

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud MAMMERI de Tizi-Ouzou

Faculté de Sciences Economiques,

Commerciales et des Sciences de Gestion

Département Sciences Economiques



MEMOIRE

DE FIN D'ETUDE

En vue de l'obtention d'un diplôme de Master Académique en Sciences Economiques.

Option : Economie Monétaire et Bancaire.



La Crypto-Monnaie : Emergence, Enjeux et Perspectives

Dirigé par :

 *Mr SAM Hocine*

Réalisé par :

 *Mlle OUMEDJANE Chanez*
Mlle RACHEDI Nadia

Promotion 2021-2022

Remerciements

*Nous remercions DIEU tout puissant de nous avoir donné la foi
et le courage pour réaliser ce modeste travail.*

*Nous tenons à remercier l'ensemble de nos familles pour leur soutien tout au
long de notre parcours d'études, que ce travail soit un témoignage de notre
gratitude envers elles.*

*Nous tenons à remercier notre promoteur monsieur SAM.H de nous avoir
accompagnés dès le début de ce projet. Nous tenons à lui exprimer notre
gratitude pour ses valeureux conseils*

*Nos plus sincères remerciements s'adressent aussi aux membres du jury qui
nous ont fait l'honneur de juger notre travail.*

*Sans oublier de remercier toutes les personnes qui ont contribuées de près ou
de loin à la réalisation de ce projet.*

Dédicaces

On dédie ce travail

*A Nos très chers parents qui nous ont toujours fait
confiance et n'ont jamais cessé de nous soutenir et de
nous encourager.*

A toutes nos familles

A tous nos camarades et amis sans exception

NADIA et CHANEZ

LISTE DES SIGLES ET ABRÉVIATIONS

ACCP :	Accise Proportionnelle
ACCS :	Accise Spécifique
ACPR :	Autorité De Contrôle Prudentiel Et De Résolution
ADA :	Cardano (crypto-monnaie)
AMF :	Autorité Des Marchés Financiers
BC :	Banque Centrale
BCE :	Banque Centrale Européenne
Bch :	Bitcoin Cash (crypto-monnaie)
BNB :	Binance coin (crypto-monnaie)
BRI	Banque Des Règlements Internationaux
BSV	Bitcoin Silver (crypto-monnaie) Bitcoin
BTC :	(crypto-monnaie)
CCP :	Comptes Courants Postaux
CFD :	Contract For Difference (Contrat pour la différence)
DGX :	
DLT :	Digix Gold (crypto-monnaie)
DTS :	Distributed Ledger Technology
ETH :	Droit De Tirages Spéciaux
Fevad:	Ethereum (crypto-monnaie)
FMI:	Fédération E-Commerce Et Vente A Distance
IBAN:	Fonds Monétaire International
ICO:	International Bank Account Number
IFNB	Initial Coin Offering
IFB	Institutions Financières Non Bancaires
	Institutions Financières Bancaires

IPO :	Initial Public Off ring
LCB-FT :	Lutte Contre Le Blanchiment Et Financement Du Terrorisme
LTC :	Lite coin (crypto-monnaie)
MCDO :	Mac Donald (crypto-monnaie)
NFC :	Near Field Communication (La communication en champ)
ONG :	Organisations Non Gouvernementales
OPCVM :	Organismes De Placement Collectif En Valeurs Mobilières
PIB :	Produit Intérieur Brut
PIHR :	Programme D'Investissement A Haut Rendement
Po: POS:	Proof of
POW:	Proof of Stack
P2P:	Proof of Work
SEPA:	Peer to Peer (pair à pair)
TIC:	Single Euro Payments Area (Espace de paiement en euro unifié)
TRX:	Technologie De L'Information Et De La Communication
TVA	Tron (crypto-monnaie)
UE:	Tether (crypto-monnaie)
US:	Stellar (crypto-monnaie)
USDT:	Ripple (crypto-monnaie)
XLM:	Taxe Sur La Valeur Ajoutée
XPP:	Union Européenne
	United States (Etats-Unis)

Sommaire

Sommaire

Thème : La crypto-monnaie : Emergence et Perspectives

INTRODUCTIONS GENERALE

Chapitre 01 : L'apparition et l'histoire de la crypto-monnaie

Introduction

Section 01 : Histoire de la crypto monnaie

**Section 02 : La crypto monnaie, une innovation fondée sur une combinaison
de techniques**

Conclusion

Chapitre 02 : L'impact des crypto monnaies, leurs enjeux, perspectives

Introduction

SECTION 1 : Les paiements de demain

SECTION 2 : RISQUES ET LIMITES DES CRYPTO-MONNAIES

**SECTION3 : LES PERSPECTIVES, RECOMMANDATIONS ET
RÉGULATION**

Conclusion

Chapitre 03 : Bitcoin et Crypto-monnaie : Expériences mondiales et perspectives

Introduction

SECTION1 : BITCOIN, Première CRYPTO-Monnaie

SECTION 2 : Évolution de BITCOIN et son cadre juridique

SECTION 3 : Débat au tour de BITCOIN

Conclusion

CONCLUSION GÈNÈRALE

LISTE DES FIGURES

Figure 3.1 : Le Principe de fonctionnement de la blockchain Bitcoin	61
Figure 3.2 : Transaction des BITCOINS	64
Figure 3.3 : Le Bitcoin, Une Monnaie Sans Frontière	65
Figure 3.4 : La Carte Géographique De La Concentration De Nœuds Bitcoin Accessibles Dans Des Pays Du Monde Entier	73
Figure 3.5 : Statut juridique du Bitcoin (la crypto-monnaie) dans le monde	75

LISTE DES GRAPHES

Graphe 3.1 : Evolution Du Cours De Bitcoin (2009-2019)	66
Graphe 3.2 : Une bulle spéculative Bitcoin	68
Graphe 3.3 : Evolution Du Nombre De Bitcoin En Circulation (2009-2019)	69
Graphe 3.4 : Evolution Du Nombre De Transactions En Bitcoin (2009-2019)	69
Graphe 3.5 : La Valeur Des Transactions En Bitcoin (2009-2019)	70
Graphe 3.6 : Evolution De la capitalisation boursière du Bitcoin (2009-2019).....	70
Graphe 3.7 : Evolution Du Nombre De Bitcoins Créés A Travers Le Temps.....	71

LISTE DES TABLEAUX

Tableau 2.1 : Une synthèse des trois piliers de la stratégie de lutte, proposée, contre les risques des crypto-monnaie.....	48
Tableau 3.1 : Dates qui ont marqué l'histoire du Bitcoin	54
Tableau 3.2 : Les 10 principaux pays par rapport au nombre de nœuds accessibles (arrêté au 16/11/2019)192.	73

Introduction Générale

INTRODUCTIONS GÉNÉRALE

Très tôt dans l'histoire de l'humanité un intermédiaire a été nécessaire afin de pouvoir réguler les échanges entre les membres d'une même tribu ou société. Les premières formes de monnaies conçues par l'homme étaient des coquillages, des chameaux ou encore des objets précieux. Nous sommes alors au tout début de la création du système monétaire dans une économie à monnaies multiples. Les débuts du système monétaire des premières sociétés où avait lieu l'échange, donc le commerce, s'apparentent à un système qui serait actuellement considéré comme du troc. Puis petit à petit le nombre d'objets acceptés en tant que monnaie a fini par devenir de moins en moins important. C'est ainsi que l'on glisse lentement d'un système semblable au troc avec de multiples monnaies à notre système actuel où la monnaie devient frappée et contrôlée par des autorités centralisées. C'est dans les républiques de Grèce durant l'antiquité qu'apparaît la monnaie fiduciaire.

Au départ, la monnaie était une marchandise qui avait une valeur propre, comme des troupeaux ou de l'or, puis avec le temps celle-ci a changé de forme et des chiffres apposés sur du papier sont venus remplacer la marchandise échangée contre la marchandise. Le papier pouvait s'échanger contre la marchandise, à l'instar des certificats-or. L'avantage de ce changement est l'accroissement de la portabilité, de la capacité à transporter de la monnaie. Ensuite elle est devenue fiduciaire, c'est-à-dire que la valeur de la monnaie repose sur la confiance du public en sa valeur car celle-ci n'est plus intrinsèque à la monnaie. En effet un billet de 10 dollars ne vaut pas réellement ces prix-là, si ce n'est grâce à une fiction juridique qui donne cette valeur-là au bout du papier imprimé d'un chiffre 10. La monnaie fiduciaire est donc une monnaie légale et émise par une autorité centrale. La confiance est l'élément central des systèmes monétaires fiduciaires.

La monnaie a trois fonctions traditionnelles. La première est d'être un moyen d'échange permettant d'éviter le troc. La seconde est d'être une unité de compte standard qui permet ainsi de comparer différents biens n'ayant aucun rapport ou *a priori* incomparable comme un fruit et un avion. Enfin la troisième fonction de la monnaie est d'être une réserve de valeur. Ces trois fonctions se retrouvent dans toutes les formes de monnaies.

Ce sont les banques centrales et les Etats qui ont le contrôle des monnaies traditionnelles. Toutefois, avec l'avènement de l'internet et l'avancée technologique, sont apparus de nouveaux systèmes monétaires, différents des systèmes monétaires fiduciaires. Ces nouveaux systèmes monétaires sont devenus numériques et virtuels. La Banque Centrale européenne définit la monnaie virtuelle : « *type de monnaie numérique non réglementée, qui est émise et généralement contrôlée par ses créateurs, et usée et acceptée parmi les membres d'une communauté virtuelle spécifique* »¹.

Le contrôle des autorités centrales sur la monnaie, la crise des *surprimes* de 2007 ainsi que les crises financières et sociales qui s'ensuivent sur toute la planète furent des éléments déclencheurs en ce qui concerne l'apparition des monnaies numériques chiffrées à l'instar du Bitcoin. En effet, à la suite de 2007, la défiance du système financier mondial et des Etats, qui protègent et tentent de sauver les banques, devient de plus en plus grande. Au point que certains se disent qu'ils vivent dans un monde très opaque où la collusion entre gouvernements et entreprises financières se fait au détriment du peuple. Ces personnes ont pour ambition d'obtenir de plus en plus de transparence et de moins en moins de contrôle de la monnaie au profit de la population mondiale. Selon eux la monnaie fiduciaire est aux mains d'une élite financière et politique se souciant bien peu de l'intérêt général et du bien-être des populations, qu'elles soient dans des pays développés ou dans des pays sous-développés n'ayant pas accès au système bancaire.

L'idéologie principale qui mène à la création de ces monnaies numériques et chiffrées, appelées crypto-monnaies, découle du mouvement libertaire dont l'un des buts est de diminuer le plus possible les pouvoirs de l'Etat.

Le commerce sur internet de nos jours passe essentiellement par les banques qui servent de tiers de confiance. En droit, les tiers de confiance sont les sociétés qui délivrent des certificats de signature, qui fournissent des outils de signature ou encore qui délivrent des infrastructures techniques. Les banques, à travers leur rôle de tiers de confiance, permettent donc le paiement électronique.

Toutefois, les banques ont d'autres activités commerciales et parfois des litiges. Leur marge économique et le coût du risque sont répercutés sur le coût des transactions, car elles sont en situation, parfois, oligopolistiques. En outre même si le système fonctionne, il y a

¹ Rapport de la BCE, les monnaies virtuelles, publié en février 2015, consulté sur (www.ecb.europa.eu) le 31/07/2019

parfois des crises de confiance, comme celle issue de la crise financière de 2007 qui va donner naissance au système Bitcoin et à l'idée de transactions à très faibles coûts pour le bien des utilisateurs, en particulier ceux des pays sous-développés n'ayant pas accès à des banques en raison de coûts prohibitifs.

Les crypto-monnaies sont créées pour s'échanger la valeur sur internet. Ces nouvelles monnaies sont fondées sur une nouvelle technologie : le block Chain. Elle autorise une gestion décentralisée de la monnaie sans Tiers de confiance à l'opposé des systèmes hiérarchisés et centralisés des monnaies officielles.

L'innovation monétaire est encore plus profonde, voir radicale. Les crypto-monnaies sont des monnaies privées, sans cours légal, sans aucun adossement physique ou financier et totalement virtuelles : elles se créent et circulent indépendamment de toute banque et sont détachées de tout compte bancaire. Ce sont des objets nouveaux, sans véritable précédent dans l'histoire. Il existe aujourd'hui plus de 2000 crypto-monnaies pour une capitalisation de marché estimée à plus de 270 milliards de dollars².

Autrement dit, le système bancaire est le résultat du développement du réseau bancaire depuis de nombreuses années, voir 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 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 Taiwan, la Russie et autres, y compris l'Algérie, ont déclaré illégale l'utilisation du Bitcoin sur leur territoire, aussi 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. Alors que les chiffres de son expansion et du développement du réseau sont cependant assez éloquentes. Si à peine 5000 transactions étaient réalisées en bitcoin par jour en 2011, leur nombre était de 50 000 en 2012, pour atteindre 4 millions de BTC par jour, le maximum historique de cet indicateur en Novembre 2017. En Janvier 2019, ce

² Jean-Pierre Landau, Alban Genais, "*Les crypto-monnaies*" Rapport au ministre de l'Economie et des Finances, du 04/07/2018, en ligne sur (<http://www.ladocumentationfrancaise.fr>) consulté le 01/08/2019

volume a atteint 2.7 millions de BTC par jour.

PROBLEMATIQUE

Face à ce paradoxe, il nous a semblé pertinent de poser la problématique suivante :

La crypto-monnaie, en tant que monnaie supranationale, pourrait-elle se substituer aux monnaies nationales de par les fonctions qui leurs sont traditionnellement attribuées ?

❖ **Sous questions :**

La réponse à cette problématique implique les réponses aux questions suivantes :

- Comment cette monnaie, sans autre réalité que celle d'un code chiffrant a-t-elle pu voir le jour ? Et comment fonctionne-t-elle ?
- Quels sont les bénéfices et les risques liés à son utilisation ? Et faut-il la réguler ?
- Va-elle bouleverser le système bancaire traditionnel, voir impacter la politique monétaire ?

❖ **Les hypothèses :**

Pour répondre à ces questions, nous formulons les hypothèses suivantes :

1. Les crypto-monnaies, en particulier le Bitcoin, représentent pour la monnaie une innovation majeure analogue à celle qu'a été le web dans le domaine de l'information. Susceptible de bouleverser la sphère monétaire.
2. La technologie décentralisée des crypto-monnaies, sophistiquée qu'elle soit, constitue un piètre substitut à des institutions solides, en l'occurrence les banques centrales, garantes de l'émission de la monnaie.
3. Les crypto-monnaies dans leur forme actuelle restent un modèle monétaire controversé.

❖ **Le choix du sujet :**

Le choix de ce sujet est né de ma passion à un univers relativement nouveau, mouvementé et novateur, et de mon désir de le découvrir et de le partager.

❖ **Les objectifs du sujet :**

Le 1^{er} objectif est que les crypto-monnaies sont encore assez méconnues, voir mal vues du grand public, donc il est nécessaire de comprendre ce nouvel écosystème pour pouvoir y participer et en profiter.

Le 2^{ème} objectif est de montrer que les crypto-monnaies ne se limitent pas à des transactions douteuses et des variations de cours erratiques, derrière elles se cachent de

vraies équipes avec de vrais projets et de nouveaux modèles.

Le 3^{ème} objectif est que nous sommes à l'aube d'une révolution qui va plus loin que la redéfinition de la monnaie et l'avènement de la décentralisation et qui se déroule sous nos yeux.

❖ **La méthodologie de recherche :**

L'étude en question entre dans le cadre d'un essai de compréhension de monnaies dites virtuelles ou digitales, qui ont connues un essor phénoménale ces dernières années, en particulier depuis l'apparition de Bitcoin. Un phénomène qui change chaque jour, chaque heure, chaque minute voir chaque seconde et qui a bouleversé le monde de la finance. Une évolution historique relativement rapide à l'échelle de l'histoire des monnaies.

Ce qui nous a amené à opter pour une démarche méthodologique d'analyse descriptive basée sur la recherche documentaire à travers la consultation d'ouvrages, recherches, revues, textes réglementaires et sites internet relatifs à ce sujet, afin de montrer l'intérêt de la création et l'utilisation de cette monnaie, son développement ainsi que son impact sur l'économie mondiale, mais aussi ses risques et limite.

CHAPITRE 1

L'apparition et l'histoire de la crypto
monnaie

Introduction :

Le monde de la finance est sur le point de changer drastiquement. Un nouvel arrivant vient de pénétrer ce gigantesque marché de plusieurs milliers de milliards de dollars et il entend s'imposer. Les monnaies du monde entier, et avec elle le reste du système financier ont été règlementées et gérées de façon centralisée depuis bien longtemps. Cependant, là où étaient attendues stabilité économique et prospérité, on a souvent vu naître des crises économiques, des krachs boursiers, voir même des guerres.

Le besoin d'un refuge capable de soutenir les futurs chocs économiques se fait clairement sentir.

La demande croissante de transaction à la fois plus rapide et plus sécurisée pourrait bien, à l'heure d'internet, trouver sa réponse dans les crypto-monnaies. Un large écosystème se développe autour de cette monnaie. Elle mobilise une population importante et active de startups et d'investisseurs. Elles perturbent potentiellement les banques et intermédiaires financiers traditionnels, à la fois soucieux d'en tirer les bénéfices technologiques et ne pas déstabiliser leur modèle de fonctionnement.

Le dynamisme des crypto-monnaies et l'engouement dont elles bénéficient résultent d'une triple évolution : un progrès technologique réel, un profond mouvement de société et, plus conjoncturellement, des conditions financières très accommodantes.

Dans ce deuxième chapitre, nous allons évoquer de la genèse de la crypto-monnaie, son évolution et de ses enjeux.

Il sera divisé en trois sections, dans la première section nous allons aborder l'histoire de la monnaie (préhistoire, naissance et évolution), dans la deuxième, la combinaison des techniques qui a permis l'existence d'une telle technologie innovatrice et dans la troisième ses enjeux et son avenir.

Section 01 : Histoire de la crypto monnaie**1. Histoire :**

L'origine du block Chain date des années 1990, alors que différents groupes d'informaticiens s'efforçaient de comprendre et de perfectionner le potentiel des nouvelles technologies numériques et des avancées en cryptographie, et ce, afin de développer des outils qui permettraient de mieux protéger la vie privée des individus³.

Le mouvement des crypter punks, un groupe ayant pour ambition de démocratiser

³ «Qu'est-ce que la crypto monnaie ? », ALTcoin conseil, 07/07/2019

l'accès aux nouvelles technologies de chiffrement, y apporte une contribution importante. Avec l'invention de la cryptographie asymétrique (à double clé) et grâce au développement du système de chiffrement RSA en 1977 développé par trois chercheurs du MIT (Ronald Rivets, Adi Shamir et Leonard Adleman, dont les initiales sont à la base de l'acronyme), la cryptographie est progressivement devenue un outil accessible à toute personne désirant communiquer de façon sécurisée sur un réseau ouvert tel qu'internet. La cryptographie à double clé permet en effet de garantir non seulement la confidentialité, mais aussi l'authenticité et l'intégrité des communications en ligne. Les cypherpunks se sont ainsi approprié ces nouvelles technologies dans le but de préserver la vie privée et la liberté d'expression et même d'en promouvoir la défense, dans un environnement numérique qui commençait déjà à remettre en question un certain nombre de libertés fondamentales.

Mais au sein du mouvement des rypberpunks, certains individus avaient des motivations qui s'étendaient bien au-delà de la protection des libertés fondamentales, animés non seulement par le désir de préserver la vie privée et la liberté d'expression des internautes, mais non moins fortement par le désir d'échapper au contrôle étatique, ainsi qu'au contrôle exercé par les grandes entreprises qui s'installaient sur le réseau. C'est le cas, notamment, des « crypto-anarchistes », qui s'inscrivent dans un courant de pensée beaucoup plus politisé, avec des tendances souvent anarcho-capitalistes. Ces individus revendiquent la suprématie du marché et recherchent une complète indépendance à l'égard de toute institution étatique ou gouvernementale. Les crypto-anarchistes refusent de se soumettre aux lois des Etats et n'obéissent qu'à leurs propres systèmes de règles, qui sont à fois définies et appliquées par le code informatique.

Les idéologies sous-jacentes à ce mouvement ont été analysées et décrites en détail par Timothy C. May, auteur du Manifeste de la crypto-anarchie, rédigé en 1989 mais toujours d'actualité, où il résume les problématiques soulevées par le développement de ces nouvelles technologies de communication décentralisée et de chiffrement : « Tout comme la technologie de l'imprimerie a modifié et réduit le pouvoir des guildes médiévales et la structure du pouvoir social, les méthodes cryptologiques vont fondamentalement modifier la nature des sociétés et l'ingérence du gouvernement dans les transactions économiques. [...] Et juste comme une invention apparemment mineure comme le fil de fer barbelé rendu possible la clôture de vastes ranchs et de fermes changeant ainsi pour toujours les concepts de terre et de droits de propriété en Occident, la découverte apparemment mineure d'une branche mystérieuse des mathématiques deviendra le coupe-file qui démantèlera les barbelés autour de la propriété intellectuelle De façon générale, quelle que soit leur appartenance politique, les cypherpunks

soutenaient un idéal de société plus libre et décentralisée, une société où la technologie permettrait aux internautes d'interagir et de communiquer librement sans être soumis à aucune forme d'intimidation ou de représailles éventuelles de la part des États ou d'autres institutions, publiques ou privées

2. Première apparition :

Bitcoin a été conçu en 2008 par un individu (ou un groupe d'individus) caché sous le pseudonyme de Satoshi Nakamoto. Le 31 octobre 2008, Nakamoto publiait un livre blanc intitulé Bitcoin : A Peer-to-Peer Electronic Cash System sur une liste de diffusion orientée crypto graphie (metzdowd.com). Le livre blanc décrivait un système de paiement décentralisé accompagné d'une monnaie virtuelle pouvant être échangée entre pairs, et ce, sans qu'il soit nécessaire de passer par aucune banque ni aucun intermédiaire financier. L'idée assez ambitieuse consistait à créer un système de paiement décentralisé capable de fonctionner indépendamment de toute autorité de confiance, et qui serait en mesure de répliquer, voire de remplacer, le rôle des institutions financières.

Bitcoin est tout d'abord un système de paiement pair à pair permettant le transfert de valeur sur Internet de façon sécurisée et complètement décentralisée. Pour son fonctionnement, Bitcoin utilise un réseau de communication pair à pair avec des mécanismes de stockage réparti qui lui permettent de fonctionner sans opérateur centralisé. Il emploie aussi des techniques cryptographiques qui, combinées les unes avec les autres, ont permis l'établissement d'un système extrêmement fiable et sécurisé qui n'a toujours pas été piraté

3. Evolution :

Les crypto monnaies ont de nouveau suscité l'intérêt des investisseurs, avec de solides performances en 2020. Une spéculation accrue, les espoirs de pouvoir se couvrir contre les baisses des marchés actions et le risque inflationniste ainsi que le développement des actifs numériques sont autant de raisons pouvant expliquer les nouveaux sommets atteints par les cours des crypto monnaies. Les risques demeurent toutefois élevés, et même si certains hedge funds peuvent trouver intéressant d'investir dans une forte volatilité, nous ne sommes pas convaincus par l'allocation aux monnaies numériques au sein d'un portefeuille stratégique.

Section 02 : La crypto monnaie, une innovation fondée sur une combinaison de techniques préexistantes :

1. Une base de données décentralisée :

Pour enregistrer les transactions effectuées sur le réseau, Bitcoin s'appuie sur une base de données assez standardisée de type clé-valeur (key-value database). Ces bases de données

sont organisées sous la forme d'un dictionnaire de clés auxquelles sont associées des valeurs.

Alors qu'il est possible de stocker tout type d'information dans le champ des valeurs, on ne peut y accéder que si l'on connaît la clé qui lui est associée. Étant donné la simplicité de ces systèmes, les bases de données de type clé-valeur sont généralement plus rapides que les autres bases de données de nature plus structurée, et peuvent gérer plusieurs millions de requêtes avec un temps de réponse très court. Base de données ne connaît pas la nature, ni la structure. Cependant, puisque la base des données stockées dans le champ de valeurs,

Elle est incapable de les traiter ou de les manipuler par elle-même. Tout traitement doit se faire par l'intermédiaire d'un système externe à la base de données.

La blockchain de Bitcoin se distingue des bases de données traditionnelles (gérées par des opérateurs centralisés), car elle est administrée de manière collective par l'ensemble des membres qui interagissent sur le système. Bitcoin s'appuie sur un protocole informatique qui va dicter les règles et les procédures à suivre afin de permettre l'enregistrement des transactions de manière sécurisée et décentralisée.

2. Le chiffrement à double clé :

L'une des briques les plus importantes utilisées par Bitcoin pour assurer la sécurité du réseau est la cryptographie asymétrique à pour assurer double clé. Alors que les mécanismes de cryptographie symétrique impliquent que les individus qui communiquent entre eux se soient accordés sur une clé de chiffrement commune, la cryptographie asymétrique est une méthode qui permet à plusieurs individus de communiquer sur un réseau non sécurisé sans avoir besoin de transmettre une clé de chiffrement.

Chaque individu génère une paire de clés, une clé privée qu'il ne dévoile à personne, et une clé publique qu'il peut communiquer librement sur le réseau. Le système est sécurisé car, même s'il est toujours possible de générer une clé publique à partir d'une clé privée, il est cependant impossible de récupérer une clé privée à partir d'une clé publique. Ainsi, lorsqu'un individu désire communiquer de façon confidentielle avec un autre individu, il lui suffira de chiffrer le message avec la clé publique de ce même individu et d'envoyer le message chiffré sur le réseau. Même si le message est intercepté, seul le destinataire pourra accéder au contenu du message, puisque le message ne pourra être déchiffré qu'avec sa propre clé privée.

La cryptographie à double clé avait initialement été conçue pour assurer la confidentialité des communications dans un réseau non sécurisé, où il serait dangereux de transmettre une clé de chiffrement symétrique. Toutefois, ce mécanisme peut aussi être utilisé pour garantir la source ou l'authenticité des communications numériques. En chiffrant un

message avec sa clé privée, un individu peut authentifier le message avant de le partager sur le réseau. Son contenu pourra ensuite être déchiffré par tous ceux qui ont accès à la clé publique de l'expéditeur.

Ce mécanisme permet d'obtenir deux résultats distincts. En premier lieu, il permet de vérifier message provient bien d'un individu donné. En second que le lieu, il rend la répudiation de ce message impossible, car le message ainsi chiffré ne peut avoir été constitué que par la personne qui détient la clé privée. Cette technique est utilisée aujourd'hui dans un grand nombre de systèmes de signature électronique.

