REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
.....
Université Mouloud Mammeri de Tizi-Ouzou

Faculté des Sciences Economiques, Commerciales et des Sciences de Gestion

Département des Sciences Economiques

MEMOIRE
DE FIN D'ETUDES

En vue de l'obtention du diplôme de Master en Sciences Economiques

Option : Economie Monétaire et Bancaire

sujet

La Crypto-Monnaie : Emergence, Enjeux et Perspectives

Présenté par

M^me^ SIDHOUM Née DJAFER CHERIF Nacéra

Membres du jury

Président : Mr MOUSSAOUI Abdelhakim. M.C.A à l'UMMTO.

Examinatrice : Mme LARBES Maleha. M.A.A à l'UMMTO

Rapporteur : Mr GUENDOUZI Brahim. Professeur à l'UMMTO

Promotion : 2018-2019

Remerciements

Au premier lieu, je remercie le bon DIEU tout puissant, de m'avoir offert l'opportunité de franchir ce stade de savoir, et de m'avoir donné le courage et la patience de réaliser ce modeste travail.

Toute ma reconnaissance et gratitude vont à mon encadrant le Professeur GUENDOUZI Brahim, pour son sérieux, son dévouement, sa disponibilité et son aide précieuse.

J'adresse aussi mes vifs remerciements et ma profonde gratitude et reconnaissance à Mon Mari Mr SIDHOUM Kamel, pour son encouragement, son soutien et sa confiance. Sans lui je n'aurai pu faire ce Master.

Je remercie plus particulièrement BOUKHARI Sid Ali, sans lui je n'aurai pu avoir la documentation nécessaire pour accomplir ce travail.

Je tiens également à remercier Mme LARBES Melha et Mme MOHAND OUALI Radia pour leurs précieux conseils et leurs encouragements.

Ainsi je remercie les membres du jury qui m'ont fait le plaisir et le grand honneur d'évaluer ce travail.

Je ne saurai omettre de remercier très sincèrement tous les enseignants que j'ai eu l'honneur d'avoir durant mon cursus universitaire en post-graduation.

Je souhaite faire preuve de gratitude et de reconnaissance envers toutes les personnes qui ont contribué de près ou de loin à l'aboutissement de ce mémoire, en particulier : RAMDANI Nacéra, OUMOHAND Dihia, SLIMANI Ouiza, KHARROUB Hafidha et Ait Taleb Sabrina.

Dédicaces

Je dédie ce modeste travail :

A mes chers parents, à qui je souhaite une longue vie;

A La mémoire de ma belle mère et mon beau père, que leur âme repose en paix ;

A mon mari et mes chers enfants ;

A mes sœurs en particulier : Malika, Fatma et Souad ;

A leurs maris et enfants ;

A toute la famille SIDHOUM ;

A tous mes amis (es) et tous ceux qui ont cru en moi ;

A tous ceux qui auront l'accasion de lire ce modeste travail.

LISTE DES SIGLES ET ABRÉVIATIONS

ACCP:	**Acc**ise **P**roportionnelle
ACCS:	**Acc**ise **S**pécifique
ACPR:	**A**utorité De **C**ontrôle **P**rudentiel Et De **R**ésolution
ADA:	**C**ardano (crypto-monnaie)
AMF:	**A**utorité Des **M**arches **F**inanciers
BC:	**B**anque **C**entrale
BCE:	**B**anque **C**entrale **E**uropéenne
Bch:	**B**itcoin **C**ash (crypto-monnaie)
BNB:	**B**inance coin (crypto-monnaie)
BRI	**B**anque Des **R**èglements **I**nternationaux
BSV	**B**itcoin **S**ilver (crypto-monnaie)
BTC:	**Bitcoin** (crypto-monnaie)
CCP:	**C**omptes **C**ourants **P**ostaux
CFD:	**C**ontract **F**or **D**ifference (Contrat pour la différence)
DGX:	**D**i**g**i**x** **G**old (crypto-monnaie)
DLT:	**D**istributed **L**edger **T**echnology
DTS:	**D**roit De **T**irages **S**péciaux
ETH:	**Eth**ereum (crypto-monnaie)
Fevad:	**F**édération **E**-Commerce Et **V**ente **A** **D**istance
FMI:	**F**onds **M**onétaire **I**nternational
IBAN:	**I**nternational **B**ank **A**ccount **N**umber
ICO:	**I**nitial **C**oin **O**ffering
IFNB	**I**nstitutions **F**inancières **N**on **B**ancaires
IFB	**I**nstitutions **F**inancières **B**ancaires

