.worldbank.org) par Gloria M. Grandolini
- *"Objectif SmaRT : agir intelligemment pour réduire le coût des envois de fonds »* le 16/06/2015

- **Autres sites**

Innovative European Studies
http://www.cvce.eu/education/unit-content/-/unit/7124614a-42f3-4ced-add8-a5fb3428f21c/94fb0a95-09b1-4ee1-b0ff-c24e661506f1

Site de la Banque de France
https://www.banque-france.fr/uploads/tx_bdfgrandesdates/focus5-qu-est-ce-que-l-etalon-or.pdf

Pièce de monnaie
http://www.piecedemonnaie.fr/lexique/monnaie-scripturale/

Site des Douanes et Droits indirects
http://www.douane.gouv.fr/articles/a10796-obligation-declarative-des-sommes-titres-et-valeurs

M. Lasserre
http://www.m-lasserre.com/educpop/dossiermonnaie/4lesystemebancaire.htm

Tout savoir sur la monnaie Bitcoin : Comprendre et utiliser le Bitcoin
http://www.monnaie-bitcoin.com/minage-bitcoins

Blockchain Info
https://blockchain.info/

Finance Watch
http://www.finance-watch.org/informer/blog/1003?lang=fr

Coin Desk
http://www.coindesk.com/

Le Cercle du Coin
https://le-coin-coin.fr/1972-terrorisme-blanchiment-trafic-le-bitcoin-se-defend/

Engadget
http://www.engadget.com/2014/07/18/new-york-cryptocurrency-regulations/

Business Insider
http://www.businessinsider.com/ben-bernanke-on-bitcoin-2013-11?IR=T