Dans le modèle de Bitcoin, le chiffrement à double clé a pour fonction de prouver que toute personne commençant une transaction est bien la propriétaire des fonds à transférer.

Avant d'être communiquée au réseau, chaque transaction est signée avec la clé privée de l'émetteur. Les membres du réseau responsables de la vérification des transactions pourront alors contrôler que la transaction a bien été signée avec la clé privée associée à l'adresse qui émet cette transaction, et que cette adresse détient suffisamment de bitcoins pour assurer cette transaction. Si ces deux conditions sont remplies, la transaction sera validée avant d'être enregistrée au sein de la blockchain de Bitcoin

3. Hachage et protocole de consensus distribué :

3.1. Les fonctions de Hachage :

Une fois validées, les transactions sont enregistrées, de façon chronologique, au sein d'un bloc de transactions, qui incorpore une référence aux blocs précédents. Cette référence, créée par le biais d'une fonction de hachage cryptographique (hash function, en anglais), joue un rôle fondamental pour garantir l'intégrité de toute la chaîne de transactions.

Une fonction de hachage est une fonction particulière qui prend une chaîne de caractères (ou un fichier numérique) comme paramètre d'entrée, et qui produit une nouvelle chaîne de caractères, de longueur prédéfinie, comme paramètre de sortie. Cette chaîne représente l'empreinte numérique (digital fingerprint) du fichier, elle permet de l'identifier de façon unique. Une particularité essentielle de toute fonction de hachage est qu'il est pratiquement impossible de générer la même empreinte numérique pour deux paramètres d'entrée différents (et le risque de « collision » peut être réduit rapidement en augmentant la longueur de la chaîne de caractères en sortie). Une autre caractéristique importante liée à la fonction de hachage est que toute modification apportée à un paramètre à l'entrée, si minime soit-elle, générera une chaîne de caractères complètement différente à la sortie. Il est donc impossible de dériver ou de déduire des informations concernant un fichier à partir de sa seule empreinte numérique

L'empreinte d'un fichier permet donc non seulement d'identifier des documents ou des fichiers numériques, mais aussi d'en vérifier l'intégrité. Bien qu'il soit impossible de renverser la fonction de hachage pour récupérer le contenu d'un fichier à partir de son empreinte numérique (à moins de procéder à une attaque en force, en essayant toutes les possibilités), l'empreinte numérique peut tout de même être utilisée pour vérifier qu'un document correspond effectivement au fichier précédemment «haché ». Cela est très utile pour la transmission de fichiers sur un réseau non sécurisé, puisqu'il est possible de comparer les empreintes d'un fichier avant et après la transmission afin de s'assurer que la communication s'est bien déroulée et de vérifier que le fichier n'a pas été altéré entre-temps.

Bitcoin utilise les arbres Merkle pour organiser les transactions au sein de chaque bloc de la chaîne, où chaque transaction peut être identifiée de façon unique grâce à son empreinte numérique. Cela permet de vérifier rapidement si une transaction a bien été enregistrée au sein d'un bloc, mais aussi de s'assurer qu'aucune transaction n'a été manipulée au cours du temps.

Chaque bloc de transactions sera, à son tour, « haché » : il en dérivera une empreinte numérique qui sera, elle, incorporée à l'intérieur du bloc suivant créant ainsi une longue chaîne de blocs qui se référencent les uns après les autres.

3.2. Le protocole de consensus distribué :

Alors que le processus de minage permet de garantir la sécurité et l'intégrité du réseau, le protocole de « consensus distribué » (distributed consensus, en anglais) adopté par Bitcoin permet de s'assurer qu'à tout moment les membres du réseau peuvent se mettre d'accord sur un état donné de la blockchain.

En effet, le réseau étant décentralisé, les transactions peuvent être reçues (et traitées) dans un ordre différent par les différents nœuds du réseau. Si plusieurs blocs de transactions sont validés en même temps par différents mineurs.

Il sera impossible de déterminer objectivement lequel de ces blocs devrait avoir la priorité sur les autres. Cela est d'autant plus critique lorsqu'il existe un conflit potentiel entre les transactions incorporées au sein de ces blocs. Par exemple, un individu avec un solde de 3 Bitcoins pourrait tenter d'effectuer deux transactions de 2 Bitcoins chacune. Ces deux transactions pourraient paraître valides si chaque opération est considérée individuellement. Pourtant, les deux transactions sont mutuellement incompatibles, car leur somme dépasse le solde existant de trois Bitcoins. Il s'agit là d'un problème plus couramment connu sous le nom de la « double dépense ».

Pour résoudre ce problème, Bitcoin a mis en place un protocole de consensus distribué

qui permet au réseau de trancher, et de déterminer, en cas de conflit, quel sera le bloc de transactions qui aura la priorité sur les autres. Ce protocole prévoit que les membres du réseau devront toujours sélectionner la chaîne de blocs la plus longue (celle qui a demandé une plus grande puissance de calcul, et donc de « preuve de travail »

Ainsi, lorsque deux blocs sont attachés simultanément à la même chaîne, une bifurcation se crée au sein de la blockchain. Étant donné que les deux bifurcations sont de la même longueur, il sera difficile pour le réseau de déterminer lequel de ces deux blocs prévaudra sur l'autre. Ce sera donc aux mineurs de décider, au moment de la création d'un nouveau bloc, lequel de ces deux blocs sera privilégié. Le conflit est résolu dès lors qu'un nouveau bloc de transactions est validé par le réseau et que l'une des deux bifurcations devient ainsi la chaîne la plus longue. Certes, rien n'empêche certains mineurs de continuer à référencer l'autre chaîne, mais cela risquerait de leur coûter cher (en énergie), puisque les blocs appartenant à la chaîne la plus courte seront tout simplement ignorés par la majorité du réseau, y compris les Bitcoins émis lors de la création de ces blocs.

Dans une perspective économique, les mineurs ont donc intérêt à respecter le protocole et à ne référencer que les blocs appartenant à la chaîne la plus longue.

L'avantage de fonder le protocole de consensus distribué sur la quantité de « travail » investi dans le processus de minage réside dans le fait que toute tentative de manipulation du réseau deviendrait extrêmement coûteuse. La modification d'une transaction enregistrée au sein d'un bloc de la chaîne obligerait en effet l'attaquant à résoudre une nouvelle fois l'équation associée à ce bloc (dont l'empreinte numérique aurait nécessairement changé), et à résoudre aussi toutes les équations associées aux blocs suivants. Puisque les membres du réseau ne considèrent que la chaîne la plus longue comme valide, il sera pratiquement impossible pour l'attaquant de « récupérer le retard ». En effet, seul un mineur (ou un groupe de mineurs) contrôlant plus de 50 % de la puissance de calcul investie dans le réseau sera capable de créer des blocs plus rapidement que le reste du réseau, c'est ce qu'on appelle une attaque à 51 %. C'est grâce à ce système que Bitcoin a résolu le problème de la double dépense, ainsi que le problème des attaques de type Sibylles qui affectent beaucoup de systèmes de paiement décentralisés.

Conclusion :

Au cours de l'année écoulée, certaines entreprises ont commencé à accepter les Crypto-monnaies comme moyens de paiement, et de plus en plus de sociétés de services financiers ont mis au point des plates-formes permettant aux utilisateurs d'acheter, de vendre

et de transférer des crypto-monnaies.

En outre, les banques centrales du monde ont commencé à se pencher sur les monnaies numériques de banque centrale (MNBC), une version numérique des monnaies traditionnelles. Les adeptes considèrent que les MNBC sont un moyen de répondre au déclin de l'utilisation de l'argent liquide dans la société actuelle, et d'améliorer la transmission de la politique monétaire. Les détracteurs se méfient des attaques informatiques, des contrefaçons et des fraudes potentielles. En particulier, les monnaies numériques de banque centrale peuvent surtout diminuer la valeur ou accroître les risques des monnaies numériques existantes¹¹.

Il est fort probable que ces moteurs de marchés des crypto-monnaies persisteront vraisemblablement dans les prochaines années, mais cela ne justifie pas forcément l'investissement dans les crypto-monnaies comme actifs à part entière. Les infrastructures sont encore récentes et exposées à divers risques, au-delà des inquiétudes liées à leur adoption, notamment à des risques légaux et réglementaires.

Selon les économistes, les crypto-monnaies coexisteront probablement avec la monnaie liquide, bien installée, émise et contrôlée par les États, mais ne la remplaceront pas. À long terme, ce pourrait être le concept sous-jacent et la technologie de la Blockchain qui se révéleront révolutionnaires.

CHAPITRE 2

L'impact des crypto monnaies,
leurs enjeux, perspectives

Introduction :

Depuis quelques années, nous assistons à l'émergence d'une monnaie d'un genre nouveau reposant sur des procédés cryptographiques, gérées en pair à pair selon un consensus distribué. Ces crypto-monnaies viennent, heurter la conception traditionnelle de la monnaie : unitaire, souveraine, territoriale et centralisée, contester un ordre monétaire fondé sur le crédit et le pouvoir bancaire, interroger la théorie et renouveler le débat sur la nature de la monnaie.

Les crypto-monnaies sont, à l'heure actuelle, en plein essor et commencent à faire parler d'elles. Or, loin de recueillir l'adhésion de plus grand nombre, elles attirent plutôt la méfiance, la suspicion et les critiques. Elles affichent de nombreuses limites les empêchant d'évoluer vers le statut de devises à part entière. Ce qui interpelle les régulateurs et les superviseurs du système financier à s'interroger sur une évolution du cadre réglementaire adaptée à l'essor de ces monnaies dans une démarche concentrée à l'échelle européenne et internationale.

En 02/11/2012, Tracfin a piloté un groupe de travail sur les nouveaux moyens de paiement qui avait, entre autres, abordé les risques et menaces liés aux monnaies virtuelles. Depuis, les crypto-monnaies n'ont cessé de faire l'objet d'une actualité dans tout en raison de leurs usages licites qu'illicites⁴. Les possibilités d'utilisation des monnaies virtuelles s'étendent, tandis que celles-ci prolifèrent et en retour, les réactions, nationales et internationales, se sont multipliées.

Après avoir procédé à une clarification de ce que sont initialement les crypto-monnaies et l'écosystème lié à ce type de monnaie. Nous analyserons dans ce chapitre, en premier lieu différents changements que peuvent apporter les crypto-monnaies au système de paiements (section 1), ensuite nous exposerons les enjeux et risques que présente l'utilisation de cette monnaie (section2) sur l'économie en général et la finance en particulier. Et enfin, nous citerons quelques recommandations proposées par des institutions européennes et internationales pour maîtriser et orienter ces crypto-monnaies, et limiter leurs risques.

⁴ A ce titre, la fermeture le 02 octobre 2013, par les forces de l'ordre américaines, du site internet "Silk Road" hébergé sur le "Dark web" spécialisé dans la vente de produits illicites, notamment des stupéfiants, utilisant exclusivement les bitcoins pour le règlement des transactions, est emblématique.

SECTION 1 : Les paiements de demain

La dimension monétaire est importante dans le projet qu'incarnent les crypto-monnaies, mais elle n'est pas exclusive. L'ambition est également, et peut-être d'abord, technologique et économique. Un véritable système de production et d'accompagnement se développe autour de l'activité des crypto-monnaies. La blockchain, elle-même, offre de nombreuses perspectives. La possibilité de stocker et de transférer de la valeur sur des unités virtuelles, divisibles et fongibles peut changer le paysage de la finance, des échanges et de la production. Dans le foisonnement actuel d'initiatives et de projets, il est important de bien identifier les opportunités et d'en mesurer les risques.

L'actualité immédiate et les vicissitudes rencontrées par les crypto-monnaies ne doivent pas pour autant éclipser leur ambition fondamentale qui, au-delà de la dimension monétaire, est également, et peut-être avant tout, technologique et économique. Un véritable système de production et d'accompagnement se développe autour de l'activité des crypto-monnaies.

Les monnaies virtuelles et la blockchain peuvent avoir une importante influence sur les paiements dans le monde réel. Ajouter à la monnaie de nouveaux rôles et même donner naissance à de nouveaux métiers.

1. Les nouveaux rôles de la monnaie

Les crypto-monnaies s'inscrivent dans la droite ligne des évolutions récentes de la monnaie : plus internationale, plus dématérialisée et moins « chères » que les monnaies fiduciaires. Si elles sont de très bons intermédiaires des échanges, les crypto-monnaies sont encore de piètres de valeur et unités de compte du fait de leur volatilité. La monnaie en plus de rester une réserve de valeur, un intermédiaire des échanges et une unité de compte, va devenir également grâce aux crypto-monnaies un vecteur d'information⁵.

1.1. L'adaptation de la monnaie aux évolutions de la société :

Comme toute chose, les monnaies évoluent. Quand le concept de monnaie est apparu, les hommes utilisaient des objets naturels tels des coquillages, des dents d'animaux, des pierres, etc. c'est au septième siècle avant J-C, que serait apparu la monnaie sous forme de pièces, et à la renaissance celle sous forme de billets. A la fin du XX^e, la

⁵ Enée Bussac, Op.cit. P177-180.

monnaie s'est dématérialisée avec l'apparition et la généralisation des comptes en banques, transfert et cartes de crédit. L'explosion d'Internet et des smartphones, respectivement au début et à la fin des années 2000, a accéléré ce mouvement de dématérialisation, si bien que beaucoup de personnes n'utilisent quasiment plus d'argent liquide et que des Etats comme la Suède pensent l'abolir. (La Suède a adopté très vite les cartes de crédit, puis les paiements par smartphone. Elle pense aujourd'hui à créer sa propre crypto-monnaie : l'e-Krona.).

En même temps, nous sommes de plus en plus connectés et mobiles : la plupart de nous avons un smartphone, on peut commander à peu près tout depuis son ordinateur ou son smartphone, et les banques sont de moins en moins gourmandes en frais quand on utilise sa carte de crédit ou envoie de l'argent à l'étranger. Dans les pays moins développés, beaucoup de personnes n'ont pas de compte en banque. De même que, dans ces pays, la population est passée directement du téléphone classique chez soi au smartphone sans passer par la case ordinateur personnel, elle va probablement passer du tout cash aux crypto-monnaies sans passer par la case compte en banque.

La monnaie doit suivre ses évolutions, à savoir, continué à se dématérialiser, être « moins chère », plus pratique et s'affranchir des frontières : c'est exactement ce que proposent les crypto-monnaies. Plus celles-ci vont être acceptées par le monde réel, plus leur usage va devenir naturel et leurs avantages vont permettre de s'imposer comme le nouveau standard monétaire. Elles ont besoin pour cela d'un cadre légal qu'elles n'ont pas encore, faute de régulation globale. Il faut bien comprendre que les crypto-monnaies, en tant que monnaie et donc réserve de valeur, unité de compte et intermédiaire des échanges, ne sont que la première application de la technologie de la blockchain, et que celle-ci peut être représenté et géré numériquement.

1.2. Le défi de la décentralisation :

Les nouveaux systèmes apportés par les crypto-monnaies, en l'occurrence la technologie de la blockchain qui se cache derrière, posent le défi de trouver un juste milieu entre la centralisation de la gestion monétaire, qui était de rigueur dans le monde pré-blockchain, et la décentralisation prônée par quasiment toutes les crypto-monnaies, pour continuer à assurer sécurité et fluidité aux marchés. Comme les Etats ne vont *à priori* pas disparaître, il y aura toujours une certaine centralisation des pouvoirs. Mais ces pouvoirs seront constamment mis à l'épreuve par les mécanismes décentralisés basés sur la blockchain.

Les banques et Etats vont devoir accepter cette nouvelle exigence de décentralisation. Comme avec Internet il y a vingt ans, les entreprises qui intégreront ce mouvement de décentralisation seront les grandes gagnantes de cette nouvelle ère qui s'annonce. Toutes les entreprises et administrations publiques s'intéressent aujourd'hui de près ou de loin à la blockchain et ont mis en place des groupes internes de travail et de réflexion et collaborent avec des sociétés spécialisées pour explorer les moyens de tirer parti de cette technologie dans leur activité.

Centralisation et décentralisation ont chacune leurs avantages et leurs inconvénients : la centralisation permet d'être efficace mais pose la question de l'ouverture et de la démocratie, la décentralisation permet à chacun de participer et de savoir ce qui se passe mais entraîne une certaine inertie dans la prise de décision et un manque de moyens. Ce que beaucoup d'entreprises derrière les crypto-monnaies essaient de trouver, c'est le juste milieu entre centralisation et décentralisation.

1.3. L'efficience des marchés :

Les crypto-monnaies sont de « super intermédiaires des échanges » car elles s'affranchissent des frontières, sont totalement dématérialisées, ont des délais et des coûts de transaction très faibles, et comportant toutes des systèmes de paiement très performants basés sur la cryptographie.

Une bonne monnaie rend les marchés efficaces, c'est-à-dire qu'elle rend les échanges très fluides et la fixation des prix des produits et services très efficaces. Les crypto-monnaies vont propulser l'efficience des marchés vers de nouveaux sommets et même acquérir une quatrième fonction.

1.4. La monnaie se dote d'une quatrième fonction :

Il semble acquis que la vague de dématérialisation de la monnaie va se poursuivre et que les crypto-monnaies vont y contribuer.

Les crypto-monnaies permettent de dissocier Etats, banques et création de monnaie. Ce service sera assuré par des entreprises, associations, ONG, administrations, etc., qui soit émettront leur propre monnaie, soit proposeront ce service ou une monnaie dédiée à un certain usage ou un certain secteur. Nous paierons notre achat sur Amazon en « Amazon coin »,

MacDonald's en « MCDO », etc., ou plutôt notre solution de paiement en crypto-

monnaie le fera pour nous.

La monnaie, en plus de devenir une réserve de valeur, un intermédiaire des échanges et une unité de compte plus efficaces, va acquérir du coup une quatrième fonction en devenant également un vecteur d'information, car suivant l'unité monétaire, le montant de crypto-monnaies et le destinataire que nous choisirons, le marché saura ce que nous souhaitons acquérir. Envoyer un certain montant d'un certain coin à un certain public adresse à un certain moment équivaldra à un ordre qui enclenchera une action.

En devenant un vecteur d'information, la monnaie va faire augmenter le volume de celles-ci car on pourra savoir, simplement en fonction des monnaies que les gens et les entreprises dépensent, quels biens, services, ..., ils utilisent et éventuellement où ils le font, ce qui pourra être utile à des fins d'analyses économiques et de traçabilité.

1.5. Le contrôle de la monnaie :

La monnaie est un instrument économique fondamental. Les Etats, si un jour n'en émettent plus telle que nous la connaissons, ou s'ils laissent des entreprises en émettre, comme c'est le cas *de facto* avec les crypto-monnaies, devront ou essayeront de contrôler son émission. Créer une monnaie va être soumis à une stricte réglementation. Les Etats encadreront cette activité par des organismes de surveillance, mais ne seront plus les seuls à assurer ce service, économisant ainsi des sommes non négligeables et accumulant même des revenus fiscaux perçus sur les licences de création de monnaie et la création de monnaie elle-même. Les

« Corporate coins », plus encore que les actions, reflèteront instantanément et directement la performance de l'entreprise émettrice. Celles-ci devront aussi nouer des alliances avec les émetteurs d'autres monnaies, les exchanges et les sociétés de solutions de paiement pour que leur monnaie se répande dans l'économie.

Une crypto-monnaie est relativement facile à créer. Tout individu pourrait émettre demain une monnaie et essayer de la « vendre ». Il aurait cependant bien du mal, car ce qui donne de la valeur à une monnaie, c'est encore et toujours la confiance en l'entité émettrice. Cette facilité potentielle de création de la monnaie pose le problème du contrôle des ICO, et de celui de l'émission de monnaie de demain. Les ICO devraient être la première partie du monde des crypto-monnaies à être régulée. Quant au contrôle de l'émission de monnaie de demain, il peut être assuré de deux façons : sur les émetteurs et sur les receveurs de la monnaie.

Si demain les Etats n'assurent plus la création de la monnaie comme nous la connaissons aujourd'hui, des sociétés privées s'en chargeront pour elles-mêmes ou pour d'autres sociétés. De grands groupes pourront émettre plusieurs monnaies avec chacune des usages et un public bien précis, internes ou externes. Les entreprises qui souhaitent émettre de la monnaie acquerront pour ce faire une licence et devront payer des taxes auprès d'une administration publique si elles respectent certains critères de solvabilités et de liquidité, et qu'elles fournissent régulièrement des comptes sur leurs activités à l'instance régulatrice. Les Etats se doteront de telles instances afin de ne pas laisser n'importe qui émettre de la monnaie sur leur territoire, et collaboreront pour éviter les fraudes.

Nous pouvons cependant, par définition, acheter des monnaies émises hors de nos frontières ; c'est pour cette raison que le contrôle des receveurs de la monnaie est aussi indispensable que celui des émetteurs. Toute entreprise, tout commerce, devra déclarer à l'instance régulatrice les monnaies qu'elle accepte de ses clients et ne pourra pas accepter d'autres monnaies que celles-ci. Cette liste de monnaies acceptées sera intéressante pour les sociétés de solutions de paiement de crypto-monnaies, car le client final ne saura la plupart du temps pas dans quelle monnaie il paie vraiment. Un Etat pourra ainsi bannir des monnaies au fonctionnement trop opaque ou émises par exemple par des Etats ou organisations considérés comme terroristes ou ennemis.

2. Les nouveaux métiers :

L'avènement de la blockchain permettra à de nouveaux métiers de voir le jour. En voici quelques exemples :

2.1. Mineur :

Déjà évoqué plusieurs fois, et essentiel au fonctionnement de la blockchain, le métier de mineur est appelé à changer rapidement avec l'évolution des algorithmes Po (Proof Of) et il demande un investissement assez conséquent en argent (pour acquérir le matériel nécessaire) et en temps (pour se former et paramétrer et surveiller ses programmes).

Avec l'évolution des capacités de calcul des processeurs, et la généralisation des blockchains, nous deviendrons demain tous mineurs avec notre smartphone, sans même nous en rendre compte, et les blockchains que nous minons diront un peu qui nous sommes ou du moins ce que nous consommons.

2.2. Créateur de système de gestion de valeur fondé sur la blockchain :

La blockchain est la technologie qui nous permettra d'atteindre un nouveau stade d'efficience organisationnelle, en créant de nouveaux systèmes économiques et en optimisant grandement tous processus nécessitant une validation.

Il faudra des personnes et des entreprises pour adapter cette technologie à chaque entreprise, administration, association, etc. Ces personnes et entreprises existent déjà (Consensus par exemple⁶) mais sont relativement confidentielles.

2.3. Emetteur de crypto-monnaie :

Quand toutes les entreprises, artisans, administrations, associations, petites ou grandes, allemandes ou colombiennes, voudront avoir leur propre monnaie parce que c'est intéressant pour elles ou parce que leur Etat cessera d'émettre une monnaie nationale comme nous le connaissons aujourd'hui, elles auront besoin de compétences pour créer et gérer cette monnaie.

Les plus petites auront peut-être recours à des sociétés spécialisées dans l'émission de crypto- monnaies par secteur et/ou zone géographique.

2.4. Programmeur de blockchain :

Techniquement, une blockchain est un algorithme informatique. Etant un code open source, nous pouvons créer notre blockchain en copiant et adaptant une blockchain déjà existante ou en créant la nôtre, ce qui est plus compliqué.

Les compétences des programmeurs de blockchain vont être très évaluées. Il est essentiel de programmer la blockchain de manière parfaite, car une fois qu'elle est lancée, elle est difficile à modifier ou arrêter. L'architecture de la blockchain et son fonctionnement, dictés notamment par l'algorithme de consensus Po, sont des points essentiels qu'il faut mûrement réfléchir et correctement programmer. Protéger la blockchain contre les pirates est également une tâche importante des programmeurs.

2.5. Programmeurs de contrats intelligents :

Comme la blockchain, il vaut mieux être sûr de soi quand on lance un contrat intelligent, car une fois lancé, rien ne l'arrête, et une petite erreur de conception peut avoir

⁶ Consensus est une solution technologique de blockchain

de lourdes conséquences financières. Si les conditions, les montants ou les échéances, par exemple, sont mal programmés, une machine ou une personne peut se trouver coincé ou se voir refuser l'accès à un bien auquel elle a pourtant droit.

Le contrat doit aussi être inviolable pour qu'une personne ne s'approprie des droits. Comme un contrat intelligent fonctionne de manière quasi autonome, il peut créer d'importants problèmes s'il est détourné et si les parties ne s'n'en rendent pas compte suffisamment vite. Là aussi, des compétences informatiques et juridiques seront essentielles pour arriver à de bons résultats, et le métier de programmeur de contrats intelligents devrait devenir important.

2.6. Oracle (pourvoyeur d'information) :

Les contrats intelligents ont besoin de données qu'ils comparent aux clauses du contrat pour fonctionner. L'idée est qu'ils soient le plus autonomes possible, c'est-à-dire qu'ils puisent le plus possible ces données dans un réseau type Internet ou blockchain en fonction du comportement des parties du contrat et du temps. Mais ce n'est pas toujours possible.

C'est pourquoi un nouveau métier d'oracle, ou pourvoyeur d'information dans le monde réel, proche de celui d'huissier, est nécessaire au bon fonctionnement de certains contrats intelligents. Un oracle ira constater ou évaluer des événements du monde réel et fournira des informations au réseau sur lequel fonctionne le contrat intelligent pour que celles-ci soient traitées par les mineurs et que certaines actions soient enclenchées ou non, conformément aux clauses du contrat.

2.7. Gestionnaire de blockchain(s) :

La blockchain est un système autonome et décentralisé de stockage et transmission d'information ; il nécessite cependant d'être surveillé, alimenté et mis à jour périodiquement, une fois qu'un programmeur l'a créé.

Le gestionnaire de blockchain doit veiller à ce que le système fonctionne bien : vérifier que chaque acteur ait sa place et joue son rôle, laisser les bonnes personnes, machines, entreprises, intervenir sur le réseau, créer le nombre nécessaire de public addresses, les distribuer aux bonnes personnes et tenir un registre, contrôler le cours de la monnaie, etc.

2.8. Spécialiste de la traçabilité des transactions sur blockchain :

Si les crypto-monnaies se généralisent et deviennent un moyen de paiement répandu, et si les utilisateurs s'identifient systématiquement auprès des échanges et des pourvoyeurs de public adresses, alors il sera possible de tracer très efficacement les transactions effectuées avec les monnaies non anonymes, ce qui peut être utile pour l'administration fiscale ou juridique, les banques, la police, les assurances, etc.

Savoir reconnaître les public adresses en fonction de leur premiers caractères, savoir naviguer entre les blockchains, savoir qui contacter pour obtenir les informations manquantes seront des compétences précieuses pour ces entités.

3. Quel impact sur les paiements :

De par leur facilité de création et l'efficacité de leurs transactions, les crypto-monnaies permettent d'améliorer grandement les paiements, faisant de l'ombre aux systèmes utilisés par les banques et autres (PayPal et western union).