IPO:	**I**nitial **P**ublic **O**ffering
LCB-FT:	**L**utte **C**ontre Le **B**lanchiment Et **F**inancement Du **T**errorisme
LTC:	**Litecoin** (crypto-monnaie)
MCDO:	**Ma**c **Do**nald's (crypto-monnaie)
NFC:	**N**ear **F**ield **C**ommunication (La communication en champ)
ONG:	**O**rganisations **N**on **G**ouvernementales
OPCVM:	**O**rganismes De **P**lacement **C**ollectif En **V**aleurs **M**obilières
PIB:	**P**roduit **I**ntérieur **B**rut
PIHR :	**P**rogramme D'**I**nvestissement A **H**aut **R**endement
Po:	**P**roof **o**f
POS:	**P**roof **o**f **S**tack
POW:	**P**roof **o**f **W**ork
P2P:	**P**eer **to P**eer (pair à pair)
SEPA:	**S**ingle **E**uro **P**ayements **A**rea (Espace de paiement en euro unifié)
TIC:	**T**echnologie De L'**I**nformation Et De La **C**ommunication
TRX:	**Tron** (crypto-monnaie)
TVA	**T**axe Sur La **V**aleur **A**joutée
UE:	**U**nion **E**uropéenne
US:	**U**nited **S**tates (Etats-Unis)
USDT:	**Tether** (crypto-monnaie)
XLM:	**Stellar** (crypto-monnaie)
XPP:	**Ripple** (crypto-monnaie)

SOMMAIRE

Introduction Générale

INTRODUCTION GÉNÉRALE

Très tôt dans l'histoire de l'humanité un medium 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 somme alors au tout début de la création du système monétaire dans une économie à monnaies multiples[1]. 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[2].

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[3]. 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 ce 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[4].

[1]Georges CONDOMINAS,"*De la monnaie multiple* "Edition Communications, 1989, p50.
[2]Raymond DESCAT,"*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
[3]Fondation d'Education Economique, *Histoire de la monnaie*, 1994, p4 en ligne (http://www.moneyandyouth.cfree.org) consulté le 22/07/2019.
[4]Ibid.

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* »[5].

Le contrôle des autorités centrales sur la monnaie, la crise des *subprimes* de 2007[6] 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 mena à la création de ces monnaies numériques et chiffrées, appelées crypto-monnaies, découle du mouvement libertarien 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

[5] Rapport de la BCE, les monnaies virtuelles, publié en février 2015, consulté sur (ww.ecb.europa.eu) le 31/07/2019.
[6] WIKIPEDIA,"*Crise des subprimes*" en ligne sur (http://www.wikipedia.org) consulté le 30/07/2019.

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 parfois des crises de confiance, comme celle issue de la crise financière de 2007qui 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[7].

Les crypto-monnaies sont crées pour s'échanger la valeur sur internet. Ces nouvelles monnaies sont fondées sur une nouvelle technologie : la blockchain. 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 dollars[8].

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 su 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.

[7] Erwan JONCHERES, «*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, Maitrise en droit des technologies de l'information, 2015, p9.
[8] 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.ladocumentationfrançaise.fr) consulté le 01/08/2019.

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, quelque 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 éloquents. Si à peine 5000 transactions étaient réalisées en bitcoin par jour en 2011, leur nombre étaient 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 volume a atteint 2.7 millions de BTC par jour[9].

Problématique

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

La crypto-monnaie, en tant que monnaie supranationale, pourra-t-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.

[9] Ressource Electronique, en ligne sur (http://www.cryptoactu.com) consulté le 15/09/2019.

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 1er 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 2ème objectif est de monter que les crypto-monnaies ne se limitent pas à des transactions douteuses et des variations de cours erratiques, derrières elles se cachent de vraies équipes avec de vrais projets et de nouveaux modèles.

Le 3ème 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 essaie 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 limites.

La structure du mémoire

C'est à partir des hypothèses et des questionnements que nous avons conçus, que nous allons entamer notre travail de recherche à travers un raisonnement et une argumentation qui seront développés et structurés en trois chapitres réalisés suivant un cadre théorique.

Chapitre1 : Le développement de la monnaie

Dans ce chapitre, nous allons nous introduire dans notre sujet en définissant la monnaie, et présentant ses différentes fonctions et formes. Nous tenterons d'expliquer en quoi consiste le système monétaire et de paiement actuel.

Chapitre2 : La genèse de la crypto-monnaie

Le 2éme chapitre sera consacré à l'émergence de la crypto-monnaie dans le cadre de la globalisation, innovation financière et la décentralisation de la monnaie. Nous verrons alors ce qu'est la crypto-monnaie de la façon la plus simple possible, son fonctionnement et les nouveautés qu'elle apporte par rapport aux monnaies classiques.

Chapitre 3 : Impacte de la crypto-monnaie, leurs enjeux et perspectives

Comme il arrive souvent, l'irruption d'une nouveauté radicale suscite un examen critique, pour cela, dans ce chapitre nous étudierons la question de la pérennité d'une telle monnaie décentralisée, ses enjeux mais aussi ses perspectives. Ainsi que les recommandations faites par des institutions nationales et internationales visant à les réguler.

Chapitre 4 : Bitcoin & Crypto-monnaie

Enfin et pour bien répondre à notre problématique, nous allons nous intéresser au modèle monétaire du Bitcoin, en étudiant plus particulièrement son intégration dans la sphère socio-économique actuelle. Nous présenterons les potentialités offertes par le Bitcoin et la possibilité de l'accepter comme moyen de paiement, les composantes de fiabilité de ce système monétaire mais aussi nous exposerons les dérives et risques associés à cette monnaie d'une façon qui nous permettra de déduire sa nature.

Chapitrel:

Le développement de la monnaie

CHAPITRE I : LE DÉVELOPPEMENT DE LA MONNAIE

INTRODUCTION

Les échanges constituent l'un des fondements de la société libérale dans laquelle nous évoluons. Sans transaction, nul ne serait en capacité aujourd'hui de satisfaire intégralement ses besoins. L'homme au fil du temps, n'a cessé d'échanger davantage et de plus en plus vite.

Progressivement, ces échanges ont été facilités par la mise en place d'outils pour aboutir à ce que nous appelons communément aujourd'hui la monnaie. Ces outils ont considérablement évolué, pour passer d'une logique de pluralité monétaire, à une logique d'unicité monétaire au sein d'un territoire défini.

La monnaie joue un rôle fondamentale dans la vie de la plupart des êtres humains, elle est présente dans de nombreux rapports entre les personnes, mais plus que ça, elle occupe une place importante dans leurs préoccupations quotidiennes.

Depuis l'avènement de la monnaie comme intermédiaire des échanges entre agents économiques, ses formes ont évolué. Ainsi, les métaux précieux (or, argent) ont été remplacés par les monnaies papiers convertibles en or qui elles mêmes, ont été remplacées (fin des accords de Bretton-Woods) par les monnaies fiduciaires émises par les banques centrales telles que nous les connaissons actuellement sous leurs formes physiques ou dématérialisées. La monnaie n'a donc pas de forme particulière mais évolue avec le temps. Le dénominateur commun est la confiance de la communauté des usagers qui confère à la monnaie une valeur d'échange permettant de conclure définitivement une transaction.