3.1. Le rôle des public adresses (adresses publiques) :

Pour rappel, les public adresses permettent de recevoir des coins, un peu comme l'IBAN d'un compte en banque. Quand nous envoyons des coins à un public adresse, nous ne pouvons pas y insérer de message comme dans un virement SEPA⁷. Pour pallier cela, il est possible de générer via un wallet un nombre quasiment infini de public adresses dérivées d'une clé privée pour recevoir des coins, ce qui a pour conséquence qu'une société ou un exchange à qui l'envoi des coins est destiné va générer une public adresse rien que pour nous, ce qui lui permettra de savoir que c'est nous qui lui avons envoyé de l'argent et pas un autre, et donc de créditer notre compte du montant correspondant.

Les public adresses permettent donc d'identifier expéditeurs et destinataires de coins, pour voir que ceux-ci se soient fait connaître (c'est-à-dire que l'utilisateur XYZ informe les personnes et sites pertinents que sa public adresse est xyzxyz).

3.2. La simplification et l'amélioration des paiements :

Nous l'avons vu les crypto-monnaies donnent aux monnaies une quatrième fonction,

⁷ La zone SEPA couvre actuellement 27 états membres de l'UE ainsi que la Suisse, le Liechtenstein, Monaco, Norvège et l'Islande. Un virement SEPA est un virement international dans la zone européenne : un transfert de fonds d'un compte vers le compte d'un bénéficiaire situé dans cette zone.

124 Enée Bussac, Op.cit. P185.

celle de vecteur d'information. C'est dans cette voie que ces monnaies peuvent simplifier et améliorer les paiements. Prenons un exemple : l'achat d'un paquet de cigarettes en France.

Aujourd'hui, le buraliste achète les paquets de cigarettes aux fabricants et les vend au détail. Quand il fait sa comptabilité, il réserve environ 80% de son chiffre d'affaires à l'Etat, qui va lui-même affecter ces revenus à trois recettes différentes : la TVA, l'accise proportionnelle et l'accise spécifique.

Demain, on pourrait imaginer le modèle suivant : le buraliste recevra les paquets des fabricants sans les payer mais en accusant leur réception. Quand le client paiera son paquet de cigarettes, il le fera avec sa solution de paiement, qui reversera directement la somme en cinq parties dont les proportions sont convenues à l'avance et dans le cas des cigarettes : une partie au fabricant dans une monnaie universelle ; par exemple LTC, une partie au buraliste, dans une monnaie universelle ou locale, la TVA en « TVA », l'accise proportionnelle en « ACCP » et l'accise spécifique en « ACCS » à l'Etat. La somme payée par le client sera ainsi instantanément reversée aux bonnes personnes dans les bonnes proportions et la bonne monnaie. C'est transparent pour le client car c'est sa solution de paiement qui gère les cinq monnaies. Le buraliste n'a plus à faire la comptabilité et l'Etat est payé immédiatement dans trois monnaies qui correspondent aux trois taxes qu'il prélève. Le prélèvement fiscal à la source peut dès lors se généraliser à la consommation.

Là encore les solutions de paiement vont jouer un rôle central : elles vont gérer des flux incessants de monnaies et permettre au système d'être fluide, efficace et économique, sans que cela ne devienne complexe pour les parties prenantes.

3.3. La traçabilité des paiements :

Revenons sur l'anonymat supposé que procurent les crypto-monnaies. Toutes les crypto-monnaies non anonymes mettent à disposition de tout un chacun un registre public en ligne affichant les transactions et les blocs minés de la blockchain en question et permettent d'effectuer des recherches afin de remonter dans le temps ou de connaître les actions liées à une certaine public adresse par exemple. Sont affichées pour une transaction donnée les public adresses d'émission et de réception, les montants échangés, les frais induits, etc. si nous nous intéressons à un bloc, nous pourrions connaître sa taille, le nombre de transactions contenues dans celui-ci, le nom du mineur, la date et l'heure de son ajout à la blockchain, etc.

Les transactions sont donc consultables publiquement, ce qui permet de savoir que telle somme de telle crypto-monnaie est passée de telle public adresse à telle public adressé à telle date et telle heure. Mais tout cela ne nous servira à rien si nous ne savons pas qui se cache derrière les publics adresses. Pour que ces paiements soient traçables et donc intéressants notamment pour l'administration fiscale mais aussi les banques ou entreprises, il faut pouvoir associer une public adresse à une personne physique ou morale. Sachant que les personnes échangent rarement des coins avec des personnes qu'ils connaissent mais utilisent presque toujours les services d'échange ainsi que les public adresses de leurs desktop et hardware wallets, ces personnes entrent en contact avec des entreprises qui pourraient leur demander de s'identifier pour utiliser leurs services et seraient donc à même d'associer leur identité ou celle de leur entreprise à un exchange wallet ou une public adresse et de livrer cette information aux autorités.

Il restera cependant toujours des crypto-monnaies anonymes. Mais les grands pays pourraient aller vers ce modèle de régulation et demander aux échanges de cesser de proposer des monnaies anonymes, comme l'a fait récemment le Japon.

SECTION 2 : RISQUES ET LIMITES DES CRYPTO-MONNAIES

La banque des règlements internationaux BRI, qui regroupe 60 Banques Centrales du monde entier, publie une étude approfondie du potentiel des crypto-monnaies. La BRI a à plusieurs reprises mis un garde sur les risques et les implications pour la stabilité financière et la politique monétaire de l'émission de monnaies digitales accessibles au grand public que pourraient décider certaines Banques Centrales.

*"Le modèle décentralisé des crypto-monnaies, pour générer de la confiance, limite leur potentiel de remplacer les monnaies conventionnelles."*⁸ Résumé Hyun Song Shin, le responsable de la recherche à la BRI.

1. Trois caractéristiques des crypto-monnaies qui sont sources de risques :

Une évaluation des risques liés aux crypto-monnaies doit notamment prendre en considération les modalités d'émission, les conditions d'utilisation et notamment la transparence des flux, la liquidité et la convertibilité en monnaie légale. Les crypto-monnaies sont de nature variée et reposent sur des modes de fonctionnement divers, mais

⁸ La tribune, publié sur (www.latribune.fr), le 18/06/2018, et consulté le 03/11/2019.

partagent néanmoins un certain nombre de traits commun susceptibles d'être sources de risques :

1.1. Intervention d'acteurs non régulés :

L'étude d'un panel de crypto-monnaies (monnaies virtuelles) montre que différents profils d'intervenants sont susceptibles d'être à l'origine de celles-ci. Il peut s'agir de personnes physiques ou de groupes de militants de sociétés commerciales. Dans certains cas, une monnaie virtuelle peut avoir été conçue afin de répondre aux besoins de personnes poursuivant des finalités illicites. L'émission de ces monnaies ne répond, en effet, à aucune qualification au regard de la réglementation bancaire et financière. En l'absence de statut légal et de cadre réglementaire, les crypto-monnaies n'offrent aucune garantie de prix ni de liquidité. Concernant les risques de volatilité et de liquidité, il convient de rappeler que la valeur des crypto-monnaies n'est pas garantie et résulte exclusivement de la confrontation de l'offre et de la demande. Pour cette monnaie, la limitation volontaire du nombre d'unités émises sans indexation de la valeur de celles-ci induit un risque de spéculation conduisant à une forte volatilité du cours⁹.

1.2. Manque de transparence :

A l'heure actuelle, l'ouverture d'un portefeuille de monnaie virtuelle ne nécessite, en général, aucune formalité particulière, notamment lorsque celle-ci est effectuée par le biais du téléchargement d'un logiciel. L'ouverture d'un compte en crypto-monnaie peut également être effectué par le biais d'un prestataire de service, auquel cas, certaines formalités de vérification d'identité peuvent être mises en œuvre, sans obligation légale, par ce prestataire. Un des principaux intérêts des monnaies virtuelles consiste dans le fait qu'elles permettent un anonymat total des transactions. Pour de nombreuses crypto-monnaies, si les identités des bénéficiaires et des donneurs d'ordre sont cryptées, en revanche, les transactions effectuées sont enregistrées dans un registre public assurant de fait leur traçabilité. Toutefois, il convient de souligner que cette traçabilité des flux en crypto-monnaies ne permet pas de répondre aux préoccupations en matière de connaissance du donneur d'ordre et du bénéficiaire effectif. En outre, d'une part, cette traçabilité n'est ni certaine ni systématique (certaines crypto-monnaies combinent anonymat et non-traçabilité, certains outils et applications permettent de combiner et mixer une transaction avec

⁹ Rapport annuel 2014 de Tracfin et un groupe de travail sur l'encadrement des monnaies virtuelles "Recommandations visant à prévenir leur usage à des fins frauduleuses ou de blanchiment", Juin 2014, consulté sur (www.economie.gouv.fr) le 05/11/2019.

d'autres...)- et d'autre part, l'exploitabilité, tant d'un point de vue technique que juridique, des transactions, lorsque traçables, n'est pas assurée.

1.3. Extraterritorialité :

L'utilisation des monnaies virtuelles permet, grâce aux facilités d'internet, de dématérialiser, d'antonyme et de démultiplier la portée de vecteurs classiques de blanchiment et de fraude. Les difficultés posées par ces monnaies tiennent tant au caractère insaisissable des acteurs qu'au contexte international (et plus encore extraterritorialité) des faits et des protagonistes, notamment quand les serveurs et les personnes physiques ou morales qui les exploitent sont installés dans des pays et territoires sur la coopération desquels il est difficile de compter.

2. Risques associés à trois usages des crypto-monnaies :

Plusieurs risques associés à trois usages des crypto-monnaies ont été distingués

2.1. Régler une transaction en crypto-monnaie :

Les crypto-monnaies peuvent être employées pour régler des transactions sur internet, mais également peuvent être dépensées dans l'économie réelle auprès de commerçants les acceptants. Les partisans des monnaies virtuelles mettent en avant le plus souvent la faiblesse des coûts de transactions, leur rapidité et leur irréversibilité, ainsi que la possibilité de se prémunir contre les vols de données personnelles. Micro-paiements, achats à l'étranger sans frais de change sont ainsi rendu possibles. Il convient de souligner que la question du coût de la méthode de paiement doit être considérée au regard du niveau de sécurité et de garantie offert.

❖ Exemples de risques associés à cet usage :

- Le remboursement d'une monnaie virtuelle n'est pas garanti et sa convertibilité dans une monnaie ayant cours légal non plus. Les risques liés à la volatilité des cours sont également importants ;
- Les monnaies virtuelles n'ayant pas cours légal, un règlement avec ces dernières n'a pas d'effet libératoire. Le consommateur doit être averti que payer en monnaie virtuelle sur des sites dont il n'est pas certain de la fiabilité représente un risque très élevé. Cela revient à donner des espèces à un inconnu dans la rue contre un produit

qu'il s'engage à vous ramener plus tard ;

- Il n'existe pas de dispositif de protection du consommateur adapté aux crypto-monnaies ;
- La sécurité opérationnelle de ces nouvelles méthodes de paiement n'est pas garantie.

2.2. Effectuer un transfert de fonds :

Les infrastructures techniques et fonctionnelles permettant la circulation des unités de monnaies virtuelles, non régulées, peuvent être utilisées pour effectuer des transferts de fonds à des coûts inférieurs à ceux du réseau bancaire ou des sociétés de transfert international de fonds. Une étude de Goldman Sachs¹⁰ estime qu'en l'état actuel, l'emploi du Bitcoin permettrait de diviser par 10 les coûts des transferts de fonds. Cette question du coût doit néanmoins être considérée au regard du niveau de sécurité offert. Enfin, reste à savoir si la régulation croissante des crypto-monnaies permettra de maintenir cet avantage-coût.

❖ Exemples de risques associés à cet usage :

- Le risque d'échange constitue un frein à la généralisation de cet usage ;
- La maîtrise des risques opérationnels de ces transferts n'est pas assurée.

2.3. Investir dans des supports d'investissement en lien avec les monnaies virtuelles :

Outre les opérations spéculatives d'achat-revente de crypto-monnaies réalisées par des particuliers, des initiatives ont vu le jour à l'étranger pour développer des produits d'investissement indexés sur le cours du Bitcoin. Il est ainsi possible de placer ses fonds dans des supports d'investissement en lien avec des monnaies virtuelles. Des fonds développent des stratégies d'investissement axées sur les crypto-monnaies et leur écosystème. Des fonds ou des produits financiers peuvent être exposés aux risques inhérents aux crypto-monnaies : des CFD (Contract For Difference)¹¹ sont déjà proposés au public.

Exemples de risques associés à cet usage :

- Les plateformes d'échange de crypto-monnaies présentent des incidences pour les utilisateurs qui tiennent entre autres, au manque de transparence dans l'exécution

¹⁰ Goldman Sachs, inscrite The Goldman Sachs Group Inc. est une banque d'investissement créée en 1869, dont le siège social mondial est situé à New York. Elle dispose de bureaux dans les plus importantes places financières dont New York, Londres, Tokyo et Paris.

¹¹ CFD : (contrat sur la différence en français), sur les marchés financiers, c'est un contrat entre un client et son courtier où l'une des parties est acheteuse et l'autre vendeuse, stipulant que l'acheteur encaissera ou décaissera la différence entre le prix de l'actif au moment de sa vente et son prix au moment de l'exécution du contrat. Si la différence est négative, alors le vendeur qui encaisse cette différence.

des ordres, à l'opacité dans la formation des prix (asymétrie d'information) et au risque de manipulations de marché. Il n'y a pas de compensation pour ces transactions de gré à gré et anonymes sur internet, et le marché manque de profondeur ;

- Il existe un risque d'arbitrage réglementaire, certains acteurs pouvant localiser leurs activités dans des centres financiers *offshores* moins-disant.

3. Risques d'utilisation des crypto-monnaies à des fins illicites :

Du fait de leurs caractéristiques (extraterritorialité et absence d'organe de régulation notamment) et de leur mode de fonctionnement, les monnaies virtuelles présentent des risques intrinsèques et sont de nature à permettre le financement d'activités criminelles et à faciliter le blanchiment de celles-ci.

3.1. Crypto-monnaies (crypto-actifs) vecteur de risque de blanchiment d'argent et de financement du terrorisme :

L'anonymat qui caractérise les mécanismes d'émission et de transfert de la plupart des crypto-monnaies favorise avant tout un risque d'utilisation de ces monnaies à des fins criminelles (vente sur internet de biens ou services illicites). Ces crypto-monnaies favorisent également le financement du terrorisme ainsi que le contournement des règles relatives à la lutte contre le blanchiment des capitaux.

En France, par exemple, l'organisme Trac fin identifie l'utilisation des crypto-actifs, notamment le Bitcoin, comme étant à l'origine d'un risque spécifique en matière de blanchiment des capitaux et de financement du terrorisme¹².

3.2. Crypto-monnaies vecteur de risque de cyber-attaques :

La conservation des crypto-monnaies est sujette à des cyber-risques importants. Il existe des risques avérés de piratage des portefeuilles électroniques qui permettent le stockage des crypto-actifs. Dans ce contexte, les détenteurs n'ont aucun recours en cas de vol de leurs avoirs par des pirates informatiques.

Les épisodes répétés de fraudes importantes (piratage de Coincheck en janvier 2018 pour 534 millions de dollars américains, faillite retentissante en 2015 de la première

¹² Banque de France, Focus, "L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives" N°16 du 05 mars 2018, consulté sur (<http://publication.banque-france.fr>) le 05/11/2019.

plateforme mondiale d'échange de bitcoin, MtGox¹³), illustrent la vulnérabilité de l'écosystème des crypto-monnaies et le niveau élevé des risques associés, en l'absence de mécanismes de garantie.

4. Autres menaces qui pèsent sur les crypto-monnaies :

Plusieurs autres menaces pèsent sur le marché des crypto-monnaies outre celles évoquées précédemment :

4.1. La faible utilisation dans le monde réel :

Les gens reprochent parfois aux crypto-monnaies de n'avoir pas, ou trop peu, d'applications dans le monde réel, même le bitcoin. Un indicateur permet d'appuyer cette constatation : le nombre de transactions journalières.

Le nombre de transactions journalières en bitcoin est estimé à environ 200 000/jour (essentiellement dans le cadre d'une activité de spéculation) en 2018 contre plus de 500 000/jour en 2017. Donc il y a moins de transactions qui sont effectuées aujourd'hui avec le bitcoin qu'il y a un an¹⁴.

Mais pourquoi voudrait-on utiliser aujourd'hui même le bitcoin dans le monde réel ? Son cours varie constamment et elle n'est légale dans aucun pays, donc les commerçants n'ont pas vraiment de raisons d'accepter le bitcoin, même si beaucoup le font déjà au Japon et en Corée du Sud. Quant aux consommateurs, pourquoi se sépareraient-ils de leurs bitcoins s'ils pensent que leur cours va augmenter dans les mois qui viennent ?

4.2. Le manque de sécurité pour les utilisateurs :

Le manque de sécurité est une des menaces majeures des crypto-monnaies qui concerne surtout les investisseurs individuels et qui est étroitement liée à l'absence de vraie réglementation et de centralisation du marché. La sécurité liée à la gestion de notre clé privée et de celles de nos investissements. Le système de création de comptes (clé privée) est fait de telle manière que rien ni personne ne peut nous rendre nos coins si nous perdons la clé privée qui y est associée, et qu'une autre personne peut nous voler nos coins si elle met la main sur celle-ci ou a accès à notre wallet à notre place, en nous volant nos codes d'accès. Le cas d'un investisseur particulier autrichien, qui a perdu autour de 100 000\$ fin 2017 car il a utilisé un

¹³ A la suite d'une fraude interne ayant entraîné le détournement de 650 000 bitcoins pour une valeur d'environ 360 millions de dollars américains.

¹⁴ Enée Bussac, Op.cit, P144.P145.

wifi public pour accéder à son wallet et s'est fait ainsi pirater ses codes d'accès, est assez éloquent.

4.3. La mauvaise réputation :

Les crypto-monnaies, surtout tant qu'elles ne sont pas régulées, font peser une menace de taille sur les investisseurs particuliers, car la majorité des PIHR¹⁵ et beaucoup d'ICO sont des arnaques. Cela contribue à la réputation de monnaie de vendeur d'armes et de drogue qu'elles ont les crypto-monnaies, comme ce fut le cas pour internet dans la première moitié des années 1990.

Il est, en outre, tellement facile de créer une crypto-monnaie qu'on en arrive à des cas de figure qui contribuent à décrédibiliser les crypto-monnaies. Voici un exemple :

Fin 2013, un jeune australien, Jackson Parker, décide qu'il veut lui aussi participer à ce nouveau marché des crypto-monnaies et décide de créer la sienne pour rire. Il utilise le logo d'un chien qu'il a trouvé sur internet et nomme son coin (logiquement) Dogecoin. Mais tout le monde l'a pris au sérieux, et le cours de son coin, dont le projet est d'être la monnaie des achats sur internet, a explosé en décembre 2017, dépassant le milliard de dollars de capitalisation boursière et se plaçant parmi les 50 premiers coins du marché.

4.4. Les arnaques :

Entre les PIHR, certaines ICO et l'absence de vrai projet derrière certaines crypto-monnaies, investir dans ce marché est un grand risque.

Pour certains, les crypto-monnaies sont même l'arnaque du siècle, et la volatilité du cours même des monnaies les plus établies est assez spectaculaire. Le fait qu'il soit si facile de créer une nouvelle monnaie et de lancer une ICO ou "une plateforme d'investissement" pour récolter quelques milliers d'ETH, ou de BTC ou autres, pose, en effet, problème. L'investissement en temps et énergie et le risque pris sont suffisamment faibles pour que cela vaille la peine.

4.5. La menace pour l'environnement :

La consommation phénoménale d'énergie requise pour faire tourner les ordinateurs

¹⁵ Une PIHR (HYIP en anglais : High Yield Investment Platform ou Program) est une plateforme d'investissement à haut rendement. Le principe des PIHR est simple : vous leur confiez vos bitcoins et autres crypto-monnaies, elles font fructifier votre investissement et vous reversent, suivant la plateforme, un certain rendement toutes les heures, tous les jours ou toutes les semaines.

qui minent le bitcoin et d'autres représente un vrai problème qui prend des proportions inquiétantes à mesure que le mining pools¹⁶ investissent à coups de millions dans du matériel informatique et dans des fermes dans des régions froides. Tout ça pour faire tourner une fonction de hachage des milliards de fois par seconde pour obtenir une empreinte qui commence par le bon nombre de zéro.

Pour la validation d'une seule opération en bitcoin, la consommation d'électricité était estimée en décembre 2017 à 215kwh, l'équivalent de six mois de travail sur un ordinateur ordinaire allumé jour et nuit. Ou encore selon des estimations, la consommation électrique mondiale entraînée par le minage serait de 71,1 TWh/an (1 térawatt-heure (TWh) = 1 milliard de kilowatts-heures (kWh)) au 1^{er} juillet 2018, soit l'énergie produite pendant un an par 6 réacteurs nucléaires de 1 300 MW fonctionnant à plein régime ou la consommation électrique annuelle du Chili ou 0,32 % de la consommation électrique mondiale¹⁷.

Cette consommation énergétique fait l'objet d'une réévaluation constante, à la hausse, en raison de la concurrence accrue associée à l'élargissement du réseau de validation des opérations.

Il est important de comprendre que seules les monnaies fonctionnant sous l'algorithme Pow comme le bitcoin sont concernées par ce problème. Les autres algorithmes de consensus comme Pos n'occasionnent pratiquement pas de dépenses d'énergie.

SECTION3 : LES PERSPECTIVES, RECOMMANDATIONS ET RÉGULATION

Les crypto-monnaies présentent des risques liés tant à leur caractéristiques qu'à leur multifonctionnalités. L'essor de nouvelles activités en lien avec les monnaies virtuelles pose la question de l'adaptation et l'évolution du cadre législatif et réglementaire. Alors quelle réglementation des crypto-monnaies pour maîtriser les risques identifiés ?

Pour les régulateurs et superviseurs du système financier européen et internationaux, une réglementation des activités liées aux crypto-monnaies est souhaitable pour quatre motifs : la lutte contre le blanchiment des capitaux et le financement du terrorisme- qui

¹⁶ Les mining pools ou un pool de mineurs est un groupe d'individus qui minent du bitcoin ou d'autres crypto-monnaies. La plupart des mineurs s'organisent en pool, afin d'être plus efficace et d'avoir plus de chance de toucher la récompense attribuée à ceux qui trouveront la solution de l'énigme informatique.

¹⁷ WIKIPEDIA. Consulté sur (fr.wikipedia.org) le 15/11/2019.

apparaît hautement prioritaire-, la protection des investisseurs, la préservation de l'intégrité des marchés, y compris face au cyber-risque, et enfin, en cas de poursuite de l'essor de ces activités, les préoccupations de stabilité financière. Ainsi, les institutions de régulation¹⁴⁷ proposent une stratégie possible qui repose sur trois volets complémentaires :

- ✓ Un volet « Régulation et coopération" ;
- ✓ Un volet « Encadrement de l'utilisation" ;
- ✓ Un volet « Connaissance et investigation".

1. Les points clés du volet "Régulation et coopération" :

Des propositions sont formulées afin d'adapter le dispositif de lutte contre le blanchiment et le financement du terrorisme aux risques posés par les monnaies virtuelles et l'essor de nouvelles activités en lien avec ces dernières. A cet effet, les recommandations suivantes ont été formulées :

1.1. Réglementer les services offerts à l'interface entre la sphère réelle et les crypto-monnaies :

La Banque de France et l'Autorité de Contrôle Prudentiel et de Résolution (ACPR)¹⁸ préconisent un élargissement de l'encadrement des prestations de services associés aux crypto-monnaies de manière à couvrir deux champs, l'un d'eux est celui de réglementer les services offerts à l'interface entre la sphère réelle et les crypto-monnaies.

L'activité des plateformes de conversion des crypto-monnaies ayant cours légale, qui jouent le rôle d'intermédiaire entre acheteur et vendeur, est considérée comme un service de paiement. Toutefois, cette exigence découle de la gestion pour le compte de tiers de comptes tenus et libellés dans une monnaie ayant cours légal, et pas de prestations associées aux crypto-monnaies.

Au-delà de cette approche, la Banque de France et l'ACPR préconisent un élargissement de l'encadrement réglementaire applicable aux prestations associées aux crypto-monnaies par la mise en place d'un statut de prestataires de services en crypto-monnaies.

Cette évolution réglementaire pourrait s'inscrire dans le prolongement de la révision

¹⁸ ACPR est une institution intégrée à la Banque de France, chargée de la surveillance de l'activité des banques et des assurances en France. Donc un organe de supervision.

de la IV^e directive de lutte contre le blanchiment des capitaux et le financement du terrorisme en cours d'adoption par l'UE (dite "V^e" directive LCB-FT)¹⁹. Cette directive prévoit, en effet, d'assujettir à cette réglementation les acteurs proposant des services d'échange de crypto-monnaies contre de la monnaie ayant cours légal, et la conservation pour le compte de leurs clients des clés cryptographiques privées permettant de détenir, stocker ou transférer les crypto-monnaies.

Un statut de prestataire de service en crypto-monnaies permettrait, au-delà de la lutte contre le blanchiment de capitaux et le financement du terrorisme qui constitue une priorité, de les soumettre à des règles portant notamment sur la sécurité des opérations et sur la protection de la clientèle. Ce statut pourrait également couvrir les services concernant les transactions entre crypto-monnaies.

1.2. Encadrer les placements en crypto-monnaies :

Encadrer les placements en crypto-monnaies est le deuxième champ visé par l'élargissement de l'encadrement des prestations de service associées aux crypto-monnaies proposé par la Banque de France et ACPR.

En effet, l'encadrement réglementaire des prestataires de service en crypto-monnaies pourrait être complété d'une limitation de la possibilité pour certaines entreprises régulées (banques, assurances, sociétés de gestion, etc.) d'intervenir sur ces crypto-actifs. Il s'agit d'abord d'interdire les activités de dépôts et prêts en crypto-monnaies. Ces produits devraient par ailleurs être assujettis à des règles strictes de protection de la clientèle. Enfin, pour les placements pour compte propre des entités régulées, un strict encadrement de ces placements, par exemple, en déduisant la totalité de ces investissements des fonds propres, devrait être envisagé. Ces dispositions supposent une évolution des textes législatifs nationaux ou européens et même internationaux.