Dans ce chapitre, nous définissons, dans la première section, la monnaie en examinant ses fonctions et son évolution à travers ses différentes formes, ensuite, dans la deuxième section nous verrons la façon dont les banques et les autres institutions de dépôts créent la monnaie, tout en définissant en premier lieu la masse monétaire et ses outils de mesure. Enfin, nous allons étudier, dans la troisième et dernière section la composition du système monétaire et de paiement actuelle et le rôle de la banque centrale dans ce système ainsi que les différents usages, classiques et nouveaux de la monnaie au sein de ce système.

SECTION 1 : LA DÉFINITION DE LA MONNAIE

A la fois cause et solution de grande partie des malheurs humains, la monnaie a, paradoxalement, traversé les siècles sans qu'on arrive à lui définir ses contours de manière précise. Si l'utilisation d'objet pour faciliter les échanges remonte à des temps immémoriaux, l'invention de la monnaie sous sa forme scripturale et métallique, en Mésopotamie et en Lydie respectivement[10], a représenté un saut de l'esprit humain vers une abstraction de plus en plus poussée de la réalité qui l'entoure, processus que nous vivons encore aujourd'hui et que ne fait que s'accélérer, internet en est une preuve et un catalyseur.

L'apparition de la monnaie s'inscrivant ainsi dans un processus de virtualisation du rapport de l'homme au monde, la monnaie est virtuelle en son essence. Comme l'explique le philosophe Pierre Lévy :"*En tant qu'objet virtuel, la monnaie est évidemment plus facile à échanger, à partager et à mettre en commun que des entités plus concrètes*."[11]

Malgré sa nature par essence virtuelle, nous percevons la monnaie aujourd'hui comme quelque chose de bien réel et tangible, qui nous rassure lorsque nous la voyons incarnée sous sa forme fiduciaire.

1-Différentes définitions de la monnaie

La monnaie n'est pas simple à définir, car elle comporte plusieurs dimensions :

1-1 -Définition étymologique

Etymologiquement, la monnaie a pour origine le mot latin ***moneta***, qu'on peut traduire par "celle qui avertit" ou "celle qui donne son avis". ***Moneta*** était le surnom donnée à la déesse JUNON à qui on attribuait le pouvoir d'annoncer les événements à venir. Sur le capital de Rome un temple était dédié à cette déesse et on y frappait les pièces de monnaie. On finit par leur donner le nom de "***moneta***".[12]

1-2 -Définition économique

Selon R.Barré : « *la monnaie est un bien d'échange généralement accepté au sein d'une communauté de paiement* ».

[10] M. Aglietta,*" Monnaie et Histoire- les univers des monnaies métalliques jusqu'à la première guerre mondiale"*, Université de Paris, 1998, P5.
[11] P. Lévy, "*Qu'est-ce que le virtuel"*, Edition La découverte, 1998, P22.
[12] François Combe, Thierry Tacheix,"*L'essentiel de la monnaie*" Gualino Editeur, 2001, p.8

Pour A.Chaineau : « *la monnaie est constituée par l'ensemble des moyens de paiement. C'est-à-dire par l'ensemble des actifs acceptés par tout, par tous et en tout temps pour le règlement des dettes issues de l'échange.* »

La monnaie peut se définir comme tous moyens de paiement généralement acceptés par une collectivité pour une livraison de biens ou règlement d'une dette au sein d'un espace géographique donné.

Cette définition nous permet de comprendre que la monnaie n'est pas obligatoirement une pièce métallique ou un billet mais elle regroupe l'ensemble des moyens de paiement ayant pouvoir libératoire immédiat susceptible d'être rapidement transformé en moyens de paiement sans risque (liquide).[13]

On trouve chez Mathieu de MORGUES trois définitions[14]:

1-3 -Définition institutionnelle

« *La monnaie est l'instrument d'échange qui permet l'achat immédiat de tous les biens, services et titres sans coûts de transaction ni coûts de recherche et qui conserve la valeur entre deux échanges. C'est un phénomène social car elle repose sur la confiance des agents dans le système qui la produit* ».