Pour sa part, l'AMF considère que l'offre de dérivés sur crypto-monnaies nécessite un agrément et ne doit pas faire l'objet de publicité par voie électronique. Par ailleurs, dans le prolongement de sa consultation publique sur les ICO, l'AMF a décidé de poursuivre le travail relatif à la définition d'un cadre juridique spécifique aux ICO prévoyant les garanties appropriées, notamment en matière d'information, qui seront nécessaires pour ce

¹⁹ Directive LCB-FT (Lutte Contre le Blanchiment et Financement du Terrorisme) est une directive du parlement européen relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou de financement du terrorisme.

nouveau type d'offre. Ce travail sera mené en coordination avec les autres autorités publiques concernées²⁰.

1.3. Une coordination européenne et internationale :

Afin d'assurer une meilleure efficacité de la réglementation, la Banque de France et l'ACPR pensent qu'il est souhaitable de développer une coordination européenne et internationale. Compte tenu du caractère dématérialisé des crypto-monnaies et de l'utilisation de technologies liées au monde de l'internet qui facilitent la fourniture de service de façon transfrontalière, l'hétérogénéité des règlements nationaux pourrait empêcher une pleine maîtrise des risques induits.

Ainsi, pour ces institutions, il est nécessaire aujourd'hui de porter un débat sur la régulation des crypto-monnaies au niveau international. Le 07 février 2018, les ministres de l'Economie et des finances et le banquier français et allemands ont saisi le G20 à cet effet. Aussi :

- Harmoniser la régulation des échanges virtuels aux niveaux communautaire et international et éviter le contournement de la loi par des échangeurs virtuels situés à l'étranger et s'adressant à une clientèle nationale, permet, entre autre, une levée de l'anonymat avant conversion des fonds en monnaie légale.
- Demander l'application par les professionnels assujettis aux dispositions de lutte contre le blanchiment des capitaux et le financement du terrorisme, de mesures de vigilance renforcée concernant les flux en lien avec des personnes utilisant les crypto-monnaies.

2. Les points clés du volet "Encadrement de l'utilisation" :

Concernant l'encadrement de l'utilisation des crypto-monnaies, sans préjudice des conclusions des débats et réflexion, au niveau national ou supranational, sur la qualification juridique des monnaies virtuelles, des propositions ont été formulées afin de limiter :

2.1. L'anonymat des utilisateurs de monnaies virtuelles :

Notamment en instaurant d'une part une obligation de prise d'identité lors de l'ouverture d'un compte en crypto-monnaies et d'autre part une obligation de déclaration des comptes en cette monnaie et en disposant d'outils permettant la connaissance et le suivi de

²⁰ Banque de France, Focus, Op.cit.

ces comptes, au moins au-delà d'un certain montant.

2.2. Les possibilités d'utilisation de la crypto-monnaie en tant que méthode de paiement anonyme :

Notamment en plafonnant strictement les montants susceptibles d'être réglés par ce biais.

2.3. Les flux espèces/crypto-monnaies :

Notamment dans le cadre de l'utilisation de bornes d'échanges de bitcoins ou de distributeurs de bitcoins, en définissant des plafonds de montant et en assortissant ces opérations d'un contrôle d'identité par une méthode fiable.

3. Les points clés du volet "Encadrement de l'utilisation" :

Compte tenu du dynamisme du secteur des crypto-monnaies, de l'évolution extrêmement rapide des technologies et de la nécessité de renforcer la coopération internationale, des propositions sont également formulées afin d'assurer un suivi des risques et des opportunités en lien avec les crypto-monnaies :

- Adapter le cadre légal et les méthodes d'investigation ;
- Améliorer la connaissance du secteur et le suivi des risques.

Tableau 2.1 : Une synthèse des trois piliers de la stratégie de lutte, proposée, contre les risques des crypto-monnaie

Volet regulation et coopération	Volet Encadrement de l'utilisation	Volet Connaissance & Investigation
• Réglementer les services offerts à l'interface entre la sphère réelle et les crypto- monnaies ; • En cadrer les placements ; • Adapter le dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme aux risques posées par les crypto-monnaies et les activités les utilisant ; • Harmoniser la réglementation au niveau national et international.	• Limiter et plafonner l'utilisation des crypto- monnaies en tant que méthode de paiement ; • Limiter et contrôler les flux espèces/crypto-monnaies ; • Limiter l'anonymat des utilisateurs de crypto-monnaies.	• Disposer de ressources et d'outils d'analyse adaptés ; • Effectuer un suivi des risques et des opportunités, notamment par des échanges avec les professionnels du secteur.

Source : Rapport annuel 2014 de Tracfin (www.economie.gouv.fr)

Conclusion :

Toutes les grandes innovations technologiques, celles qui sont capables de faire bouger de manière importante la frontière de ce que nous croyons possible, comportent un côté d'ombre ainsi qu'un autre de lumière. Elles peuvent servir à améliorer les conditions de vie des hommes de la même façon qu'elles peuvent être utilisées pour les asservir. Les responsables politiques et autorités doivent donc procéder avec beaucoup de prudence, puisque il leur est confié la délicate mission de trouver l'équilibre entre la nécessité d'éviter une trop importante déstabilisation de l'ordre, et celle de permettre aux forces de changement desquelles est faite l'histoire, de se manifester.

Dans le cas des crypto-monnaies, il n'est pas différent. Certains pays demandent leur interdiction, d'autres l'exhortent. Cette cacophonie de positions résulte de regards concentrés tantôt sur les aspects négatifs et tantôt sur les aspects positifs que ces monnaies contiennent.

Les risques présentés par ce nouvel instrument d'échange sont réels et important, et concernent à la fois ses utilisateurs directs comme les personnes n'ayant jamais entendu parler des crypto-monnaies, en ce qu'elles ont le potentiel de bouleverser des structures économiques, politiques et sociales, dans lesquelles nous sommes insérés. Cela justifie une approche prudente qui tienne en compte les usages peu souhaitables et les façons de les éviter.

Une ambivalence des crypto-monnaies fait que celles-ci nécessitent une régulation équilibrée qui soit capable à la fois de protéger les utilisateurs, d'assurer le respect de leur vie privée et permettre à l'Etat de les protéger des menaces à la stabilité macro-économique et à la légalité.

Lorsque surgiront des régulations plus complexes, soient-elles au niveau domestique ou au niveau international, celles-ci devraient se nourrir des débats qui tiennent compte des deux côtés de cette technologie. Les nombreux effets positifs doivent être pris en compte, et pas seulement l'alarmisme résultant des risques identifiés, bien que ces risques soient réels.

CHAPITRE 3

BITCOIN et Crypto-Monnaie :
Expériences mondiales et
perspective

Introduction :

Il y a quelques années, la plupart des articles de presse (ou site internet) consacrés à Bitcoin étaient essentiellement négatif. On évoquait un dispositif obscur, au mieux sans grand intérêt ; au pire potentiellement dangereux. Beaucoup estimaient que Bitcoin était seulement une "arnaque" évoquant "les systèmes pyramidaux" appelé aussi "système de Ponzi"²¹, des mécanismes financiers frauduleux. D'autres soulignaient "*qu'on ne peut rien acheter en bitcoin*" et qu'il s'agit davantage d'un "amusement pour informatique" que d'une véritable monnaie²².

Au fil du temps, un changement presque palpable s'est opéré. Au fur et à mesure que la popularité de Bitcoin grandissait, beaucoup se sont intéressés de plus près au fonctionnement et à la philosophie de Bitcoin, y découvrant des principes novateurs et un potentiel bien réel. De nombreuses entreprises spécialisées, proposant de nouveaux produits et services autour de Bitcoin sont apparues, partout dans le monde, participant à une forme "de mission" pour faire comprendre l'intérêt de la puissance de la crypto-monnaie.

Gouvernements et banques centrales ont d'ailleurs dû prendre position et les déclarations officielles, même si elles demeurent souvent mitigées, attestent d'une prise de conscience quant à l'importance prise par Bitcoin et sa réalité.

Bitcoin est une réalité, Bitcoin fonctionne et il est en train de prendre une ampleur considérable.

L'essentiel de la littérature consacrée aux crypto-monnaies se concentre sur Bitcoin. Non seulement parce que Bitcoin est la plus ancienne, la plus importante (en capitalisation) et la plus répandue des monnaies virtuelles. Mais aussi ce à quoi elle a donné naissance. L'intérêt du Bitcoin ne réside pas uniquement dans la monnaie qu'il représente.

La révolution qui se produit actuellement est la libéralisation et la démocratisation du concept de monnaie. Bitcoin est, pour l'instant, la partie la plus visible de cette révolution.

²¹ Un système de Ponzi est un montage financier frauduleux qui consiste à rémunérer les investissements des clients essentiellement par les fonds procurés par les nouveaux entrants. Ce type d'escroquerie financière prend aussi le nom de "vente pyramidale" car il ne peut fonctionner que si le nombre d'entrants est en augmentation. Pratiqué pour la 1ère fois par un Italo-américain qui s'appelait Charles Ponzi.

²² Cyril fièvet, " Comprendre Bitcoin et les crypto-monnaies alternatives." Edition Lbrinova, 2014, P3.

L'objectif central de ce chapitre consiste à poser les jalons théoriques d'une évaluation du Bitcoin comme projet monétaire. Le cadre d'analyse que nous privilégions est celui de la monnaie en tant que système de paiement par lequel le Bitcoin institue une unité de compte et des règles d'organisation des transactions, de sorte qu'il obéit à des logiques qui lui sont propres.

Dans un premier temps, nous parlerons de l'apparition du Bitcoin, son historique, sa création et ses principes de fonctionnement (section1). Ensuite, nous discuterons de son évolution et de ses différentes caractéristiques en testant la capacité du Bitcoin à opérer comme monnaie (section2). Et enfin, en faisant le point sur ses apports ainsi que les vrais enjeux et les faux problèmes qu'il soulève, nous analyserons les différentes positions.

SECTION1 : BITCOIN, Première CRYPTO-Monnaie

Bitcoin est la plus importante des crypto-monnaies, c'est également la devise numérique la plus utilisée par les investisseurs. En effet, la première crypto-monnaie qui fonctionne dans le système de blockchain. Inconnu du public jusqu'à récemment, le Bitcoin suscite depuis quelques années un engouement médiatique sans précédent ainsi qu'un intérêt croissant. Bitcoin est la crypto-monnaie la plus valorisée au monde, ses caractéristiques séduisent de plus en plus les professionnels, fonds d'investissement comme établissements financiers. En décembre 2017, le Bitcoin avait presque atteint les 20 000 dollars, une hausse spectaculaire qui a fait le bonheur des investisseurs. Après trois ans de hauts et des bas, Bitcoin s'est finalement stabilisé en 2019 et se maintient actuellement à environs 11 700 dollars²³. Alors d'où vient cette monnaie ? Et comment fonctionne-t-elle ?

1. Définition de BITCOIN :

1.1. Présentation :

Le terme Bitcoin est composé d'une contraction de l'unité d'information binaire (Bit) et du mot coin (pièce de monnaie). Le Bitcoin est à la fois un concept, un logiciel, un protocole mais aussi une monnaie électronique (virtuelle, digitale, numérique,...). Le bitcoin, avec une minuscule, désigne l'unité de compte mais aussi la monnaie au sens de devise, à la différence de Bitcoin, avec majuscule, qui désigne le protocole ou encore le système de paiement.

²³ Top des crypto-monnaies prometteuses en 2020 consulté sur (alti-trading.fr) le 10/11/2019.

L'idée fut présentée pour la première fois en novembre 2008 par une personne, ou groupe de personnes, sous le pseudonyme de Satoshi Nakamoto²⁴. Le code de l'implémentation de référence fut quant à lui publié en 2009.

Les symboles utilisés pour représenter Bitcoin sont : BTC, XBT, ₿ ou B ou encore ₿.

L'unité de compte qu'est bitcoin est définie au sein même du protocole Bitcoin de manière extrêmement précise. La plus petite unité de bitcoin est communément nommée le Satoshi en hommage à son créateur et elle égale à 0,00000001BTC (1BTC=1/100000000satoshi).

Le bitcoin peut également être subdivisé en millibitcoin (mXBT, 1mXBT=0,001XBT), microbitcoin (μXBT, parfois dénommé bit) ou nanobitcoin (nBXT).

Il faut savoir que la divisibilité est aussi régie par le protocole qui sera potentiellement mis à jour s'il advient que la valeur du bitcoin soit trop élevée et nécessite une plus grande division. Il sera toujours possible de diviser davantage bitcoin sans pouvoir pour autant avoir à modifier sa rareté et le rythme de sa création monétaire.

Le Bitcoin est une monnaie électronique, décentralisée basée sur un système "P2P" et dont les unités sont créées à partir d'un algorithme mathématique.

Les utilisateurs peuvent échanger des bitcoins dans le monde entier via le réseau internet sans passer par un tiers de confiance. Pour certains il constitue un moyen de paiement et pour d'autres, un produit de spéculation.

1.2. Historique :

Comme nous l'avons souligné précédemment, Bitcoin est une amélioration du concept b-money, imaginé par Wei Dai en 1994, et de bit gold, décrit en 2005 par Nick Szabo.

Satoshi Nakamoto a affirmé qu'il avait travaillé sur Bitcoin de 2007 à 2009. Dès 2008, il publie un document sur une liste de diffusion décrivant la monnaie numérique Bitcoin. En février 2009, il diffuse une annonce concernant son travail sur le site P2P Foundation. Le 03 janvier 2009, le premier bloc ou *bloc genesis* est créé. En février 2009,

²⁴ Pour certains, Nakamoto, serait le groupement de Samsung, Toshiba, Nakamichi et Motorola, tandis que pour d'autres se serait un mathématicien surdoué ou encore un économiste finlandais.

il diffuse la première version du logiciel Bitcoin sur le site P2P Foundation et pour faire fonctionner le réseau, il met à contribution son ordinateur et engendre ainsi les premiers bitcoins. Avec d'autres développeurs, Nakamoto continue l'implémentation du logiciel et de sa version Bitcoin-Qt jusqu'en 2010²⁵.

Les développeurs et la communauté bitcoin perdent progressivement contact avec Nakamoto au milieu de l'année 2010. Le 12 décembre 2010, un dernier message est posté par lui sur le principal forum. Peu de temps avant de disparaître, Nakamoto désigne Gavin Andresen comme son successeur en lui donnant accès au projet Sourceforge bitcoin et une copie de la clé d'alerte.

Le 27 décembre 2012, la fondation Bitcoin est créée.

Tableau 3.1 : Dates qui ont marqué l'histoire du Bitcoin

Date	Evénement
09/08/ 2008	Satoshi Nakamoto réserve le nom de domaine bitcoin.org.
03/01/2009	Création du 1 ^{er} bloc de transaction de blockchain bitcoin.
12/01/2009	1 ^{ère} transaction bitcoins entre Satoshi Nakamoto et Hal Finney, son montant était de 10 BTC.
21/05/2010	Un programmeur, Laszlo Hanyecz achète deux pizzas pour 10 000 bitcoins.
17/07/2010	Création d'une plateforme d'échange de cartes à collectionner, nommée MtGox qui deviendra ensuite la plus grande place d'échange de bitcoins.
15/06/2011	Pour contourner les sanctions américaines, Wikileaks décide d'accepter les dons en bitcoins.
Juin 2011	La plateforme MtGox est hackée.
27/12/2012	La fondation Bitcoin est créée afin de standardiser, protéger et promouvoir le bitcoin.
10/12/2013	Apple interdit l'utilisation de bitcoins via ses applications.
25/02/2014	Fermeture de MtGox.
18/07/2014	Dell devient la plus grande entreprise du monde qui adopte bitcoin.

²⁵ WIKIPEDIA, Op.cit.

19/05/2015	Le New York Stock Exchange intègre le cours du bitcoin sous l'indice NYXBT.
01/08/2015	Arrestation de Mark Karpeles ex-PDG de MtGox.
22/10/2015	La cour de justice de l'UE se prononce en faveur d'une exonération de la TVA sur les échanges euros/bitcoins.
01/01/2017	Le cours du bitcoin atteint pour la 1 ^{ère} fois les 1000 dollars.
01/04/2017	Le Japon reconnaît le bitcoin et les monnaies virtuelles comme des moyens de paiement légaux.
01/08/2017	Un fork de bitcoin donne naissance au bitcoin cash (BCH).
31/10/2017	CME groupe, bourse d'échange de marché à terme, annonce son intention de lancer des contrats à terme en bitcoins.
19/04/2018	Le parlement européen vote une directive pour encadrer plus strictement l'activité des plateformes d'échange de crypto-monnaies.
03/08/2018	La maison mère NYSE, Intercontinental Exchange, annonce la création d'une plateforme d'échange de bitcoins.
15/03/2019	Mark Karpeles, ex-PDG de MtGox, est condamné par le tribunal de Tokyo à 02 ans de prison avec sursis.
19/06/2019	Publication du livre blanc de libra, la monnaie numérique de facebook.
23/09/2019	Lancement de Bakkt, la plateforme de futures bitcoins (gérée par la maison-mère de New York Stock Exchange).
01/10/2019	Une commission d'enquête sénatoriale rend un rapport sur la souveraineté numérique. Elle y aborde la question des "crypto-actifs" et plaide en faveur du déploiement d'une crypto-monnaie banque centrale.

Sources : JDN (journaldunet.fr) et Bitcoin (bitcoin.fr)

1.3. Acceptation du Bitcoin dans le monde :

- Le 16 novembre 2012, Word Press accepte les bitcoins pour ses services payants²⁶.
- Le 14 février 2013, le site communautaire Reddit met en place un système permettant d'acheter des "Reddit Gold" avec des bitcoins.

²⁶ WIKIPEDIA, Op.cit.

- Le 16 février 2013, le site de stockage en ligne Mega²⁷, successeur de Megaupload, accepte les paiements en bitcoins.
- Le 14 octobre 2013, le géant Baidu (équivalent chinois de Google) accepte les transactions en bitcoins pour son service pare-feu Jiasule.
- Le 29 octobre 2013, le premier distributeur-échangeur automatique de bitcoins est mis en service à Vancouver (Canada). En septembre 2016, plus de 770 de ces distributeurs- échangeurs automatiques sont installés dans le monde, dont quatre en France.
- Le nombre de bitcoin ATMs a augmenté de 500% depuis 2016. Il y a 5 457 bitcoin ATMs dans le monde au 1^{er} septembre 2019.
- Le 21 novembre 2013, l'université de Nicosie (plus grande université privée de Chypre, créée en 1980) annonce qu'elle accepte le bitcoin et ouvre un master de Sciences Economiques spécialisée dans les monnaies numériques.
- Le 22 novembre 2013, Richard Branson annonce que Virgin Galactic acceptera désormais les bitcoins comme moyen de paiement pour ses vols de tourisme spatial.
- Le 29 novembre, Jiangsu Telecom (troisième plus grand opérateur chinois) filiale de China Telecom, accepte désormais les bitcoins.
- Le 25 mars 2014, le fisc américain déclare que le bitcoin ne doit pas être considéré comme une monnaie, mais comme un bien, dont les transactions sont soumises à la fiscalité sur les plus-values. Cela implique de tenir compte du taux de change auquel on a acquis un bitcoin et de celui auquel on l'utilise afin de calculer la plus-value réalisée, ce qui rend l'utilisation légale du bitcoin aux Etats-Unis partiellement difficile.
- Le 09 mai 2014, la commission électorale des Etats-Unis accepte que les campagnes électorales soient financées en bitcoins dans une limite de 100 USD par cycle électoral.
- Le 23 septembre 2014, PayPal permet à certains marchands de biens numériques d'Amérique du Nord sélectionnés par les processeurs de paiement bitcoin partenaires, d'accepter les paiements en bitcoins, et s'ouvre ainsi très

²⁷ Mega est le site web remplaçant le site d'hébergement de fichiers Megaupload, fermé par le FBI le 19 janvier 2012. Son lancement s'est fait le 19 janvier 2013, soit un an exactement après la fermeture du précédent service.

progressivement au Bitcoin.

- En décembre 2017, le ministre français des Comptes publics, Gérard Darmanin, rappelle aux contribuables français l'exigence de la déclaration de revenus, quand il s'agit de plus-values réalisées lors d'opérations en bitcoins.
- En novembre 2018, le gouvernement de l'Ohio a annoncé accepter les paiements de taxes en bitcoins.

1.4. Racines théorique de Bitcoin :

Les racines théoriques de Bitcoin se trouvent dans l'école autrichienne d'économie et dans sa critique du système monétaire actuel et des interventions des gouvernements et d'autres organismes, qui, selon cette école exacerbe les cycles économiques et l'inflation massive.

Un des sujets sur lequel l'école autrichienne d'économie, dirigée par Eugen Von Böhm-Bawerk, Ludwig Von Mises et Friedrich A. Hayek, s'est concentrée est le cycle économique : selon la théorie autrichienne, les cycles économiques sont la conséquence des interventions monétaires sur le marché, par lesquelles une expansion excessive du crédit entraîne une augmentation de l'encours du crédit bancaire dans un système de réserve fractionnaire, ce qui entraîne à son tour des taux d'intérêt artificiellement bas.

Dans cette situation, les entrepreneurs, guidés par des signaux de taux d'intérêt déformés, se lancent dans des projets d'investissement trop ambitieux qui ne correspondent pas aux références des consommateurs à ce moment-là en matière de consommation intertemporelle (c'est-à-dire leurs décisions à court terme et consommation future). Tôt ou tard ce déséquilibre généralisé ne peut plus perdurer et conduit à une récession, au cours de laquelle les entreprises doivent liquider les projets d'investissement qui échouent et réadapter (restructurer) leurs structures de production en fonction des préférences intertemporelles des consommateurs, en conséquence, de nombreux économistes des écoles autrichiennes réclament l'abandon de ce processus en abolissant le système bancaire de la réserve fractionnaire et en retournant à une monnaie basée sur l'étalon-or, qui ne peut pas être facilement manipulée par n'importe quelle autorité.

Un domaine connexe dans lequel les économistes autrichiens ont été très actifs est la théorie monétaire. Friedrich A. Hayek est l'un des noms les plus connus dans ce domaine. Il a écrit quelques publications très influentes, comme *Dénationalisation de la*

monnaie(1976), dans lequel il postule que les gouvernements ne devraient pas avoir un monopole sur l'émission de l'argent. Il suggère plutôt que les banques privées soient autorisées à émettre des certificats non productifs d'intérêts, sur la base de leurs propres marques déposées. Ces certificats (c'est-à-dire les devises) devraient être ouverts à la concurrence et seraient négociés à des taux de change variables. Toutes devises pouvant garantir un pouvoir d'achat stable éliminerait du marché d'autres devises moins stables. Le résultat de ce processus de concurrence et de maximisation des profits serait un système monétaire hautement efficace dans lequel seules des monnaies stables coexisteraient.

Les idées suivantes sont généralement partagées par les partisans Bitcoin :

- Ils considèrent Bitcoin comme un bon point de départ pour mettre fin au monopole des banques dans l'émission de monnaie ;
- Ils critiquent vivement le système bancaire actuel des réserves fractionnaires, qui permet aux banques d'étendre leur offre de crédit au-delà de leurs réserves réelles et, en même temps, aux déposants de retirer leurs fonds sur leurs comptes courants à tout moment ;
- Le schéma est inspiré de l'ancien étalon-or.

Bien que les racines théoriques du système se trouvent dans l'école autrichienne d'économie, le Bitcoin a suscité de sérieuses inquiétudes chez certains économistes autrichiens d'aujourd'hui. Leurs critiques couvrent deux aspects généraux :

- Les bitcoins n'ont pas de valeur intrinsèque comme l'or ; ce ne sont que des bits – s'est-il- dire de la donnée- stockée dans un ordinateur ;
- Le système ne satisfait pas au « théorème de la régression »²⁸, ce qui explique que

²⁸ En statistiques, en économétrie et en apprentissage automatique, un modèle de régression linéaire est un modèle de régression qui cherche à établir une relation linéaire entre une variable, dite expliquée, et une ou plusieurs variables, dites explicatives. « La valeur n'existe pas en dehors de la conscience des hommes ». C'est ainsi que Carl Menger a énoncé ce qu'on appelle la subjectivité de la valeur. Ludwig Von mises a repris les travaux de Carl Menger et en a déduit le théorème de régression. D'où vient la valeur que chacun de nous accorde à la monnaie ? Considérons d'abord une monnaie marchandise, comme l'or. J'accepte de l'or comme paiement à un instant t si à l'instant $t-1$, j'ai constaté le pouvoir d'achat qu'il possédait. Les personnes qui l'ont accepté comme paiement à l'instant $t-1$ l'ont fait parce qu'ils ont constaté qu'à l'instant $t-2$, l'or avait un pouvoir d'achat. Ainsi de suite, en remontant jusqu'à la première utilisation de l'or comme monnaie, on trouve que la première personne qui l'a accepté comme paiement ne l'a fait que parce qu'elle avait constaté que l'or servait à un certain nombre d'usages valorisés par d'autres personnes. Ainsi, le théorème de régression affirme que toute monnaie tire sa valeur de son utilisation non monétaire. Ceci est aussi valable pour les monnaies décréées : l'euro vient du franc, de la lire, etc. qui eux-mêmes étaient grosso modo échangeables contre de l'or jusqu'en 1971.

l'argent est accepté non pas à cause d'un décret gouvernemental ou d'une convention sociale, mais parce qu'il a ses racines dans une marchandise exprimant un certain pouvoir.

1.5. Principes de base de bitcoin :

Le Bitcoin est la première crypto-monnaie apparue, Satoshi Nakamoto a défini à travers cette monnaie :

- Un modèle de monnaie ultrasécurisée, il est impossible de falsifier une transaction réalisée en bitcoins.
- Une monnaie qui permet de garantir l'anonymat, si tant est que l'échange a lieu directement entre deux individus-sans passer par une plateforme intermédiaire.
- Divers algorithmes visant à réguler à tout moment l'émission de la monnaie, et aussi sur le long terme, ses fluctuations.

Cette monnaie repose sur plusieurs principes essentiels, que nous pouvons retrouver dans la plupart des crypto-monnaies qui ont suivi :

- ❖ Un logiciel libre, ou open source, accessible à tous et que les autres peuvent utiliser comme base pour la création d'autres monnaies dérivées du Bitcoin.
- ❖ Une signature cryptographique qui rend chaque transaction unique et infalsifiable.
- ❖ Une technologie révolutionnaire reposant sur un registre des transactions ou bien la Blockchain (voir fonctionnement de la blockchain bitcoin plus bas).
- ❖ Une validation de chaque transaction prenant en compte l'identifiant crypté de chaque intervenant mais aussi une preuve de travail issue d'un calcul ultra complexe pour vérifier que la transaction est valide.
- ❖ Un système de production de la monnaie par des mineurs qui assurent la validation de ces transactions, et qui sont régulièrement récompensés par des bitcoins.

2. Principes de fonctionnement :

A l'inverse des monnaies traditionnelles, les bitcoins ne peuvent pas être matérialisés. Cette monnaie virtuelle prend la forme de données chiffrées et ne peut, par conséquent, être possédées physiquement, à l'instar des devises ayant cours légal. De plus, ils ne sont pas émis par une banque centrale.