1-4 -Définition fonctionnelle

« *La monnaie est par nature, l'instrument d'échange universel dont l'existence préalable est la condition de l'échange. Sa détention est rationnellement justifiée par la nécessité soit de rompre les relations de troc, soit de différer l'échange en situation d'incertitude*. »

1-5 -Définition se référant aux propriétés de la monnaie

« *Dans un monde dominé par l'incertitude et la peur du risque, la monnaie est le bien dont la valeur relative est la plus stable et qui présente une supériorité absolue sur les autres biens pour conserver le pouvoir d'achat en minimisant les risques. C'est la raison pour laquelle elle sera toujours acceptée dans l'échange contre n'importe quel bien*. »

[13] Bassino J.P,"*Monnaie et Finance*», Edition Fouché, Paris, 2000, p.12
[14] Mathieu de Morgues,"*Macroéconomie monétaire*", Edition Economica, Paris, 2000, p20-21

2- Les fonctions de la monnaie

Selon L.Dupriez : « *la monnaie se reconnait aux fonctions qu'elle exerce au sein de l'économie. Les fonctions déterminent la valeur d'usage de la monnaie* »[15].

Une manière d'appréhender la monnaie consiste à rechercher l'usage qu'on fait. Plus précisément, cette approche est ancienne, elle date de l'antiquité avec Aristote qui fut le premier à définir la monnaie selon ses fonctions. Celles-ci sont au nombre de trois :

2-1- Unité de compte (Etalon de valeur)

La monnaie est un bien qui permet de mesurer la valeur des biens et services et remplit ainsi la fonction d'unité de compte. C'est donc le bien qui sert d'**étalon de mesure** de la valeur de tous les autres biens et services[16].

Le rôle d'unité de compte est celui de la monnaie comme instrument de mesure de la valeur relative de bien hétérogène. Il arrive que la monnaie soit réduite à cette unique fonction d'étalon de valeur, c'est le cas du Franc français avec l'instauration de l'Euro[17].

L'étalon de mesure veut dire que la monnaie permet de donner, au moyen du prix, une valeur à tout bien ou service échangeable sur un marché.

Chaque bien et service est évalué par un prix d'échange qui représente la quantité de monnaie qu'un individu doit fournir pour son acquisition.

2-2- Instrument de paiement (Intermédiaire d'échange)

C'est certainement la fonction la plus connue de la monnaie. Comme instrument des échanges, la monnaie a pour rôle de fournir une contrepartie aux flux de biens et services[18].

Avec ce rôle de moyen de paiement, elle sert au règlement d'un achat ou à l'extinction d'une dette, on dit que la monnaie a un pouvoir libératoire[19].

Pour J.B.SAY (1803) :" *La monnaie dans son rôle d'intermédiaire facilite les échanges, et en circulant elle- même elle permet aux biens de mieux circuler* "[20].

---

[15] L.Dupriez,"*la monnaie dans l'économie*", Edition Cujas, 1976, P.52.

[16] François Combe, Thierry Tacheix, Op.cit, P30.
[17] Sophie Brana, Michel Cazals,"*la monnaie*", Ed° Dunod, Paris, 2006, P.19.
[18] François Combe, Thierry Tacheix, Op.cit, P30.
[19] Sophie Brana, Michel Cazals. Op.cit, P.20.
[20] JB Say (1803), « Traités d'économie politique », Paris, Calmann-Lévy, 1972, p.138.

La monnaie est un bien directement échangeable contre tous les autres biens, un instrument de paiement permettant d'acquérir n'importe quel bien ou service et elle représente un actif liquide[21], elle est un instrument de règlement d'une transaction ou d'une dette. Donc la monnaie élimine les coûts de transaction car elle permet d'éviter ceux afférents à la recherche de partenaires, à l'attente et au transport, et elle définit pour chaque bien une valeur précise.

Plus généralement avec cette fonction, la monnaie doit être définit comme un moyen de règlement :

- **Indéterminé :** C'est-à-dire qui permet d'acquérir n'importe quel bien ou service et de régler n'importe quelle dette.
- **Général :** C'est-à-dire admit partout dans le monde et en toutes circonstances dans un espace donné, ou dans une communauté de paiement.
- **Immédiat :** c'est-à-dire que le simple transfert de cet instrument de paiement entraine d'une manière définitive l'extinction de la dette[22].

2-3- Réserve de valeur (Instrument de réserve)

Selon J.M. KEYNES : « *L'importance de la monnaie découle essentiellement du fait qu'elle constitue un lien entre le présent et le futur* »[23].

La troisième fonction de la monnaie est de servir de réserve de valeur car elle permet de dissocier dans le temps la vente d'un bien de l'achat d'un autre. Plus précisément, la monnaie devient l'instrument par excellence grâce auquel les agents économiques aménagent leur décisions par rapport au présent, au passé et à l'avenir. Elle confère un pouvoir de rétention qui s'étale dans le temps et qui s'exerce librement au moment le plus opportun. Pour DOSTOIEVSKY, « *la monnaie est la liberté de frappée* ».

Cette fonction de réserve de valeur évolue en fonction de l'inflation, c'est-à-dire l'augmentation du niveau général des prix. En période de hausse de prix le pouvoir d'achat de

la monnaie baisse, ce qui dégrade sa capacité à être une réserve de valeur.

En cas d'hyperinflation la monnaie n'assure plus du tout cette fonction[24].

[21] C'est la capacité d'un actif à être aisément transformable en moyen de paiement sans perdre de la valeur.
[22] Valerie le lierre, Raimbourg Philipe, "*la monnaie*", Edition Breal, Rome, 1991, p.33.
[23] J.M.Keynes, " *Théorie générale de l'emploi, de l'intérêt et de la monnaie* ", Edition MacMillan, 1973, p.295.
[24] François Combe, Thierry Tacheix, Op.cit, P32.

En plus de ces trois fonctions économiques traditionnelles de la monnaie, d'autres fonctions peuvent lui être attribuées :

2-4- Autres fonctions de la monnaie

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 d'autres fonctions[25] :

2-4-1-La monnaie est un langage

Elle est un langage car elle permet à tous les individus de partager les mêmes références et les mêmes règles car le langage de la monnaie est universel. Par exemple l'Euro est une forme d'identité (monétaire certes) européenne partagée (voulu ou non) par chaque agent économique.

Elle leur permet de communiquer, si un bien est cher, cela a une ou plusieurs significations :

- ✓ cela peut vouloir dire qu'il est précieux, recherché ou que sa demande est supérieure à son offre.
- ✓ Qu'il est rare, ou que son offre est insuffisante par rapport à sa demande.

2-4-2- La monnaie a une fonction politique

Une fonction même politico-sociale car elle permet d'unifier un territoire, de pacifier les échanges économiques et donc les relations et d'asseoir le pouvoir en place (à l'époque où les Rois frappaient la monnaie à leur effigie) ou celui d'une institution comme par exemple l'Euro pour l'Europe. La monnaie permet donc l'intégration sociale par l'intégration économique[26].

En conclusion, sera monnaie l'objet économique qui remplira simultanément ces trois fonctions d'unité de compte, moyen de paiement et réserve de valeur. Si l'une venait de manquer, il ne s'agirait plus de monnaie proprement dite.

3- Les formes de la monnaie

La réflexion sur les formes de la monnaie passe par un détour historique qui permet d'éclairer la réalité actuelle de la monnaie.

[25] Blog De Cours En Economie disponible sur http://www.ses-nouilles.fr (consulté le 06/10/2019).
[26] Blog De Cours En Economie disponible sur http: //triste.over-blog.com (consulté le 06/10/2019).