2.1. Principes de création de Bitcoin :

Les bitcoins sont créés, de manière aléatoire, à partir d'un algorithme développé par un logiciel libre de "minage" dont le fonctionnement nécessite de puissants outils de calcul que leurs propriétaires (les mineurs) mettent en réseau afin d'augmenter leur chance de gagner un bitcoin.

L'émission des bitcoins est limitée à un total de 21 millions, par le protocole Bitcoin. Plus de 80% du nombre total de bitcoins sont déjà en circulation. D'après différentes estimations, le nombre 21 millions de bitcoins sera atteint aux alentours de 2028²⁹.

Le dispositif algorithmique de création du Bitcoin est ajusté de sorte que lors des quatre (04) premières années du réseau Bitcoin, 10 500 000 unités soient créées. Le chiffre est divisé par deux (02) tous les quatre (04) ans.

En effet, la création d'un nouveau bloc est récompensée par des bitcoins créés à cet effet. Le montant de cette récompense est divisé par deux (*halving*), chaque fois que 210 000 blocs de transactions sont ajoutés à la chaîne de blocs.

De la création du premier bloc (bloc *genesis*) jusqu'au 209 999^e bloc créé le 28 décembre 2012, chaque mineur fut récompensé de 20 bitcoins nouvellement créés pour la création d'un nouveau bloc valide.

Du bloc 210 000 au bloc 419 999, créé le 09 juillet 2016, la récompense était de 25 bitcoins pour chaque bloc nouvellement créé.

Le prochain halving devrait avoir lieu aux alentours de Mai - Juin 2020, le récompense passera donc à 6,25 bitcoins par bloc¹⁷⁹.

2.2. Principe de fonctionnement de la blockchain Bitcoin :

Le Bitcoin fonctionne avec des logiciels et un protocole qui permet aux utilisateurs d'émettre cette monnaie et de gérer les transactions y relatives de façon collective et automatique.

Pour avoir des bitcoins sur un compte, il faut soit qu'un détenteur de bitcoins nous en ait donnés, par exemple en échange d'un bien, soit il faut passer par une plateforme qui

²⁹ Gilles Quoistiaux, Op.cit, P17.

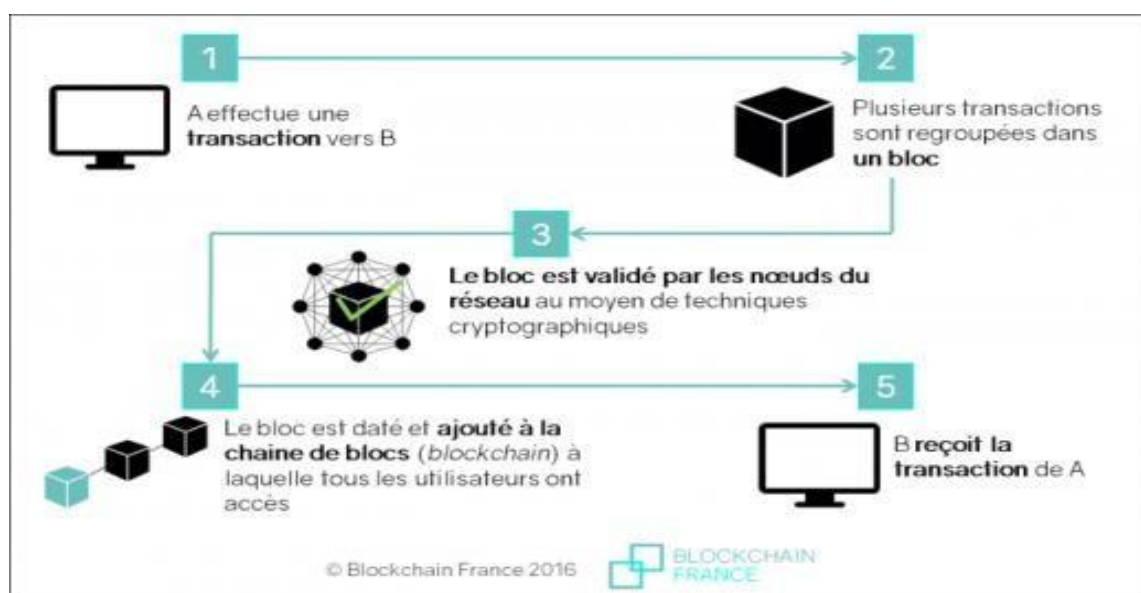
change et convertit des devises classiques en bitcoins, soit les avoir gagnés en participant aux opérations de contrôle collectif de la monnaie sur la blockchain (travail de minage).

Cette blockchain, qui constitue une base de données contenant l'historique de tous les échanges effectués entre utilisateurs, est partagée par ses différents utilisateurs, sans intermédiaire, et permet à chacun de vérifier la validité de la chaîne (appelé aussi logiciel de minage).

La blockchain, constituée de plusieurs blocs, est le principe de base du fonctionnement du système Bitcoin.

En effet, lorsque les transactions sont effectuées entre les utilisateurs du réseau, elles sont regroupées par bloc. Chaque bloc est validé par les nœuds du réseau (mineurs), selon des techniques de proof of work ou preuve de travail (expliqué précédemment), une fois le bloc est validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau (voir figure 3.1).

Figure 3.1 : Le Principe de fonctionnement de la blockchain Bitcoin



Source : Blockchain France (www.blockchain.fr)

2.3. Les principaux utilisateurs Bitcoin :

- Les utilisateurs (simples) : Ce sont les plus nombreux. Ils émettent et reçoivent des paiements en bitcoins. Ils ont le droit de lecture de la base de données (c'est-à-dire qu'ils ont accès à l'ensemble des transactions bitcoin).
- Les mineurs : Ils vérifient et valident les messages de transactions qu'ils reçoivent

en utilisant un logiciel spécifique de minage. Ils ont donc un droit de lecture et d'écriture de la base de données (Blockchain), et sont en quelque sorte garants de la sécurité du système. En effet, plus il y a de mineurs, plus la puissance de calcul du système Bitcoin est grande, et donc les attaques frauduleuses sont moins aisées (attaque des 51%).

2.4. Créations des BITCOINS :

Les monnaies fiduciaires ordinaires que nous utilisons dans la vie réelle sont frappées et émises par les banques centrales.

Les unités de Bitcoin sont quant à elles conçues et émises non pas par une banque centrale, mais par une catégorie de volontaires qui mettent à disposition du réseau d'utilisateurs Bitcoin la puissance de calcul de leurs ordinateurs.

Ces ordinateurs créent la monnaie en résolvant des opérations informatiques codées suivant un algorithme de cryptographie appelé SHA-256 (voir le lexique). Les ordinateurs travaillant à l'émission de ces bitcoins sont appelés des mineurs, ils effectuent un travail de découverte et que la blockchain est le gisement abritant l'or numérique qu'est le Bitcoin.

En retour de leur travail, le réseau gratifie les mineurs proportionnellement à la quantité de travail fourni. Les mineurs ne font pas qu'émettre la monnaie, ils contrôlent et valident aussi les transactions opérées sur le réseau Bitcoin.

La création monétaire du Bitcoin peut sembler très abstraite, car elle ne repose que sur une relation mathématique. C'est pourquoi, pour la compréhension de son fonctionnement, il faut admettre que le bitcoin et sa création repose sur un algorithme, et donc rien de concret, ou du matériel. Ce qui le différencie des monnaies existantes, qui ont une valeur reconnue par tous. C'est pourquoi la valeur du Bitcoin est contestée, elle ne repose sur rien de connu. Certains disent même que "l'électricité est transformé en or".

Une fois créé, le bitcoin peut faire l'objet de transaction. Il peut soit être cédé contre des devises ayant cours légal, soit être utilisé comme moyen de paiement auprès d'un commerçant acceptant le paiement par une monnaie virtuelle.

2.5. Transactions des BITCOINS :

Quand un utilisateur acquiert des bitcoins, il obtient une adresse, qui lui permet de recevoir, stocker et envoyer des bitcoins (aussi bien qu'une adresse mail permet de recevoir et envoyer des mails). Il peut ensuite créer autant d'adresses qu'il le souhaite. Pour pouvoir transférer des bitcoins ; l'utilisateur a également besoin d'une clé privée qui lui permet de calculer la clé publique de l'adresse.

A chaque bitcoin reçu correspond une clé privée. En effet, la clé privée (ou clé secrète) est liée à l'adresse bitcoin par une relation mathématique. Donc elle change à chaque transaction car l'adresse du destinataire des bitcoins est différente de celle de l'expéditeur.

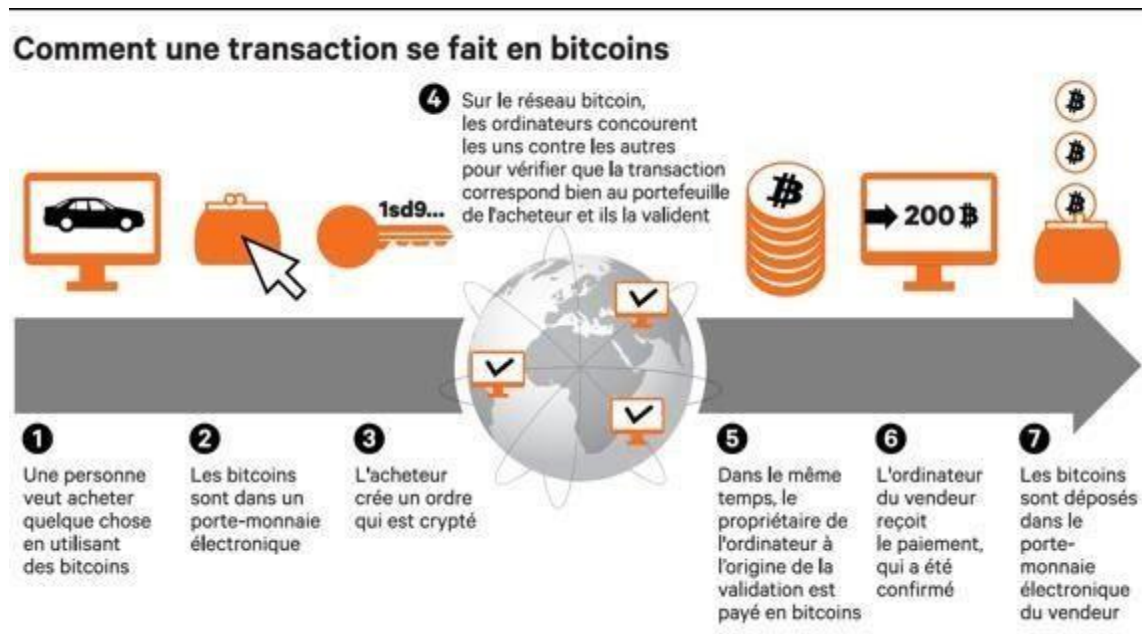
L'adresse et les clés privées sont quasiment impossibles à mémoriser, puisque l'adresse est composée au maximum de 34 caractères, et que la clé privée est une suite de 50 chiffres au plus. C'est pourquoi elles doivent être enregistrées dans une application spécifique. Il existe une application officielle gratuite, qui contient toutes les clés privées. Elle repose sur un fichier, qui est appelé "wallet"(porte-monnaie électronique ou portefeuille).

La clé privée est nécessaire à l'utilisateur pour signer un message. Pour vérifier le message, les autres utilisateurs ont accès à la clé publique de l'émetteur du message, qui est liée par une relation mathématiques (et cryptographique) à la clé privée.

Par analogie, nous pouvons dire que l'adresse est un coffre-fort et que la clé privée est la clé qui ouvre ce coffre.

Ainsi, pour envoyer des bitcoins, une personne (par exemple) émet un message de transaction, qui est composé par le porte-monnaie bitcoin. Le message est en clair (non chiffré), et signé par cette personne. Ce message contient le numéro d'identification de la transaction précédente, le montant de la transaction, la clé publique, l'adresse bitcoin du destinataire, et la signature du message (par la clé privée). Ce message est ensuite vérifié par les mineurs, qui le valident, ou non. Les mineurs vérifient que les transactions précédentes permettent de financer la transaction en question, que l'image de la clé publique du message correspond bien à l'adresse bitcoin de cette personne, et que le message a bien été signé par cette dernière grâce à sa clé publique (voir figure 3.2).

Figure 3.2 : Transaction des BITCOINS



Source : Les Echos (www.lesechos.com)

2.6. Base de donnée Bitcoin et traçabilité :

En effet, les bitcoins sont traçables dès leur origine et organisés en chaîne de blocs.

Les transactions sont donc liées par une chaîne chronologique.

Nous pouvons imaginer qu'un bloc est un document qui passerait de bureau en bureau et recevrait un coup de tampon sur chaque bureau (le coup de tampon étant la signature numérique).

La transparence du Bitcoin est une de ses caractéristiques majeures, c'est pourquoi les utilisateurs ont accès aux bases de données Bitcoin. Une base de données Bitcoin est une sorte de livre de compte public, où nous pouvons voir l'ensemble des transactions Bitcoin à travers le monde. Ce système permet de garantir les transactions et les comptes.

SECTION 2 : Évolution de BITCOIN et son cadre juridique

Dix ans passé sur la création de Bitcoin, depuis quelques années déjà, il a fait beaucoup parler de lui. Le parcours de Bitcoin, bien qu'il soit court, a été émaillé de nombreuses critiques et interdictions de certains Etats, en parallèle le système a connu son lot de piratages du fait de sa nature virtuelle, ou de faillites de plateformes de transactions. Malgré tout, son succès ne s'est pas encore démenti et la progression est impressionnante

depuis l'origine mais avec une volatilité de plus en plus forte. L'écosystème du bitcoin se développe et ses fondamentaux sont solides. Sur ce plan-là les évolutions sont très bonnes. La proportion de personnes utilisant le bitcoin a énormément augmentée, également le nombre de transactions effectuées. La puissance de calcul du réseau n'a jamais été aussi haute et le nombre de développeurs occupés à améliorer le réseau semble également augmenter.

1. Evolution de Bitcoin :

1.1. Le Bitcoin, une monnaie qui s'inscrit dans un processus de mondialisation :

Le Bitcoin ne dépend pas d'un émetteur central. De plus, ce n'est pas une devise : il n'est donc rattaché à aucune entité territoriale. En effet, nous pouvons effectuer des transactions dans le monde entier sans frais supplémentaires contrairement à des devises comme l'euro ou le dollar américain. Aucun change n'est nécessaire pour acheter un bien ou un service à l'étranger. Nous pouvons donc parler du Bitcoin comme d'une "entité monétaire sans frontière". Cependant, nous pouvons voir que les transactions sont émises principalement au niveau des pays développés notamment la Triade tandis que l'Afrique réalise très peu de transaction (voir figure 3.3). Cela peut s'expliquer par les disparités financières et en termes d'accès au réseau internet. La répartition des transactions montre donc que le Bitcoin s'inscrit dans le processus de mondialisation puisque, outre la possibilité de transaction sans distinction de frontière, ce sont toujours les mêmes espaces qui sont lésinés.

Figure 3.3 : Le Bitcoin, Une Monnaie Sans Frontière



Source : www.CoinMap.org

Une carte géographique affichée sur CoinMap.org, un site Web qui répertorie les

endroits où nous pouvons utiliser Bitcoin, montre qu'il existe désormais plus de 15643 (au 16 novembre 2019) entreprises (marchands) qui acceptent la crypto-monnaie comme moyen de paiement.

1.2. Evolution du cours de bitcoin depuis sa création à ce jour (2009-2019) :

La diffusion du bitcoin auprès du grand public se fait soit par l'acceptation d'un règlement en bitcoin lors de la vente d'un bien ou d'un service, soit par l'achat de bitcoin sur sites de ventessur internet (Bitfinex pour le dollar, Okcoin pour le yen...) ³⁰. Ces achats de bitcoin contre des monnaies à cours légal (dollar, euro, etc.) se font simplement de pair en pair et de façon anonyme. Le prix du bitcoin sur ces sites dépend de l'offre et de la demande.

Le cours du bitcoin depuis 2009, date de sa création, a connu de nombreux rebondissements. Très volatile, le prix du bitcoin a déjà connu plusieurs pics et corrections. En l'espace de quelques années, le bitcoin est passé de 0,01 à 20,000 \$.

Selon le graphe, en 2009 et pendant quelques premières années d'existence, le "cours" du bitcoin est resté stable : il faut alors 03 \$ pour obtenir 1000 bitcoins.



Graphe 3.1 : Evolution Du Cours De Bitcoin (2009-2019)

Source : www.blockchain.info

A partir de 2012, le cours commence à s'accroître 0,562 \$ pour un bitcoin au

³⁰ J.M.Figuet, "Bitcoin et blockchain : quelles opportunités ?" Revue d'économie financière, N° 123, 2016, consulté en ligne sur ([Cairn.info](http:// Cairn.info)) le 15/11/2019.

1^{er} janvier 2012, 400 \$ pour un bitcoin, au 1^{er} janvier 2014, 1028 \$ pour un bitcoin au 1^{er} janvier 2017 et presque 20 000 \$ pour un bitcoin le 17 décembre 2017. Actuellement ce cours est à 8 748 \$ pour un bitcoin (au 13/11/2019).

- ❖ Au lancement du bitcoin, en 2009, il n'y avait presque pas de mineurs sur le réseau. La difficulté du minage s'adapte au nombre de mineurs sur le réseau, il était extrêmement facile et peu cher de miner des bitcoin depuis un PC portable.
- ❖ En 2011, la médiatisation du bitcoin entraîne la première bulle spéculative, et le prix du bitcoin prend réellement son envol entraînant un accroissement de la compétition entre mineurs.
- ❖ L'année 2012 est marquée par la fin de l'éclatement de la bulle et une légère reprise des cours, cette année voit également apparaître des innovations dans l'histoire du bitcoin et des crypto-monnaies.
- ❖ L'année 2013 sera marquée par deux pics spéculatifs (avril et novembre). En cette année est apparue la première ICO (Mastercoin aujourd'hui Omni).
- ❖ L'année 2014 sera une année de décroissance pour le cours du bitcoin. Plusieurs événements expliquent cette tendance, parmi autre, la fermeture de MtGox en février, ainsi qu'une série de hack contre les plateformes d'échanges et de nombreuses mises en garde des autorités de tutelles Européenne, Russe et Chinoise.
- ❖ L'année 2015 commence par un crash retentissant du bitcoin qui descendra jusqu'à 177\$ dû au hack de 19 000 bitcoins sur la plateforme Bitstamp. Sera ensuite marquée par une reprise des cours (438 \$).
- ❖ L'année 2017 : la valeur la plus haute du bitcoin. En effet, le cours du bitcoin en cette année a connu une ascension fulgurante en multipliant par 20 sa valeur. Le prix du bitcoin en 2017 est passé de 950 \$ à 20 000 \$ avant de retomber à 15 000 \$ fin décembre 2017, chute déclenchée par des annonces restrictives des autorités chinoises (interdiction des ICO).
- ❖ 2018 fut marqué par l'explosion de la bulle des crypto-actifs et la chute des cours de presque toutes les crypto-monnaies. Aucun événement n'est parvenu à enrayer la tendance baissière.
- ❖ 2019. Il est clair que le prix du bitcoin a connu une forte chute en 2018, entraînant avec la majorité des autres altcoins. Le prix des crypto-monnaies est en effet corrélé à celui du bitcoin

Jusqu'où les prix vont descendre, c'est difficile à dire. La courbe de la bulle peut prendre plusieurs formes.

➤ Analyse graphique d'une bulle spéculative :

Voici un graphique qui décompose très nettement les phases successives d'une bulle spéculative :

Cette courbe ressemble beaucoup à la courbe traditionnelle des bulles, avec un premier rebond après la première chute puis une chute plus bas que le prix initial avant de repartir.

Graph 3.2 : Une bulle spéculative Bitcoin



Sources : JDN (www.journaldunet.com)

D'après les analystes, une chose est certaine est qu'un nouveau cycle haussier va s'enclencher ensuite, prenant comme exemple le cours des actions Apple et Amazon qui ont subi l'éclatement de la bulle internet en 2000. De la même manière que l'éclatement de la bulle internet n'a pas mis fin à internet, l'éclatement de la bulle Crypto ne mettra pas fin au déploiement des crypto-monnaies et de la technologie blockchain en général. Il est donc fort probable que le cours des meilleures crypto-monnaies suive le même parcours que celui des actions Apple et Amazon³¹.

1.3. Evolution des transactions en bitcoins :

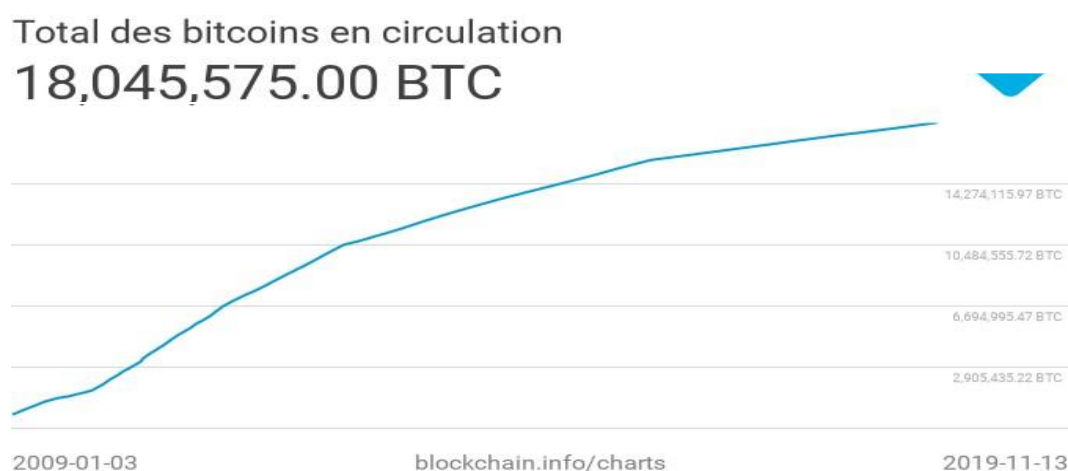
Bien qu'essentiellement acquis à des fins spéculatives, le Bitcoin peut-être

³¹ BEX (Blockchain-expert) consulté en ligne sur (blockchain-expert.com) le 16/11/2019.

également utilisé pour les transferts internationaux entre particuliers et comme monnaie de paiement pour les commerces.

Dans de nombreux pays émergent le Bitcoin est apparu comme un outil de développement pour des populations non bancarisées qui ont accès à la téléphonie et à internet. Par ailleurs, il est utilisé comme valeur refuge par certaines personnes pour éviter la fluctuation de leur propre monnaie.

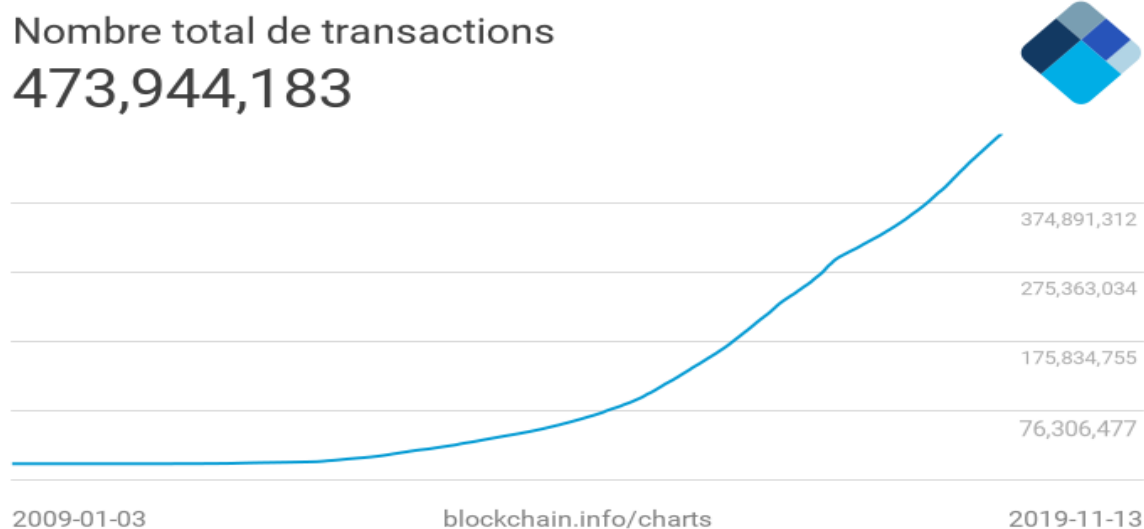
Graph 3.3 : Evolution Du Nombre De Bitcoin En Circulation (2009-2019)



Source : <https://www.blockchain.info>

Actuellement dans le monde, il existe plus de 18 millions de bitcoins en circulation (18.045.575,00 BTC) au 13/11/2019. A terme, il en existera 21 millions.

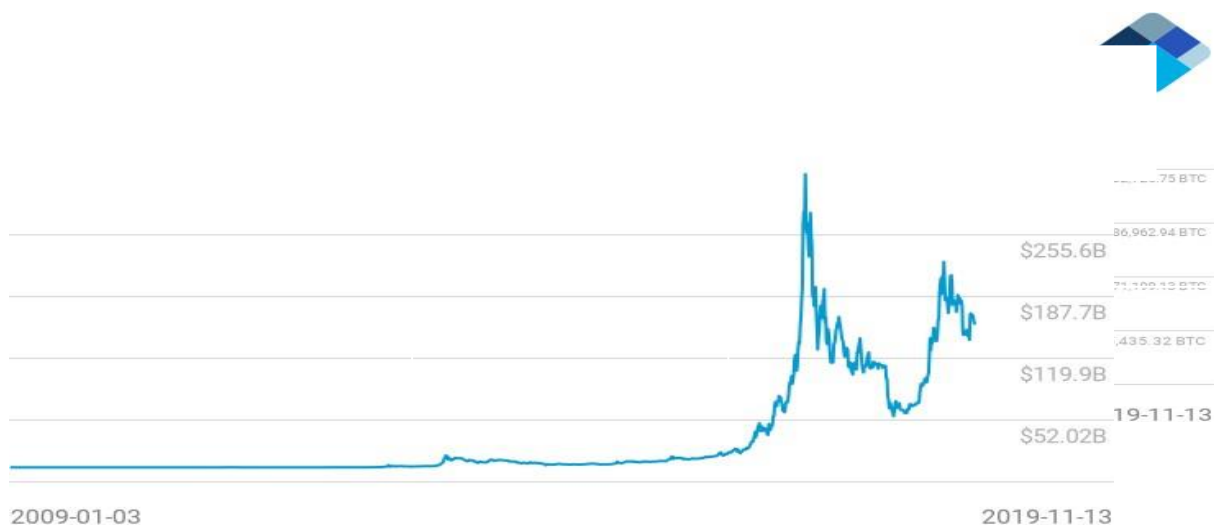
Graph 3.4 : Evolution Du Nombre De Transactions En Bitcoin (2009-2019)



Source : <https://www.blockchain.info>

Les transactions en bitcoins en croissance continue, notamment à partir de 2017 où la valeur des transactions a dépassé 5 milliards de dollars. aujourd'hui le nombre de ces transactions est de 473.944.183 transactions qui est l'équivalent d'une valeur de 170.325,99 BTC. (Le 13/11/2019).

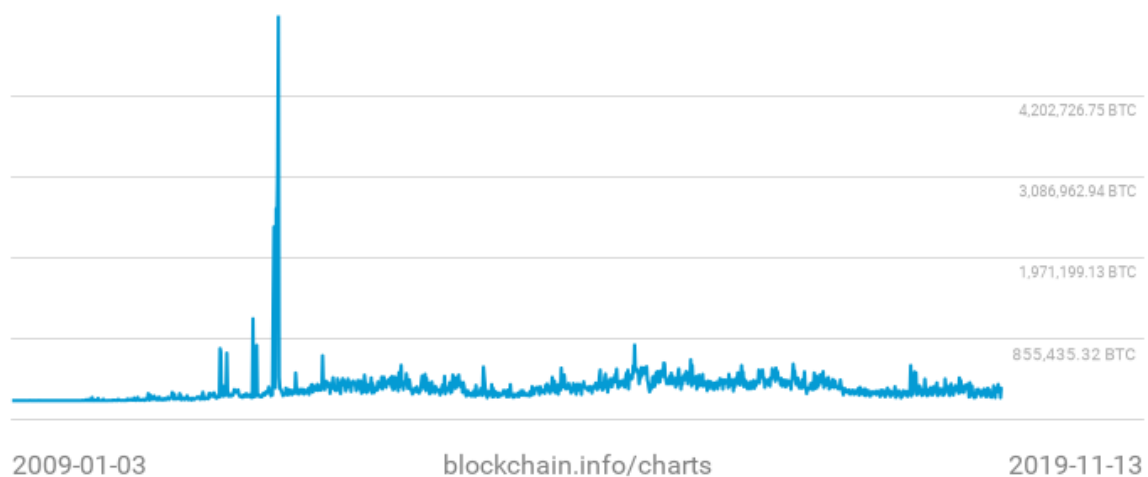
Graphe 3.5 : La Valeur Des Transactions En Bitcoin (2009-2019)



Source : <https://www.blockchain.info>

Graphe 3.6 : Evolution De la capitalisation boursière du Bitcoin (2009-2019)

Valeur estimée des transactions
170,325.99 BTC



Source : <https://www.blockchain.info>

Quant à la capitalisation boursière de Bitcoin, elle est estimée à 157.870.058.710 \$ (1 579 B) toujours au 13/11/2019.

Donc ces graphiques présentent l'évolution de la valeur totale estimée des transactions sur la blockchain Bitcoin sur le marché mondial depuis sa création (2009) jusqu'à novembre 2019. La valeur estimée des transactions sur la blockchain Bitcoin a connu de fortes variations notamment au cours des années 2017, 2018 et 2019, une accélération liée surtout à une augmentation de la taille des blocs de la blockchain.

Graph 3.7 : Evolution Du Nombre De Bitcoins Créés A Travers Le Temps



Source : <https://www.blockchain.info>

- Au bloc 210 000 : 10 500 000 BTC sur le marché ;
- Au bloc 420 000 : 15 750 000 BTC sur le marché ;
- Au bloc 630 000 : 18 375 000 BTC sur le marché ;
- Au bloc 840 000 : 19 687 500 BTC sur le marché ;
- Au bloc 1 050 000 : 20 343 750 BTC sur le marché.

L'engouement des personnes pour cette monnaie explique sa comparaison fréquente à l'or. On parle alors de "l'or numérique".

1.4. Distribution globale des nœuds Bitcoin :

Selon une étude réalisée en 2019³², il y a 36 pays dans le monde avec au moins 1% de leur population qui utilise Bitcoin. Cette étude supposait une relation entre le rapport entre les nœuds Bitcoin dans deux pays et le nombre d'utilisateurs dans ces pays.

Selon ce rapport, il semble théoriquement possible d'examiner la répartition des utilisateurs de Bitcoin dans le monde. Ce qui suit est une estimation du nombre d'utilisateurs de Bitcoin sur différents continents.

❖ Europe et Amérique du Nord :

L'Europe et l'Amérique du Nord ne sont pratiquement jamais absentes des discussions relatives aux avancées technologiques. Sur les 36 pays où les utilisateurs de Bitcoin constituent au moins 1% de leur population, 26 se trouvent en Europe ou en Amérique du Nord.

Ces pays comprennent le Canada, la France, la Belgique, la Biélorussie, l'Allemagne, le Royaume-Uni et les États-Unis. Les autres pays sont la Lituanie, le Luxembourg, la Norvège, la Roumanie, l'Islande, la Slovénie et la Suède

En regardant la distribution actuelle des nœuds mondiaux, il existe une forte densité de nœuds en Europe et en Amérique du Nord. En outre, parmi les dix premiers pays en fonction du nombre de nœuds, seuls trois (Chine, Singapour et Japon) viennent de pays autres que l'Europe et d'Amérique du Nord (voir tableau N°6).

❖ Amérique du Sud, Asie et Australie :

Novembre 2018, le nombre total de nœuds Bitcoin avait dépassé les 10 000 selon les derniers chiffres de Coin Dance,

Outre le Japon et Singapour, la Corée du Sud, l'Australie et l'Inde comptent également au moins 1% de leur population d'utilisateurs de Bitcoin. La Chine n'entre toutefois pas dans cette catégorie, ce qui rend la présence de l'Inde particulièrement remarquable compte tenu des similitudes entre leurs chiffres de population.

En Amérique du Sud, le Brésil, l'Uruguay et l'Argentine comptent le plus grand nombre d'utilisateurs de Bitcoin. Le Venezuela ne semble toutefois pas se classer sur une échelle

³² Block Blog, distribution des noeuds bitcoins dans le monde, consulté en ligne sur (blockblog.fr) consulté le 16/11/2019.

significative.

❖ Afrique :

En Afrique, seulement Afrique du Sud enregistre un nombre important d'utilisateurs. Selon l'étude entre 0,1 et 0,99 % de sa population d'utilisateurs de Bitcoin. Des pays comme l'Angola et la Tanzanie comptent entre 0,01 et 0,099%.

L'accès à l'électricité étant encore un luxe dans de nombreuses régions du continent, les résultats de l'étude ne sont pas surprenants. Selon Bitnodes, la nation africaine la mieux classée sur la base du nombre de nœuds Bitcoin, l'Afrique du Sud, est à la 33ème position (sur 100).

Figure 3.4 : La Carte Géographique De La Concentration De Nœuds Bitcoin Accessibles Dans Des Pays Du Monde Entier

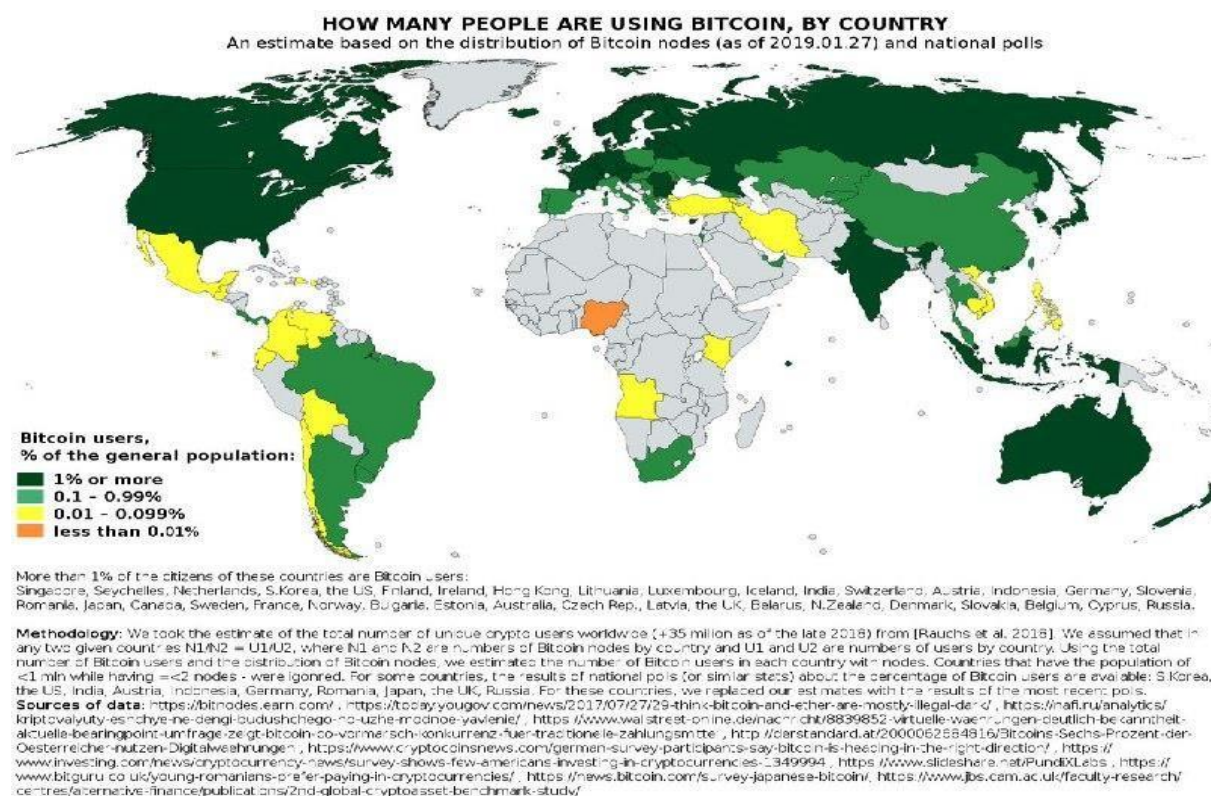


Tableau 3.2 : Les 10 principaux pays par rapport au nombre de nœuds accessibles (arrêté au 16/11/2019)³³.

RANG	PAYS	NŒUDS	RANG	PAYS	NŒUDS
1	<u>États Unis</u>	2465 (26, 09%)	6	<u>Canada</u>	334 (3, 54%)
2	<u>Allemagne</u>	1896 (20, 07%)	7	<u>Royaume-Uni</u>	328 (3, 47%)
3	<u>France</u>	605 (6, 40%)	8	<u>Chine</u>	306 (3, 24%)
4	<u>Pays-Bas</u>	502 (5, 31%)	9	<u>Fédération Russe</u>	240 (2, 54%)
5	<u>Singapour</u>	365 (3, 86%)	10	<u>Japan</u>	196 (2, 07%)

Ce tableau confirme l'analyse précédente faite sur le volume de distribution des nœuds bitcoins dans le monde. Les Etats unis et l'Allemagne en tête avec des taux respectivement de 26,09 % et 20,07 %, suivi de la France et Pays Bas avec 6,40 % et 5,31 %. Ceci est expliqué par la forte densité des innovations technologiques qui favorise l'évolution de cette monnaie dans ces régions.

2. Cadre juridique du Bitcoin :

La nature juridique du bitcoin n'est pas une question uniformément tranchée.

La dimension internationale du bitcoin, en regard du caractère régional des cadres juridiques (UE, Etats-Unis, Chine, notamment), écarte toute réponse juridique globale, en l'état actuel d'aujourd'hui.

En particulier, le G20 a considéré que, si les crypto-actifs soulèvent des problèmes en ce qui concerne la protection des consommateurs et des investisseurs, l'intégrité du marché, l'évasion fiscale, le blanchiment d'argent et le financement du terrorisme, alors ils doivent être gérés par les Etats plutôt que par le G20 lui-même.

³³ Bitnodes (bitnodes.fr) consulté le 16/11/2019.

Légal
 Soumis à restriction
 Interdit indirectement suivant l'interprétation d'anciennes lois
 Interdit
 Pas de données

2.1. Union européenne :

Le 22 octobre 2015, la Cour de justice de l'UE a confirmé que les opérations d'échange de bitcoins contre des devises traditionnelles étaient exonérées de TVA, considérant le bitcoin comme une "devise virtuelle" et non comme un bien ou un service.

Le rapport conclut à l'intérêt économique du bitcoin et à la nécessité d'en réguler le développement, afin d'en contenir les risques spécifiques. Il n'offre pas davantage de

définition juridique ferme du bitcoin.

Le 26 février 2014, le sénateur américain Joe Manchin demande l'interdiction du bitcoin aux USA, en raison de sa volatilité incontrôlée et des risques qu'il soit utilisé à des fins illégales.

Le 10 décembre 2017, la Bourse de Chicago a institutionnalisé le Bitcoin.

2.3. Japon :

La banque centrale du Japon reconnaît officiellement le bitcoin et crypto-monnaies comme un moyen de paiement (article 2-5 du PSA amendé, précise que les monnaies virtuelles sont acceptées comme moyen de paiement sans qu'elles soient des monnaies légales).

2.4. France :

En France ni loi ni jurisprudence n'ont réglementé spécifiquement et avec clarté la nature et le régime juridique du bitcoin. Pour certains juristes, il ne s'agit pas d'une monnaie. Pour d'autres serait "une monnaie, de nature électronique, dépourvue de cours légal".

Pour la commission nationale des comptes de campagne et des finances politiques, il s'agit d'une "monnaie sans statut légal défini". Pour la direction générale des finances publiques, le bitcoin est considéré comme un bien meuble, la valeur à l'achat ou à la vente et sa valeur en fin d'année fiscale faisant valeur légale.

En janvier 2018, le ministre de l'économie, Bruno Le Maire, demande d'appréhender "les risques de spéculation et les possibles détournements". Il confie une mission sur bitcoin à Jean-Pierre Landau, ancien sous-gouverneur de la Banque de France. Dans son rapport, Jean-Pierre Landau préconise de ne pas réguler directement les crypto-monnaies (sauf dans le cadre de la lutte anti blanchiment), de créer un environnement favorable au développement de cette technologie et de limiter strictement l'exposition du secteur financier aux crypto-monnaies.

Le 12 septembre 2018, la France devient le premier pays du monde à accorder un cadre légal aux ICO. Ces levées de fonds en crypto-monnaies ; si ne sert pas de régulation à l'usage du bitcoin, ouvre un premier pas.

2.5. Chine :

Le 05 décembre 2013, la Banque centrale chinoise interdit aux banques locales toute transaction en bitcoin, mesure entraînant le début d'un crash sur la valeur de la monnaie virtuelle. BTC China, première plateforme mondiale de transaction en bitcoin, interdit aux usagers de nouveaux dépôts en Yuan sur leur compte "suite à de nouveaux règlements gouvernementaux".

Le 08 janvier 2014, le groupe chinois Ali Baba interdit les paiements en bitcoin, conformément à la nouvelle réglementation chinoise.

Une circulaire du 04 septembre 2017 conduit soit à la fermeture de plateforme d'échange soit à la fin de l'acceptation de monnaies fiat.

En février 2018, le gouvernement chinois annonce vouloir renforcer l'interdiction par la censure de tous les sites internet d'échange de bitcoin chinois ou étrangers.

2.6. Corée du Sud :

Le bitcoin et les crypto-monnaies sont légales et reconnues comme des instruments financiers.

Aucune restriction n'existe pour la détention et l'échange de bitcoin entre particuliers. Les plateformes d'échange doivent s'assurer de posséder au moins 500 millions de wons coréens pour protéger les commerçants contre les malversations et les fraudes.

Le gouvernement de la Corée du Sud dispose d'accords avec 14 plateformes d'échange d'"espèces virtuelles" dites *currency exchanges*. Grâce à ces accords, ces plateformes n'acceptent que les seuls utilisateurs dont l'identité soit contrôlée par un acteur financier comme une banque.

L'Etat sud-coréen régit aussi les points suivants :

- Interdiction pour les mineurs d'échanger de l'argent ;
- Taxe sur les bénéfices issus de la vente de bitcoin ;
- Interdiction des ICO.

2.7. Royaume-Uni :

Le bitcoin est considéré comme de l'argent privé. Lorsque les crypto-monnaies sont

échangées contre des livres sterling ou d'autres monnaies fiduciaires, comme l'euro ou le dollar, aucune TVA n'est due. Toutefois, la TVA s'applique pour tous les biens et services qui pourraient être échangés contre des bitcoins. Les profits réalisés sur les crypto-monnaies sont assujettis à l'impôt sur les gains en capital.

2.8. Suisse :

En Suisse, le Conseil Fédéral a considéré que le bitcoin est une monnaie virtuelle d'un usage marginal, et qu'à ce titre il est soumis en principe à la législation des monnaies régulières. Il recommande toutefois aux autorités et aux organisations de défense des consommateurs responsables d'appeler les utilisateurs de bitcoins à la prudence.

D'après lui, l'exécution des contrats passés en monnaies virtuelles peut en principe être assurée et les infractions commises avec ses monnaies sont punissables.

2.9. Australie :

En décembre 2013, le gouverneur de la banque d'Australie (RBA) a indiqué, dans une interview sur la légalité du bitcoin que *"il n'y aurait rien pour empêcher les gens de décider de faire des transactions dans une autre monnaie dans un magasin s'ils souhaitaient. Il n'y a pas de loi contre cela, donc nous avons des monnaies concurrentes."*

L'Australie a confirmé officiellement que le bitcoin serait traité comme de l'argent le 01 juillet 2017 et qu'il serait soumis à une double imposition.

2.10. Russie :

Le 06 février 2014, la Russie déclare le bitcoin une monnaie illégale sur son territoire, et que la seule monnaie officielle est le rouble et qu'aucune autre monnaie ne peut légalement être utilisée dans le pays. Cependant, à partir de novembre 2016 elle a déclaré, que celui-ci n'était "pas illégal" selon le service fiscal fédéral de la Russie.

2.11. Algérie :

«L'achat, la vente, l'utilisation et la détention de la monnaie dite virtuelle est interdite», stipule la loi de finances 2018 dans son article 117. Cet article précise que la monnaie virtuelle est celle utilisée par les internautes, à travers le web et qu'elle est caractérisée par l'absence de support physique, tel que les pièces, les billets, les paiements par chèque ou carte bancaire. Le même article prévient que toute personne qui commet une

infraction à cette disposition est puni, conformément aux lois et règlements en vigueur³⁴.

Selon Nassim Belouar, master en conseil et expertise à l'université de Lille, invité à la matinale de CARE (Centre d'action et de réflexion autour de l'entreprise) en novembre 2018, «*Il y a quelques 300 000 transactions quotidiennes effectuées par 60 000 utilisateurs en Algérie* ». Partant de ce constat dont il n'a pas apporté de preuves concrètes, il a plaidé l'autorisation de l'usage de la crypto-monnaie en Algérie afin de contribuer à la construction d'une économie numérique. Un avis qui n'est pas partagé par d'autres spécialistes et acteurs sur le terrain. Lors de la même matinale, Nassima Babaci, directrice des partenariats à Macirvie a indiqué que «*la crypto-monnaie n'est pas faite pour concurrencer la monnaie légale*» et qu'elle «*n'est pas non plus faite pour être une monnaie légale*»³⁵.

➤ Un bitcoin égale à 970 928,23 DA³⁶.

2.12. Maroc :

Le 20 novembre 2017, l'Office des changes du Maroc déclare que les transactions effectuées via les monnaies virtuelles constituent une infraction à la réglementation des changes, passible de sanctions et d'amendes.

2.13. Tunisie :

Le gouverneur de la Banque centrale de Tunisie Chedly Ayari a affirmé son opposition au bitcoin le 05 avril 2016, du fait de son risque supposé pour le financement du terrorisme. Son successeur à la tête de la Banque centrale de Tunisie, Marouane Abassi, a quant à lui annoncé en avril 2019 que la Tunisie "étudiait sérieusement la possibilité d'émettre une obligation souveraine Bitcoin.

Il paraît que 2018 est une année de réglementations. Les choses ont déjà commencé à se chauffer, les pays du monde entier se battent avec les crypto-monnaies et cherchent à décider comment les traiter. Certains sont accueillants, d'autres – méfiants. Et, il y en a ceux qui s'y opposent totalement.

³⁴ El watan "Les crypto-monnaies indésirables en Algérie " publié en ligne le 12/02/2018 consulté sur (<https://www.elwatan.com>).

³⁵ Dziri "crypto-monnaie. Pourquoi l'Algérie a interdit l'usage du Bitcoin" publié en ligne le 21/05/2018 consulté sur (dziri-dz.com)

³⁶ Données fournies par Morningstar pour la devise et Coinbase pour la crypto-monnaie la journée du 19/11/2019.

SECTION 3 : Débat au tour de BITCOIN

Le Bitcoin constitue sans doute l'expérimentation monétaire la plus retentissante de l'histoire.

En 10 ans d'existence, l'invention du mystérieux Satoshi Nakamoto pèse désormais plus de cent milliard de dollars. Et la technologie blockchain, ainsi été mise au point, n'en est sans doute qu'à ses débuts. En effet, le Bitcoin attire de plus en plus l'attention des spéculateurs, des consommateurs et des sites marchands, et augmente rapidement en capitalisation. Les autorités de régulation sont plus que jamais préoccupées par la façon dont il doit être traité. De point de vue économique, est-il une monnaie ? Une chaîne de Ponzi ou un actif financier très spéculatif ? Selon les réponses données à cette question les réactions et opinions sont très différentes et divergent.

1. Avantages et inconvénients du Bitcoin :

Dès l'origine, Bitcoin a fait l'objet de nombreuses discussions aussi bien techniques qu'économiques ou mêmes politiques. De ces discussions, un nombre d'avantages et d'inconvénients ont été tirés :

1.1. Avantages allégués :**Souplesse et versatilité :**

- Avec Bitcoin, il est possible d'envoyer et de recevoir de l'argent, en le convertissant en monnaie virtuelle ;
- Partout dans le monde ;
- A n'importe quel moment et sans rupture (indépendamment des jours fériés) ;
- Quasi instantanément (les transactions sont très rapides de quelques secondes à quelques heures) ;
- Sans limitation (contrairement à une banque qui instaure des plafonds quotidiens ou mensuels ;
- Indépendamment des politiques d'émission de monnaie d'autorités monétaires.

Sécurité :

- Dans le principe, les utilisateurs sont les seuls à pouvoir commander la réalisation d'une transaction ;
- La transaction est irréversible, ce qui constitue une protection pour le vendeur, qui

ne peut subir de répudiation par l'acheteur après avoir expédié le bien ou le service ;

- Les commerçants ne peuvent pas facturer de frais supplémentaires sans le faire savoir au préalable à l'acheteur ;
- Le Bitcoin (comme toute autre crypto-monnaie) est insaisissable si elle est suffisamment protégée ;
- Le protocole ne peut pas être manipulé par un individu, une organisation ou un gouvernement.

Transparence transactionnelle :

- Toutes les transactions finalisées sont disponibles et consultables par tout le monde sur la blockchain ;
- Toute personne peut à tout moment vérifier les transactions ;
- Les transferts transactionnels peuvent être tracés d'adresse en adresse.

Valeur refuge :

- Le bitcoin conserve (et même accroît) sa valeur face à des monnaies subissant une forte inflation.

Large diffusion :

- Le protocole de paiement est parvenu à s'implanter progressivement chez des commerçants, et il continue de croître rapidement.

Robustesse :

- Malgré plusieurs crises (explosion de la bulle des cours en 2010, faillite de Mt. Gox), Bitcoin s'est montré résilient.

Pertinence du concept :

- Le concept sous-jacent aux monnaies virtuelles ouvertes est également considéré par des banques, des institutions financières et des autorités monétaires qui pourraient développer des monnaies virtuelles régulées juridiquement sécurisées ;
- La technologie intéresse de plus en plus les banques et les autorités monétaires officielles.

1.2. Risques allégués :**1.2.1. Risques pour le porteur :****Volatilité :**

- Le bitcoin est volatile car le nombre de pièce est limité face à une demande qui croît ;
- Le cours évolue au gré de l'actualité sur les crypto-monnaie ;
- La crypto-monnaie est flottante comme n'importe quelle devise et fluctue différemment face à différentes devises.

Irréversibilité :

- Une transaction en bitcoins est irréversible et ne peut être annulée.

Dépendance à internet :

- Le protocole Bitcoin est une surcouche du protocole IP qui est la base du fonctionnement d'internet. En cas de coupure internet (panne électrique/informatique ou bien arrêt forcé par un gouvernement des routeurs des fournisseurs internet par exemple) ou si un gouvernement ne promeut/défend pas la neutralité d'internet, le protocole Bitcoin pourrait être ralenti voire complètement bloqué par des fournisseurs internet ou un Etat.

1.2.2. Gigantisme (Limite technique) :

- La taille de la base de données s'est accrue de manière très rapide et requiert plusieurs giga-octets de mémoire dans un disque dur. Certains experts se sont interrogés sur la taille future de cette base de données et discutent de solutions possibles pour économiser de l'espace disque comme d'élaguer les transactions les plus anciennes ;
- Augmentation des besoins en bande passante pour charger tous les blocs de la blockchain ;
- La taille du bloc : des "super-nœuds" bitcoin sont envisagés pour faciliter la propagation de l'information à travers les nœuds du réseau et qui peinent à suivre l'augmentation de la taille de la base de données.

1.2.3. Risque lié aux établissements :

Pour convertir la crypto-monnaie en devises, il est obligatoire de passer par une plateforme d'échange opérée par des entreprises privées et qui sont potentiellement vulnérables aux défaillances ou aux faillites, comme cela est arrivé à MtGox.

1.2.4. Impact et risques environnementaux :

Ils sont liés à la consommation électrique générée par le minage, qui représente, selon les estimations, de 0,15% à 0,32% de la consommation mondiale d'électricité. Ils sont faibles quand celle-ci est produite à partir d'énergie renouvelables, mais importants pour les énergies fossiles (réchauffement climatique et pollution de l'air).

De plus en plus de fermes de serveurs sont installées dans des pays au climat froid (pour faciliter leur refroidissement) disposant d'énergie renouvelables bon marché, comme le Canada et l'Islande.

1.2.5. Risque éthique :

Critique sur la philosophie de Bitcoin et son concept économique, en comparaison avec les monnaies des Etats ou l'étalon-or : Bitcoin favoriserait les premiers acquéreurs de la monnaie ("early adopters"). Cette allégation est tantôt confirmée par certaines études montrant que la répartition de la richesse dans bitcoin est très inégalitaire, tantôt infirmée par d'autres.

1.2.6. Risques de fraude, risques systémiques et risques spéculatifs :

- Il a été évoqué que Bitcoin pouvait être assimilé à un schéma de Ponzi, mais cela n'est pas applicable : le cours de la crypto-monnaie est un équilibre entre acheteurs qui cherchent acquérir la monnaie et des vendeurs qui cherchent la vendre. Dans un schéma de Ponzi les nouveaux entrants rémunèrent les anciens entrants.
- Lorsque le cours du bitcoin a franchi les 1 200 \$, certains articles de presse qualifient le phénomène de topomanie³⁷.
- Certaines Banques Centrales (BCE, Banque de France, Banque de Chine) ont lancé des mises en garde sur l'usage du bitcoin insistant sur son caractère hautement spéculatif et sur son utilisation possible à des fins criminelles.

2. Bitcoin est-il une monnaie ?

Le Bitcoin et les crypto-monnaies sont-elles économiquement viables et compétitives, notamment au regard des systèmes de paiement centralisés traditionnels, eux-

³⁷ Tulipomanie, (tulipe mania en anglais) est le nom donné au soudain engouement pour les tulipes dans le nord des Provinces-Unies au milieu du XVIIe siècle, qui entraînera l'augmentation démesurée puis l'effondrement des cours de l'oignon de tulipe : ce qu'on appelle "crise de la tulipe" en histoire économique (1636-1637 : Pays Bas).

mêmes en amélioration constante ? Le Bitcoin est-il une monnaie ? La question mérite d'être au regard de leurs performances actuelles.

C'est un vaste débat quasi-philosophique, mais nous allons essayer de fournir quelques pistes de réflexion.

2.1. Le Bitcoin n'est pas une monnaie :

*"Le Bitcoin n'est pas une monnaie"*³⁸ : voici une phrase souvent prononcée par des observateurs qui estiment que cet actif numérique, dont la valeur n'est soutenue par aucune institution, ne peut être qualifié comme tel.

Les économistes s'accordent généralement sur les trois fonctions essentielles de la monnaie, déjà spécifiées par Aristote dans l'antiquité, à savoir : moyen d'échange, unité de compte et réserve de valeur.

La monnaie au sens moderne émerge avec l'exploitation de ses trois fonctions par les pouvoirs politiques, ce qui amène la monnaie à se doter progressivement de deux autres fonctions, à savoir la fonction de procurer des revenus de seigneurage et la fonction de stabilisation macroéconomique et financière.

Plusieurs études ont examiné si le Bitcoin remplissait les trois fonctions classiques de la monnaie et ont parfois discuté les deux autres fonctions sans l'explicitier.

2.1.1. Moyen d'échange :

Pour l'instant, l'utilisation du bitcoin dans le commerce quotidien est plutôt restreinte. Il est accepté surtout par des sociétés qui vendent des logiciels et du matériel informatique au service du fonctionnement du système Bitcoin ainsi que par les plateformes fournissant des services spéculateurs sur le marché du Bitcoin. Étant donnée sa faible utilité en tant que moyen de paiement dans les transactions commerciales, le bitcoin n'a pas de valeur intrinsèque significative.

Un aperçu de l'adoption du bitcoin peut être obtenu à partir des données tirées du grand livre de compte enregistrant les transactions en bitcoin. Le nombre de transactions par

³⁸ Estelle Hemdane, Alain Beitone, "le Bitcoin (BTC) est-il de la monnaie ?" janvier 2018, consulté en ligne sur le blog d'Alain Beitone (alainbeitone.blogspot.com) le 17/11/2019.

jour avoisine 304 671 au 18/11/2019³⁹. La majeure partie de ces transactions impliquent des transferts entre des spéculateurs. Les achats de biens et services présentent seulement 10% à 20% de ces transactions. Cela semble très peu, vu le grand nombre de commerces en ligne et hors ligne annonçant l'acceptation du paiement en bitcoin.

Le bitcoin n'est pas efficace pour assurer la fonction de moyen de paiement. Un obstacle sérieux résulte de la difficulté de se fournir des nouveaux bitcoins. Un consommateur peut se procurer des bitcoins en tant que "mineur" de bitcoin. Cette activité n'est plus rentable actuellement pour un mineur individuel disposant de moyens techniques limités car le résultat ne couvre pas les coûts en matériel et en énergie. L'activité de minage est actuellement dominée par des acteurs disposant des superordinateurs très onéreux. Il est donc obligé de se procurer des bitcoins auprès des plateformes de marché ou des revendeurs en ligne avec la charge pour lui de trouver un moyen de les stocker en toute sécurité. Le paiement de ces achats est peu pratique puisque ceci doit généralement se faire par un virement bancaire ou en liant un compte bancaire existant à la transaction. Les marchés de bitcoin sont peu liquides, ce qui implique des écarts importants entre prix d'achat et de vente. Par ailleurs, les coûts de transactions et les risques liés à l'exécution des ordres et à la conservation des bitcoins sont non négligeables.

2.1.2. Unité de compte :

Pour qu'une monnaie puisse servir comme unité de compte, il faut que les agents privés l'acceptent comme un numéraire de référence pour exprimer et comparer des prix des biens et services, des actifs et des facteurs de production, et l'utilisent dans leurs calculs économiques et dans leurs comptabilités.

La forte volatilité du prix du bitcoin l'empêche de devenir une unité de compte. Un changement trop fort et trop fréquent du prix du bitcoin ne permet pas aux vendeurs d'afficher un prix fixe durant une certaine durée sans subir de risque. Le changement fréquent du prix entraînerait un coût non négligeable et créerait de la confusion pour les acheteurs qui auraient du mal à comparer les prix en bitcoin chez différents vendeurs. Les bitcoins reçus posent aussi un problème de risque de change qui semble trop important pour les vendeurs ayant un gros volume de transactions en bitcoin à cause de la forte variation quotidienne de son prix.

³⁹ Source Blockchain.com, Op.cit.

Outre ce problème, il y a aussi celui dû à la grande divergence des prix du bitcoin à un moment donnée sur les différentes plateformes de marché. Cette disparité constitue une violation flagrante de la loi d'unicité des prix. Le calcul des prix moyens par certains sitesweb ne résout pas le problème d'information concernant le prix effectif de l'achat ou de la vente d'un bitcoin au moment où les acheteurs et les vendeurs veulent réaliser une transaction en bitcoin. Ils sont frustrés par le fait de ne pas pouvoir vendre librement là où le prix de bitcoin est le plus élevé et acheter là où il est le moins cher. La difficulté de faire des arbitrages sur les différents marchés pour des raisons techniques implique que cette situation puisse persister pour longtemps. Cela n'arrive pas pour les monnaies officielles qui sont quotidiennement échangées sur les marchés de change interconnectés.

Aussi, le fait de limiter la quantité de bitcoins à 21 millions d'unités peut générer une tendance déflationniste très forte si son adoption est généralisée. Une déflation associée au bitcoin serait beaucoup plus néfaste que celles observées dans l'histoire économique, étant donnée le rythme de hausse de la valeur du bitcoin prévisible suite à la généralisation de son usage.

Le développement de l'usage du bitcoin dans le commerce se heurte à une autre grande difficulté, souvent négligée ou sous-estimée par les promoteurs du bitcoin, qui résulte du fait que la valeur unitaire du bitcoin est très élevée par rapport à la plupart des produits et services ordinaires. Cela oblige les commerçants à fixer des prix de la plupart des biens et services en quatre décimales ou plus car la limite de la division des bitcoins est de huit décimales. Or, les agents privés peuvent ne pas comprendre ces prix d'autant plus qu'ils sont habitués à avoir des prix en zéro ou deux décimales dans les monnaies officielles sauf sur les marchés de change.

2.1.3. Réserve de valeur :

La fonction de la monnaie en tant que réserve de valeur traduit sa capacité de permettre à son détenteur de reporter la consommation à une date future incertaine sans perdre trop de valeur. Dans cette fonction, la monnaie est jugée sur deux critères :

- La monnaie doit être facile à conserver en sécurité, notamment contre les vols ou la perte. Dans le système monétaire officiel, les détenteurs de monnaie peuvent réduire considérablement les vols ou la perte en la conservant à la banque.
- La valeur de la monnaie doit être stable dans le temps. Les banques centrales

s'efforcent à l'heure actuelle de stabiliser le taux d'inflation à un niveau faible, ce qui permet de donner confiance aux agents économiques en la capacité de la monnaie officielle à conserver de la valeur pour le futur.

Pour l'instant, le bitcoin a du mal à satisfaire ces deux critères. Concernant la conservation, les bitcoins doivent être détenus dans des comptes informatiques ou des disques durs (wallet). La sécurité de ces portefeuilles est une difficulté majeure pour le fonctionnement du système bitcoin. En tant que réserve de valeur, le bitcoin fait face à de grands défis en raison d'attaques informatiques, de vol et d'autres problèmes liés à la sécurité. Il est possible de souscrire des contrats d'assurance contre les vols, mais cela implique des coûts de détention assez significatifs.

Outre ce problème de sécurité, ses détenteurs sont confrontés à un problème de gestion du risque résultant de la volatilité élevée de la valeur du bitcoin. Les études statistiques montrent que la volatilité du bitcoin est comparable à celle des actions les plus spéculatives, dépassant 100% contre une volatilité autour de 10% pour les devises officielles et de 20% pour le prix de l'or⁴⁰. La détention de bitcoins, même pendant une courte période, est très risquée, ce qui est incompatible avec une monnaie servant comme réserve de valeur et remet en cause la capacité d'une monnaie à fonctionner comme unité de compte. Bien que la possibilité d'une hausse fulgurante du prix du bitcoin attire les spéculateurs, les périodes de forte baisse suivant l'éclatement d'une grosse bulle sur son prix seront cauchemardesques pour ses détenteurs dont l'objectif principal est de transférer des pouvoirs d'achat des biens et services vers le futur.

2.1.4. Droit de seigneurage :

Le droit de seigneurage représente une source de revenu important pour le budget de l'Etat. Par exemple, en 2016, la FED a versé 92 milliards de ses profits nets au gouvernement fédéral des Etats-Unis. En Europe, les profits nets de la BCE varient entre 10 et 30 milliards d'euros sur la période 2002-2015.

Les crypto-monnaies telles que le bitcoin privatisent les revenus de seigneurage. Pour l'instant, la création de bitcoins a enrichi énormément ses créateurs et des spéculateurs qui ont acquis les bitcoins à un prix dérisoire.

⁴⁰ Bulletin de l'Observatoire des Politiques économiques en Europe, Op.cit, P10.

Dans le système financier actuel, les banques commerciales privées réalisent aussi des revenus de seigneurage grâce à leur activité de création monétaire via les activités de crédits et de dépôts, qui sont à hauteur de 1% à 3% du PIB au Royaume-Uni et de 0,2% à 1% du PIB au Danemark selon des estimations. Toutefois, il y a un certain équilibre dans le partage des revenus de seigneurage entre les banques privées et la banque centrale. L'apparition de crypto-monnaie brise cet équilibre. Dans le cas extrême, où les monnaies souveraines sont entièrement remplacées par les crypto-monnaies qui ont pris une grande importance dans les échanges commerciaux et financiers, les Etats perdent leur droit de seigneurage et donc une part importante de leurs recettes. Si cela s'avère vrai, on peut anticiper que les Etats vont prendre, d'une manière ou d'une autre, le contrôle de la création des crypto-monnaies, pour récupérer ces revenus de seigneurage.

2.1.5. Stabilisation macroéconomique et financière :

Le bitcoin remplit mal les fonctions de moyens d'échange et de réserve de valeur associées à une monnaie. Le bitcoin par son principe de création et de fonctionnement, ne remplit pas la fonction régulatrice d'une monnaie officielle dans l'économie moderne.

En effet, une des raisons du remplacement de l'or par la monnaie fiduciaire est que sa production limitée ne suit pas le rythme de croissance de l'économie mondiale et génère de la déflation, à laquelle les économies ont du mal à s'adapter.

Un obstacle majeur que le bitcoin remplisse le rôle d'une monnaie régulatrice de la production et de l'inflation provient de ce que sa quantité est limitée ; conformément au principe fixé par ses promoteurs pour attirer des spéculateurs. Ce principe remet en cause son existence en tant que monnaie ayant un rôle régulateur de l'économie. L'ascension fulgurante de son cours depuis sa création implique un taux de déflation très important pour les prix des biens et services exprimés en termes de bitcoins. Relâcher la contrainte de limitation de la production de bitcoins enlèverait tout intérêt spéculatif de la crypto-monnaie et peut conduire à l'effondrement des désirs de détention exprimés par les spéculateurs et d'autres agents économiques.

Le bitcoin en tant qu'actif spéculatif souffre de l'inefficience des marchés sur lesquels il est échangé. Jusqu'à une date récente, il ne pouvait pas être vendu à découvert, et les dérivés financiers tels que les contrats à terme et les swaps qui sont routiniers pour d'autres devises ou actifs financiers n'existent pas pour le bitcoin. L'absence de ces outils

d'arbitrage permettant de corriger le mauvais fonctionnement du marché du bitcoin semble être l'explication de la facilité avec laquelle sont formées les bulles spéculatives spectaculaires sur le prix du bitcoin pendant plusieurs épisodes, ce qui amène certains à parler d'une chaîne de Ponzi.

Alors d'après cette analyse, le bitcoin a pour l'instant surtout des caractéristiques d'un actif très spéculatif avec la formation régulière de bulles spéculatives très exubérantes. Cette spéculation repose sur l'anticipation selon laquelle le bitcoin sera utilisé largement dans les transactions commerciales et financières, mais l'existence d'une telle spéculation remet en cause une généralisation de l'usage du bitcoin en tant que monnaie avec ses fonctions essentielles. Néanmoins, selon d'autres analyses, le bitcoin exerce certaines fonctions de la monnaie et constitue une révolution de celle-ci.

2.2. Le Bitcoin est une révolution de la monnaie :

D'après la Réserve Fédérale des États-Unis, pour mériter une telle appellation, une monnaie doit comporter six caractéristiques : la durabilité, la portabilité, la divisibilité, l'uniformité, une offre limitée, ainsi qu'une acceptabilité.

S'il n'est encore possible de payer en bitcoin que dans un nombre limité de commerces, il est permis de penser que l'actif numérique remplit les autres critères - en parvenant même à dépasser les monnaies fiduciaires sur ceux-ci.

Nous allons nous intéresser à cinq de ces caractéristiques -qui permettent de comprendre pourquoi le Bitcoin est venu, pour beaucoup, donner un nouveau souffle à la notion même de la monnaie.

2.2.1. Un bien durable :

Le Bitcoin offre aux utilisateurs la possibilité de devenir leur "propre banque" -un pouvoir qui suppose toutefois certaines précautions en matière de sécurité. En effet, l'actif a été conçu pour que seule la personne qui détienne la clé privée associée à un portefeuille puisse avoir le contrôle de celui-ci.

Alors que certains remplissent des valises de lingots d'or ou de billets, un utilisateur de Bitcoin va ainsi pouvoir "stocker" facilement autant d'argent qu'il souhaite sur une unique adresse. Et les coûts de stockage seront nuls, quelque soient les montants concernés - qu'il s'agisse de conserver un dollar ou un million de dollars de BTC.

Le concept de durabilité n'est donc plus pertinent, dans la mesure où l'argent est détenu sous une forme numérique, et que sa possession est enregistrée sur un réseau mondial d'ordinateurs.

2.2.2. Un actif facile à transporter et à envoyer :

Avec le bitcoin, c'est possible de transférer, en quelques minutes, n'importe quelle somme et sans faire appel à un tiers.

Avec les monnaies fiduciaires, c'est déjà compliqué. Les virements bancaires supposent des délais d'attente de plusieurs jours. Par ailleurs, il est impossible d'emporter à l'étranger plus de 10 000 euros en espèces (par exemple) sans déclarer ces sommes à la douane. Il faudra alors présenter les raisons pour lesquelles nous transportons une telle somme, sous peine d'avoir à payer de lourdes amendes. Le bitcoin contourne cet élément. Ce qu'il faut comprendre, c'est qu'il est, techniquement, impossible de "détenir" des bitcoins sur un smartphone ou un wallet hardware. Ces périphériques ne contiennent qu'une clé, qui offre à l'utilisateur un accès à ses fonds- ses BTC sont "stockés" sur le réseau Bitcoin, prêt à être utilisés dès qu'il en aura besoin.

L'utilisateur du réseau aura également la possibilité de mémoriser une simple "phrase secrète", qui lui permet de contrôler ses fonds dans le monde entier, à partir de n'importe quel ordinateur.

2.2.3. Le Bitcoin est très facilement divisible :

Même si l'or est divisible, le fait de scinder un lingot en 10, 100 ou 1000 unités est particulièrement compliqué. Il faudra de la patience, et disposer du matériel adéquat pour faire fondre ou couper le métal.

De son côté, le bitcoin peut être divisé en huit(8) décimales. La plus petite unité est Satoshi qui correspond à un centième de millionième de bitcoin.

2.2.4. Le Bitcoin est une "rareté numérique" :

Le Bitcoin est parvenu, en se prémunissant contre la fraude de la double-dépense, à introduire le concept de "rareté numérique". Avec une offre limitée à 21 millions, les participants peuvent avoir la (quasi-) certitude que personne ne parviendra jamais à créer artificiellement des bitcoins. Du côté des monnaies fiduciaires, la donne est toute autre, puisque ce sont les banques centrales qui décident de l'offre émise.

Afin de protéger les actifs de ses usagers, le réseau Bitcoin a été conçu pour empêcher une attaque potentielle. En effet, il faudrait disposer d'un pouvoir de calcul gigantesque pour pouvoir "pirater" le réseau.

Enfin, l'uniformité bitcoin peut être expliquée par le fait qu'un bitcoin est perçu comme étant totalement identique à un autre bitcoin.

2.2.5. Le Bitcoin est une monnaie décentralisée et apolitique :

Le Bitcoin est une technologie (un protocole) qui permet de transférer et de stocker de la valeur, au même titre que l'internet qui permet de transférer et de stocker des données.

Le Bitcoin offre à l'ensemble des individus la possibilité d'ouvrir un compte, et de bénéficier de services bancaires de base. Même si l'actif est décrié pour sa volatilité, de nombreux individus (au Zimbabwe, au Venezuela,...) semblent lui faire plus confiance qu'à la monnaie nationale, dont la valeur s'érode à cause de politiques monétaires inflationnistes.

Ainsi, le réseau Bitcoin est totalement neutre : les données ne sont pas traitées différemment selon la nature, la fonction ou l'histoire de la personne qui est à l'origine d'un transfert.

Aussi, le Bitcoin ne représente pas une technologie statique.

Certains diront que l'utilisation du Bitcoin est encore relativement complexe pour des néophytes. D'autres vont fustiger la lenteur et le coût du réseau. Mais comme pour toute technologie, il faudra sans doute patienter plusieurs années avant que le réseau ne puisse s'adresser à un public bien plus large. Aussi c'est possible que la croissance de son taux d'adoption soit bien plus rapide que celle de l'automobile, de l'aviation ou même des ordinateurs – en partie grâce à une infrastructure (internet) qui est déjà en place.

En conclusion, malgré les crashes et les arnaques qui émaillent sa courte histoire, malgré les critiques des économistes et des régulateurs, la crypto-monnaie résiste. Elle n'est pas devenue le concurrent du dollar que certains imaginaient, mais l'histoire n'est pas terminée.

Conclusion :

Les crypto-monnaies sont déjà aux portes de nos économies, Bitcoin à la tête, et tendent à révolutionner le monde. De plus en plus des petits commerces dans certains pays acceptent d'être réglés en bitcoin.

Du point de vue technologique, le Bitcoin est sans conteste une véritable innovation. En effet, la création d'unité monétaire par un algorithme mathématique limitée à un nombre défini dès sa création est un concept inédit. La décentralisation de la gestion de cette monnaie virtuelle est innovante. A l'évidence, l'utilisation du bitcoin ou d'autres monnaies virtuelles comparables apporte de nombreux avantages à ses utilisateurs, notamment en termes de simplicité et de coût de gestion.

Pour autant, le développement du Bitcoin n'est pas exempt de risque – intrinsèquement, le bitcoin apparaît comme une monnaie spéculative et donc volatile. A l'évidence beaucoup d'utilisateurs du bitcoin le considèrent davantage comme un possible bon placement que comme moyen de paiement, ce qui génère des bulles spéculatives.

De même, du fait de son caractère décentralisé, le bitcoin est considéré par certains comme facilitant certaines pratiques illégales telles que la fraude fiscale, le blanchiment d'argent ou le commerce de biens et services illicites.

Si le Bitcoin ne devait pas poursuivre son développement du fait de ces défauts intrinsèques, il demeurerait en tout état de cause le précurseur d'une véritable révolution monétaire basée sur les monnaies virtuelles.

Aujourd'hui, la société est plus complexe, la rapidité, la fongibilité, la sécurité de la monnaie sont plus nécessaires que jamais. Cependant, il ne faut pas faire l'erreur de croire que la définition actuelle de la monnaie ne peut pas changer, car les crypto-actifs peuvent déjà servir de monnaie à titre occasionnel. La seule question qui reste est la suivante : Deviendront-ils véritablement une monnaie aux yeux de tous ? Seul l'avenir nous le dira.

Conclusion

Générale

CONCLUSION GÉNÉRALE

L'évolution technologique, et surtout l'avènement de l'internet, a conduit à la création et à l'émergence d'une nouvelle forme de monnaie : la monnaie virtuelle ou digitale, baptisée aussi crypto-monnaie ou monnaie numérique. Les monnaies électroniques, sont créées à partir d'un protocole cryptographique de pair à pair, donc sans banque centrale, comme c'est le cas habituellement. Au sens strict du terme, il s'agit de monnaie privée. Les crypto-monnaies constituent une innovation en termes de combinaison des caractéristiques : ce sont à la fois des émissions privées, digitales et décentralisées. Les crypto-monnaies visent simultanément à changer les formes de la monnaie (en la détachant du système bancaire), à transformer sa nature (de publique à privée) et à révolutionner sa gestion (de centralisée à décentralisée).

L'engouement pour la nouveauté mêlé à la curiosité croissante face à cette monnaie d'un nouveau genre, a donné lieu à un foisonnement impressionnant de travaux, d'analyse, de commentaire et de débats. Or force, est de constater qu'un manque de clarté, si ce n'est une réelle confusion, règnent la plupart du temps dans les études sur le sujet et notamment sur le fait de considérer ou pas ce type de monnaie comme une monnaie à part entière.

En fait, le débat crypto-monnaie : monnaie ou non, dépend des fonctionnalités essentielles proposées dans la définition de la monnaie.

En effet, pour être considéré comme de la monnaie, selon l'école classique, il faut pouvoir remplir les trois fonctions :

- Agir comme moyen d'échange ;
- Etre une unité de compte ;
- Et pouvoir servir de réserve de valeur.

La crypto-monnaie, à la tête Bitcoin, a, dans une faible mesure, réussi à servir comme moyen d'échange car certains magasins ou commerçants les acceptent comme moyen de payer les transactions. Mais cette crypto-monnaie n'est pas parvenue à se placer sur un pied d'égalité avec les devises traditionnelles car le prix, par exemple, est encore souvent exprimé en devise de référence (dollar, euro). Comme le dit la Banque Nationale de Belgique (BNB), *"il n'existe pas pour l'argent virtuel de garantie légale qu'il puisse être échangé directement à sa valeur initiale"*. Les commerçants peuvent donc refuser d'être

payé en crypto-monnaie contrairement aux monnaies qui ont un "cours légal". En outre, le cours de la crypto-monnaie est souvent mis à jour, ce qui implique qu'une fois le montant encaissé, la transaction est souvent convertie en une autre devise traditionnelle. La raison est la grande volatilité de la valeur de la crypto-monnaie (bitcoin par exemple) et la nécessité pour les commerçants d'obtenir des revenus relativement stables.

La volatilité extrême des crypto-monnaies nous amène à la deuxième fonction, celle d'unité de compte. La valeur d'une monnaie doit être fixe afin que nous puissions exprimer les biens et services en unité monétaire ce qui n'est pas le cas pour la crypto-monnaie dont la valeur fluctue fortement par rapport aux monnaies traditionnelles.

La troisième fonction d'une monnaie est de pouvoir servir de réserve de valeur, qui n'est efficace que si la valeur de cette monnaie reste relativement stable, ce qui n'est pas le cas du Bitcoin et autres crypto-monnaies, qui ne sont donc pas des valeurs refuges.

La crypto-monnaie ne répond donc qu'à une seule des fonctions d'une monnaie, et encore, dans une très faible mesure. Sa forte volatilité la rend impropre aux rôles d'unités de compte et de réserve de valeur.

Aussi les positions des autorités monétaires internationales ne permettent pas de répondre clairement à cette problématique vu leurs divergences. La BCE considère le Bitcoin, comme une bulle plutôt que comme une potentielle concurrente de l'euro et pointe les risques de blanchiments de capitaux posés par le développement des crypto-monnaies. Des responsables de la Reserve Fédérale Bank (Fed) ont aussi exprimés des craintes sur le sujet, tandis que la BC de Singapour a recommandé aux investisseurs d'agir avec une extrême prudence vis-à-vis de cette nouvelle monnaie. Les réflexions s'orientent vers un besoin de légiférer pour en assurer la traçabilité.

Par opposition, à ce qui a été dit là-dessus, d'autres économistes pensent que le bitcoin et les altcoins sont une forme de monnaie ou qu'elles en deviendront dans le futur.

L'essence de la monnaie - non sa définition légale - est d'être un "pouvoir d'achat généralisé"

Cette définition de l'économiste français Pascale Salin dans son ouvrage *les systèmes monétaires* implique que *"la monnaie peut être échangée contre n'importe quoi, à n'importe quel moment et auprès de n'importe qui"*. De ce point de vue, la crypto-monnaie n'est évidemment pas une monnaie. Toutefois, Pascale Salin précise qu'aucune monnaie ne correspond parfaitement à cette définition : même un dollar ou un euro ne sera jamais

systématiquement accepté par n'importe qui, n'importe quand, n'importe où. Ce qui est important, d'après lui c'est donc la qualité monétaire des biens, certaines choses peuvent jouer plus ou moins le rôle de monnaie. Cela dépend de deux facteurs : leur capacité à conserver du pouvoir d'achat dans le temps et la taille de leur aire de circulation. De ce double point de vue, il est indéniable que la qualité du bitcoin se renforce globalement depuis sa création, même si, sur certaines périodes, elle peut se dégrader, par exemple quand son cours diminue fortement ou quand moins de commerces l'acceptent. D'après cela nous pouvons dire que le bitcoin, avec lui toutes les crypto-monnaies, est une "quasi-monnaie", ou une "monnaie en devenir" car nous pensons que sa qualité monétaire continuera de se développer dans les années qui viennent. Cela nécessitera que son cours se stabilise et que son usage se développe. Historiquement, les nouvelles formes de monnaie ont toujours mis beaucoup de temps à s'imposer, parfois des siècles.

Bien que cette monnaie perturbe des acteurs et des intérêts qui ont des moyens d'influence, de propagande et de coercition illimités à mobiliser contre lui pour ralentir son essor. Le chemin parcouru en dix ans par bitcoin est assez stupéfiant, d'autant plus qu'il a été créé et diffusé sans leader identifié, sans entreprise, sans budget, sans salariés, sans marketing, sans lobbying... d'une part, et d'autre part, nous vivons une époque où les changements permis par la technologie sont de plus en plus rapides, souvent même exponentiels et non seulement linéaires ; et Bitcoin bénéficie d'une forte externalité de réseau et d'un avantage de premier entrant sur le marché. En effet, le caractère décentralisé des crypto-monnaies favorise un rythme d'innovation technologique et financier sans commune mesure avec ce que l'on observe dans les systèmes financiers traditionnels.

En définitive, il faudra encore un peu de temps pour que nous puissions se faire une opinion précise sur l'avenir et la définition des crypto-monnaies mais, du fait de sa "plateformisation" et de son alternative décentralisée à la situation de monopole, certains pensent déjà que la notion même de monnaie éclate. Pour les libéraux, la monnaie est une chose trop importante pour être confiée à l'Etat.

➤ **Les difficultés rencontrées (les limites) :**

Comme tous les travaux de recherche, le mien contient un certain nombre de limites, nous citons essentiellement :

▪ **Difficulté du sujet :**

La première difficulté majeure que nous avons rencontrée dans ce travail a été

celle de travailler sur un sujet récent et peu connu, ou pas du tout surtout en Algérie. 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, même inexistante en Algérie. 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.

▪ **Ecueil de la répétition :**

Tout au long de ce mémoire il m'a 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.

▪ **Un peu de technique dans le travail de recherche :**

Nous ne pouvons pas éluder un peu de technique ou de science dans notre travail sachant que la crypto-monnaie en générale et le bitcoin en particulier, chef d'œuvre d'agencement de plusieurs idées, n'est pas proprement dit une révolution scientifique. Donc des explications techniques et un peu de vocabulaire, juste ce qu'il faut, sont nécessaires pour comprendre l'écosystème de ce nouveau-né avant de toute réflexion et de critique.

▪ **La stratégie de recherche adoptée s'appuyant uniquement sur l'étude théorique.**

Vu la nouveauté du sujet et de par le caractère innovant de la crypto-monnaie, il n'existe pas de situation empirique spécifique à étudier puisque la tendance de cette monnaie est globale.

A la fin de ce travail de recherche, notre mérite est que nous avons pu aborder, traiter et analyser le sujet de manière approprié, claire, et pu également apporter des éclaircissements concernant une forme de monnaie inédite. Bien que ce soit encore un thème qui demande.

Encore d'autres investigations qui laisse la porte ouverte à de plus ample travaux de recherche afin d'aborder des points qui n'ont pas fait l'objet de la présente étude mais également de confirmer ou infirmer nos premiers résultats. Nous espérons que ce travail soit

utile et pratique et d'une importance qui permettra aux autres de connaître au mieux la crypto-monnaie.

.

Bibliographie

Bibliographie

Ouvrage :

- AGLIETTA M. (1998) : " *Monnaie et Histoire- les univers des monnaies métalliques jusqu'à la première guerre mondiale*", Université de Paris.
- BASSINO J.P. (2000) : " *Monnaie et Finance*", Edition Fouché, Paris.
- BERGER I. A. (1995) : " *la monnaie et ses mécanismes*" collection Que sais-je ? Paris.
- BRANA S. CAZAL M. (2006) : " *la monnaie*", Ed° Dunod, Paris.
- BUSSAC E. (2018) : " *Bitcoin, Ether & Cie : guide pratique pour comprendre, anticipé et investir.*", Dunod.
- CHAUM D. (1983): "Blind signatures for Untraceable payments".
- COMBE F. TACHEIX T. (2001) : " *L'essentiel de la monnaie*" Gualino Editeur.
- CONDOMINAS G. (1989) : " *De la monnaie multiple* "Edition Communications.
- DE LAPLACE M. (2007) : " *Monnaie et financement de l'économie.*", Edition Dunod, Paris.
- DE MORGUES M. (2000) : " *Macroéconomie monétaire*", Edition Economica, Paris, 2000.
- DUMAS J.G. PASCAL la Fourcade. (2015) : " *Les crypto-monnaies, une réalité virtuelle*",Dunod.
- DUPRIEZ L. (1976) : " *la monnaie dans l'économie*", Edition Cujas.
- FIEVET C. (2014): " *Comprendre Bitcoin et les crypto-monnaies alternatives.*" Edition Lbrinova.
- GAILLY P.A. (2015) : " *Les nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux*», les éditions des journaux officiels.
- KEYNES J.M. (1973) : " *Théorie générale de l'emploi, de l'intérêt et de la monnaie* ",Edition MacMillan.
- LE LIERRE V. RAIMBOURG P. (1991) : " *la monnaie*", Edition Breal, Rome.

- LEVY P. (1998) : "*Qu'est-ce que le virtuel*", Edition La découverte.
- OTTAVI C. (2014) : "*Monnaie et financement de l'économie*", Edition Hachette, ParisCedex.
- PLIHON D. (2004) : "*la monnaie et ses mécanismes*", Edition la découverte, Paris.
- PRYPTO. (2018) : "*Bitcoin pour les nuls*", Edition First, Paris.
- QUOISTIAUX G. (2019) : "*Bitcoin et crypto-monnaie*", Edition MARGADA, Bruxelles.
- ROUSSEAU J.J. (1762) : "*Emile ou de l'éducation*" Edition A. Belin, Paris, 1762.
- RUMY M. (2004) : "*Économie Monétaire*", Edition Ellipses, Paris.
- SAY J.B. (1972) : « Traités d'économie politique », Paris, Calmann-Lévy.
- TAKKAL BATAILLE A. FAVIER J. (2018) : "*Bitcoin, la monnaie acéphale*", CNRS Editions.
- VOISIN M. (2014) : "*Comprendre la monnaie et les politiques monétaires*", Edition Bréal.

Revues, Périodiques et Rapports :

- Banque de France, Focus, "L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives" N°16 du 05 mars 2018, consulté sur (<http://publication.banque-france.fr>) le 05/11/2019.
- Bulletin de l'Observatoire des Politiques économiques en Europe, "*Le Bitcoin est-il une monnaie ?*", N°37, 2017, P8, consulté en ligne sur (unistra.fr) le 17/11/2019.
- CAMPBELL.C, "*le bitcoin en une leçon*", la revue libre d'agir publié le 05/09/2017, consulté en ligne sur (www.libredagir.fr) le 22/10/2019.
- CONOBAFI Newsletter N°1 (Comité Ouest Africain d'Organisation et de Normalisation Bancaire et Financière) rapport sur le bitcoin publié le 12 mars 2018 consulté en ligne sur (conobafi.org) le 30/10/2019
- DELAHAYE.J.P, "Le Bitcoin : la crypto-monnaie" revue Pour la science, N°434, Décembre 2013, en ligne consulté sur (www.pourlascience.fr) le 26/10/2019.
- DELAHAYE Jean-Paul, "Les preuves de travail" revue Pour la science, N°60, Avril 2014, en ligne consulté sur (www.pourlascience.fr) le 26/10/2019.
- DELAHAYE.J.P, "*les monnaies cryptographiques et les systèmes à blockchain*" consulté en ligne sur (inference-reviw.com) le 28/10/2019.

- DE MONTPELLIER.C," *Le Bitcoin est-il vraiment une monnaie ?*", publié le 28/05/2019 consulté en ligne sur (www.ing.be) le 25/11/2019.
- DESCAT.R, "*Monnaie multiple et monnaie frappée en Grèce*", Revue numismatique, 6e sérié, tome 157, année 2001, en ligne sur (<http://www.persee.fr/web/revue/home>) consulté le 22/07/2019.
- DZIRI "*crypto-monnaie. Pourquoi l'Algérie a interdit l'usage du Bitcoin*" publié en ligne le 21/05/2018 consulté sur (dziri-dz.com) consulté le 18/11/2019
- EL WATAN "*Les crypto-monnaies indésirables en Algérie* " publié en ligne le 12/02/2018 consulté
- Fondation d'Education Economique, *Histoire de la monnaie*, 1994, p4 en ligne (<http://www.moneyandyouth.cfree.org>) consulté le 22/07/2019
- FIGUET.J.M, "Bitcoin et blockchain : quelles opportunités ?" Revue d'économie financière,N° 123, 2016, consulté en ligne sur ([Cairn.info](http:// Cairn.info)) le 15/11/2019
- GOLDMAN.S, "*tout sur Bitcoin*", Global macro research, top of mind, N°21, mars 2011.
- Rapport de la BCE, "*les monnaies virtuelles*", publié en février 2015, consulté sur (www.ecb.europa.eu) le 31/07/2019.
- Rapport de Jean-Pierre Landau, Alban Genais,"*Les crypto-monnaies*", ministre de l'Economie et des Finances, du 04/07/2018, en ligne sur (<http://www.ladocumentationfrançaise.fr>) consulté le 01/08/2019.
- Rapport économique annuel 2018, P4 .consulté en ligne sur (www.bis.org) le 29/11/2019 (Bank for international settlements).
- Rapport BMO. Nesbitt burns Inc., "*Introduction au bitcoin et aux autres crypto-monnaies*", publié par la banque de Montréal, Canada, octobre 2017, consulté en ligne sur (www.nesbittburns.bmo.com) le 01/07/2019.
- Rapport annuel 2014 de Tracfin et un groupe de travail sur l'encadrement des monnaies virtuelles "*Recommandations visant à prévenir leur usage à des fins frauduleuses ou blanchiment*", Juin 2014, consulté sur (www.economie.gouv.fr) le 05/11/2019.

Thèses et Mémoires :

- AMEYE Hanane, AMEYE Lynda, «*les cartes électroniques comme substitut à la monnaie*»,Mémoire de fin d'études en vue d'obtention du diplôme de Master, option Finance, Université de Tizi-Ouzou UMMTO, 2014/2015.

- JONCHERES Erwan, «*Encadrement juridique des monnaie numérique* » Mémoire présenté à la faculté de Droit de l'Université de Montréal, en vue de l'obtention du grade LL.M, Maîtrise en droit des technologies de l'information, 2015

Sites internet :

- <http://nassimbelouar.com>. Blog de BELOUAR Nassim (Entrepreneur, formateur et consultant Blockchain). .
- <http://www.ses-nouilles.fr>. Blog De Cours En Economie.
- <http://www.triste.over-blog.com>. Blog De Cours En Economie.
- <http://www.alainbeitone.blogspot.com>. Blog d'Alain Beitone.
- <http://www.wikipedia.org>. .
- <http://www.cryptoactu.com>. .
- [http://www.Yaka Saider.fr](http://www.YakaSaider.fr)..
- [http : //www.fr.m.wikipedia.org](http://www.fr.m.wikipedia.org)..
- <http://www.e-gold.com>. .
- <http://www.bitcoin.org>. .
- <http://www.cryptoencyclopedia.com>..
- <http://www.coinmarketcap.com>. .
- <https://www.fr.slideshare.net>. .
- <http://www.lesechos.fr>. Blog les Echos.
- <http://www.journaldunet.com>.
- <http://www.latribune.fr>. .
- <http://www.economie.gouv.fr>..
- <http://www.alti-trading.fr>.
- <http://www.bitcoin.fr>.
- <http://www.conseilcrypto.com>.
- <http://www.crypto-France.com>.
- <http://www.fr.statista.com>.

- <http://www.blockchain.fr>.
- <http://www.coinlist.me/fr/altcoins/bitcoin>.
- <http://www.crypto-monnaie.pro>.
- <http://www.lockchain-expert.com>.
- <http://www.blockchain.com>.
- <http://www.blockchain-expert.com>.
- <http://www.cryptonaute.fr>.
- <http://www.blockblog.fr>.
- <http://www.bitnodes.fr>.
- <https://www.commonswikimedia.org>.
- <http://www.bloomerg.com>.
- <http://www.cryptofrance.com>.
- <http://www.cryptoast.fr>.
- <http://www.usbeketrica.com>.
- <http://www.coin.org>.
- <http://www.coicoin.com>
- <http://www.diskcoin.org>.

LE LEXIQUE :

A

Algorithme de consensus : protocole par lequel les nœuds d'un réseau blockchain arrivent à un consensus pour valider les transactions ou d'autres engagements sur la chaîne de blocs. Les algorithmes de consensus les plus souvent employés sont Pow (preuve de travail) et Pos (preuve d'enjeu).

Altcoin : crypto-monnaie alternative, un autre coin que le bitcoin.

B

Bloc : composant principal de la blockchain, un bloc est un regroupement de plusieurs transactions effectuées par les utilisateurs du réseau. Dans le cas de Bitcoin, la création d'un

nouveau bloc est faite par les mineurs qui résolvent des calculs compliqués et vérifient les transactions du bloc.

Blockchain : « chaîne de bloc ». La blockchain est une technologie qui permet de stocker des données numériques de manière décentralisée et sécurisée. C'est une sorte de registre en ligne qui contient tous les échanges effectués entre utilisateurs. Mis à jour en temps réel, ce registre est réputé infalsifiable grâce à un système cryptographique.

C

Clé privée : il s'agit du code secret (composé d'une longue suite de chiffres et de lettres) qui donne accès aux crypto-monnaies stockées. Pour éviter tout risque de piratage, il faut protéger ses clés privées grâce à un système de sécurisation en ligne ou via un appareil.

Coin : est une monnaie cryptographique, ou crypto-monnaie, un terme anglais qui veut dire pièce de monnaie.

Consensus : c'est un accord d'un groupe de personnes sur ce qui s'est passé, autrement dit sur la réalité perçue. Dans les crypto-monnaies, la réalité ce sont les transactions, le solde des comptes et éventuellement d'autres types de données. Une blockchain peut être vue comme un système d'établissement d'un consensus.

Contrat intelligent : c'est un protocole informatique qui peut être exécuté automatiquement, ou presque, *via* des outils numériques, notamment la blockchain. Alors c'est un programme informatique autonome qui exécute automatiquement les conditions et les termes d'un contrat.

D

Dapp : c'est une application décentralisée fonctionnant sur un réseau lui-même décentralisé (par exemple Ethereum). Elle est hébergée sur plusieurs ordinateurs à la fois et elle peut fonctionner même si une partie du réseau est endommagé ou inaccessible.

E

Exchange : ou place de marché, c'est un site permettant de vendre, acheter, envoyer, recevoir et stocker les crypto-monnaies.

F

Fiat : ou une monnaie fiduciaire, est une monnaie émise par un Etat ou un groupe d'Etats. Appelée aussi devise lorsque elle a une certaine envergure.

Fork : (bifurcation en français) est un événement qui se produit au sein d'une crypto-monnaie quand le consensus de la communauté qui participe à cette blockchain est rompu. Ceci arrive souvent lorsqu'une partie de cette communauté veut mettre en place des changements du protocole qui régit ladite blockchain et que l'autre partie refuse ces modifications. Un fork est alors nécessaire afin que ces modifications puissent être appliquées (renforcement de la sécurité, une augmentation de la taille des blocs ou un changement du nombre des coins émis par bloc ou au total. Il existe deux types de forks, un soft fork qui est une simple mise à jour, et un hard fork qui est la mise en place de changements importants dans la blockchain.

H

Hash : ou "somme de contrôle" ou "empreinte" est le résultat de l'application d'un logiciel de chiffrement à un message donné pour le sécuriser.

Hachage : (dans les crypto-monnaies) Le hachage est la technique cryptographique qui permet de valider et de sécuriser les transactions. Une fonction mathématique à sens unique qui transforme une suite binaire très longue en une suite de chiffres et de lettres bien courte.

I

ICO (Initial Coin Offering) : c'est une introduction en bourse version crypto-monnaie, une levée de fonds typique du secteur crypto qui vise à réunir des capitaux pour financer les start-up. A cette occasion un token (un coin) est créé, que les investisseurs peuvent se procurer pour participer à la campagne de financement.

M

Mining : (pour le cas de bitcoin) est l'opération par laquelle les transactions sont validées et de nouveaux bitcoins sont créés. Pour ce faire, les mineurs mettent à disposition du réseau les capacités informatiques de leurs puissantes machines.

N

Nœud : dans un système P2P, les nœuds sont simplement des ordinateurs reliés à d'autres, qui font partie du réseau. Ce sont donc des unités de calcul actives qui reçoivent, traitent, transmettent et renvoient les données aux autres nœuds.

O

Oracle : sont des pourvoyeurs d'informations professionnels, neutres et certifiés, qui récolte dans le monde réel un type bien précis d'informations et les entrent dans les réseaux de blockchain.

P

Pool : c'est un groupe d'individus qui minent des crypto-monnaies et s'organisent en pool afin d'être plus efficace et d'avoir plus de chance de toucher la récompense.

Proof of (Po) : c'est un algorithme qui fixe les règles de détermination du consensus d'une blockchain donnée.

Pos (Proof of Stake): preuve d'enjeu ou preuve d'intérêt ou encore preuve de participation, procédé alternatif à la preuve de travail selon lequel les mineurs (appelés ici masternodes : nœuds majeurs) devront prouver qu'ils possèdent une certaine quantité de crypto-monnaie pour pouvoir valider des nouveaux blocs dans la blockchain et prétendre à la récompense.

Pow (Proof of Work) : preuve de travail, méthode de validation des blocs basée sur la puissance de calcul.

S

SHA-256 : Dans le cas du Bitcoin, par exemple, le protocole est basé sur un algorithme de hashing (une fonction mathématique) qui s'appelle SHA-256.

SHA est une fonction qui, à partir d'un nombre donné (ou d'une suite de caractère) renvoie un hash, soit une très longue séquence de chiffres de 256 bits.

En fait, la séquence ci-dessus correspond à cette suite de 0 et 1. Si l'on change une seule lettre au message d'origine, on obtient un hash qui n'a absolument rien à voir avec le premier.

Notons que SHA-256 pourrait aussi bien être appliqué à un fichier entier

Stable coin : c'est un coin qui réplique la valeur d'un actif financier, comme une monnaie fiat, en faisant une valeur refuge pour les investisseurs qui veulent se protéger contre la forte volatilité du marché des crypto-monnaies sans en sortir, exemple de Tether qui réplique le dollar US.

T

Token : "Jeton numérique". C'est un actif numérique (représentation digitale de valeur) créé à l'occasion du lancement d'une ICO. Le token se voit attribuer une certaine valeur du projet faisant l'objet de l'ICO. Il ne peut pas être comparé à une action, il n'est pas corrélé à un droit de vote. Il a parfois une utilité future telle que acheter des biens ou services qui seront créés par la start-up.

W

Wallet : un portefeuille en ligne, c'est une application ou un périphérique qui gère les clés privées et donc les crypto-monnaies. Ils offrent plusieurs fonctions : afficher le solde des coins de ce portefeuille, créer des clés publiques et privées, envoyer et recevoir des coins, etc.

White paper : "Livre blanc". C'est le prospectus initial qui précède une ICO, document de présentation d'un projet de type blockchain ou crypto-monnaie. Il décrit l'objectif de l'ICO, le token qui sera émis, les éventuels droits liés au token, etc.

White List : Liste blanche, c'est une liste de personnes habilitées à participer à une ICO.

Tables des matières

TABLES DES MATIERES

INTRODUCTIONS GENERALE	10
------------------------------	----

Chapitre 01

Introduction	17
Section 01 : Histoire de la crypto monnaie	17
1. Histoire	17
2. Première apparition	19
3. Evolution	19
Section 02 : La crypto monnaie, une innovation fondée sur une combinaison de techniques préexistantes	19
1. Une base de données décentralisée	19
2. Le chiffrement à double clé	20
3. Hachage et protocole de consensus distribué.....	21
3.1. Les fonctions de Hachage.....	21
3.2. Le protocole de consensus distribué.....	22
Conclusion.....	23

Chapitre 02

Introduction	26
SECTION 1 : Les paiements de demain	27
1. Les nouveaux rôles de la monnaie.....	27
1.1. L'adaptation de la monnaie aux évolutions de la société :	27
1.2. Le défi de la décentralisation :	28
1.3. L'efficience des marchés :	29
1.4. La monnaie se dote d'une quatrième fonction :	29
1.5. Le contrôle de la monnaie :	30
2. Les nouveaux métiers.....	31
2.1. Mineur	31
2.2. Créateur de système de gestion de valeur fondé sur la blockchain.....	32
2.3. Emetteur de crypto-monnaie	32
2.4. Programmeur de blockchain	32
2.5. Programmeurs de contrats intelligents.....	32
2.6. Oracle (pourvoyeur d'information) :	33
2.7. Gestionnaire de blockchain(s) :	33

2.8. Spécialiste de la traçabilité des transactions sur blockchain :.....	34
3. Quel impact sur les paiements :	34
3.1. Le rôle des publics adresses (adresses publiques) :	34
3.2. La simplification et l'amélioration des paiements :.....	34
3.3. La traçabilité des paiements :	35
SECTION 2 :RISQUES ET LIMITES DES CRYPTO-MONNAIES	36
1. Trois caractéristiques des crypto-monnaies qui sont sources de risques :.....	36
1.1. Intervention d'acteurs non régulés :	37
1.2. Manque de transparence :	37
1.3. Extraterritorialité :	38
2. Risques associés à trois usages des crypto-monnaies :.....	38
2.1. Régler une transaction en crypto-monnaie :	38
2.2. Effectuer un transfert de fonds :	39
2.3. Investir dans des supports d'investissement en lien avec les monnaies virtuelles :	39
3. Risques d'utilisation des crypto-monnaies à des fins illicites :.....	40
3.1. Crypto-monnaies (crypto-actifs) vecteur de risque de blanchiment d'argent et de financement du terrorisme :	40
3.2. Crypto-monnaies vecteur de risque de cyber-attaques :	40
4. Autres menaces qui pèsent sur les crypto-monnaies :	41
4.1. La faible utilisation dans le monde réel :	41
4.2. Le manque de sécurité pour les utilisateurs :	41
4.3. La mauvaise réputation :	42
4.4. Les arnaques :	42
4.5. La menace pour l'environnement :	42
SECTION3 : LES PERSPECTIVES, RECOMMANDATIONS ET RÉGULATION	43
1. Les points clés du volet "Régulation et coopération" :	44
1.1. Réglementer les services offerts à l'interface entre la sphère réelle et les crypto- monnaies :	44
1.2. Encadrer les placements en crypto-monnaies :	45
1.3. Une coordination européenne et internationale :	46
2. Les points clés du volet "Encadrement de l'utilisation" :	46
2.1. L'anonymat des utilisateurs de monnaies virtuelles :	46
2.2. Les possibilités d'utilisation de la crypto-monnaie en tant que méthode de	

paiement anonyme :.....	47
2.3. Les flux espèces/crypto-monnaies :	47
3. Les points clés du volet "Encadrement de l'utilisation" :	47
Conclusion :	48

Chapitre 03

Introduction :.....	51
SECTION1 : BITCOIN, Première CRYPTO-Monnaie.....	52
1. Définition de BITCOIN :	52
1.1. Présentation :	52
1.2. Historique :	53
1.3. Acceptation du Bitcoin dans le monde :	55
1.4. Racines théorique de Bitcoin :	57
1.5. Principes de base de bitcoin :	59
2. Principes de fonctionnement :	59
2.1. Principes de création de Bitcoin :	60
2.2. Principe de fonctionnement de la blockchain Bitcoin :	60
2.3. Les principaux utilisateurs Bitcoin :	61
2.5. Transactions des BITCOINS :	63
2.6. Base de donnée Bitcoin et traçabilité :	64
SECTION 2 : Évolution de BITCOIN et son cadre juridique.....	64
1. Evolution de Bitcoin :	65
1.1. Le Bitcoin, une monnaie qui s'inscrit dans un processus de mondialisation :	65
1.2. Evolution du cours de bitcoin depuis sa création à ce jour (2009-2019) :	66
1.3. Evolution des transactions en bitcoins :	68
1.4. Distribution globale des nœuds Bitcoin :	72
2. Cadre juridique du Bitcoin :	74
2.1. Union européenne :	75
2.2. Etats-Unis :	75
2.3. Japon :	76
2.4. France :	76
2.5. Chine :	77
2.6. Corée du Sud :	77
2.7. Royaume-Uni :	77

2.8. Suisse :	78
2.9. Australie :	78
2.10. Russie :	78
2.11. Algérie :	78
2.12. Maroc :	79
2.13. Tunisie :	79
SECTION 3 : Débat au tour de BITCOIN.....	80
1. Avantages et inconvénients du Bitcoin :.....	80
1.1. Avantages allégués :.....	80
1.2. Risques allégués :.....	82
2. Bitcoin est-il une monnaie ?.....	83
2.1. Le Bitcoin n'est pas une monnaie :	84
2.2. Le Bitcoin est une révolution de la monnaie :	89
Conclusion :	91
CONCLUSION GÉNÈRALE	94
Bibliographie.....	100

Résumé

RÉSUMÉ

Depuis quelques années, nous assistons à l'émergence de monnaies d'un genre nouveau, reposant sur des procédés cryptographiques, gérées en pair à pair selon un consensus distribué : il s'agit des crypto-monnaies, dont la plus représentative est "le bitcoin» ; lancée après la crise financière de 2008. Le système des crypto-monnaies s'affiche clairement comme une alternative au capitalisme contemporain dont la dynamique est portée par une collusion Banques-Gouvernements. Aussi s'inscrit-il dans un mouvement de contestation des pouvoirs politiques et bancaires, qui ont été jugés incapables d'offrir une "monnaie de qualité". Les crypto-monnaies viennent alors heurter la conception traditionnelle de la monnaie unitaire, souveraine, territoriale et centralisée, mais aussi constituer un moyen de "démocratiser la finance" au sein d'espaces alternatifs (transnationaux) et restituer aux individus ce "bien commun" qu'est la monnaie. Par conséquent, dans ce mémoire nous proposons d'analyser la nature de la crypto-monnaie. Après avoir exposé les différentes définitions liées à cette monnaie et parler de son mode de fonctionnement, nous examinerons et nous étudierons la nature de ce nouveau-né (monnaie numérique) tout en présentant ses avantages, les risques auxquels elle expose ses utilisateurs, ainsi que son étendu juridique.

Toutefois nous apercevrons que le caractère disruptif de sa technologie, tout comme son potentiel d'innovation, font de la crypto-monnaie un objet d'étude stimulant des débats fondamentalement nouveaux dans l'histoire des idées monétaires. Les crypto-monnaies, si l'on admet que c'est un phénomène, est loin d'être parvenu à maturité, à tous les égards. L'immense majorité des gens sont donc encore dans une phase d'ignorance, d'apprentissage et de découverte.