En effet, la monnaie est essentielle au fonctionnement d'une économie moderne mais sa nature a sensiblement varié au fil du temps. Les agents économiques ont cherché à concevoir des instruments monétaires plus faciles d'utiliser.

Dans l'histoire, la monnaie a pris différentes formes :

3-1-Les formes historiques

3-1-1-Le troc

Le troc est le terme qui définit un échange sans compensation monétaire. Son origine étymologique est peu claire, il viendrait de l'ancien français ***"Troche"*** signifiant faisceau.

Ce sont les civilisations les plus anciennes qui ont commencé à utiliser le troc pour échanger. L'Egypte ancienne notamment ou des peuples amérindiens n'ayant pas encore de monnaie, échangeaient des biens afin de pouvoir obtenir ce dont ils avaient besoin. L'économie est basée donc sur le troc[27]**.**

Le troc est un moyen d'échange qui permet d'acquérir un bien contre un autre bien. En effet, pour qu'il y ait échange, il est nécessaire que les individus se déplacent afin de satisfaire la double coïncidence des désirs d'échange. Mais au-delà de cette double coïncidence, un accord relatif aux quantités à échanger doit être établi pour chaque échange. Ainsi, pour chaque échange, les individus doivent s'entendre *à priori* sur les valeurs d'échange respectives de leurs biens.

La préférence des individus pour le troc est expliquée par le fait que la monnaie n'est pas nécessaire pour effectuer leurs échanges.

Mais rapidement le troc va poser des problèmes :

- Problème de conservation : on ne garde pas indéfiniment des denrées alimentaires ;
- Problème de transport : volume, facilité, usure ou fatigue (cas d'animaux) des biens à troquer ;
- Impossibilité dans certains cas de fractionner le bien à échanger ;
- La qualité de la marchandise varie ;
- Risque de conflit.

[27] Yaka Saider.fr (consulté le 09/10/2019)

Le troc va donc laisser la place à un autre moyen d'échange, même s'il n'a pas complètement disparu à l'heure actuelle[28].

3-1-2-La monnaie marchandise

Pour remédier aux inconvénients de troc, il fallait trouver un moyen d'échange intermédiaire, c'est-à-dire un bien dont la valeur est généralement connue et admise de tous, de consommation courante et de conservation aisé comme les coquillages en Polynésie, le sel en Abyssinie ou les têtes de bétail dans le bassin méditerranéen.

La monnaie marchandise permettait donc de remplir déjà deux fonctions de la monnaie :

- ✓ Fonction d'instrument d'échange : permet d'acquérir un bien ;
- ✓ Fonction d'instrument d'épargne : a de la valeur et peut se conserver[29].
- ✓ Les outils donc ont constitué les premières formes de monnaie. Mais la monnaie marchandise utilisée pour les transactions présentaient de nombreuses limites : comparaison de valeur, les biens entre eux aléatoires, transport et conservation difficiles, etc.

La monnaie a pris donc d'autres formes plus pratiques et plus *"normalisées"*. Ce fut le recours aux métaux précieux et le début du monopole de l'Etat sur l'émission de la monnaie.

3-1-3-La Monnaie métallique (les métaux précieux)

La monnaie métallique emploie dans un premier temps le fer, le cuivre et le bronze puis les métaux précieux comme l'or et l'argent sous forme de lingots pesés lors de chaque transaction d'échange, ou de pièces. Les premières pièces sont frappées par les Lydiens en Asie Mineure par la suite, le recours aux pièces métalliques se répond en Grèce, puis sous la Rome Antique et se développe également en Chine cinq siècles A.J.C.

Cette évolution se poursuit jusqu'au XIX^{e} siècle où l'essor du capitalisme s'inscrit dans un système bimétallique (or et argent) prolongé par le système d'étalon –or, par la suite de nouvelles formes de monnaie apparaissent[30].

Cette forme de monnaie aussi représente des inconvénients :

- Perte de temps (il fallait chaque fois peser avant d'échanger) ;

[28] Marie de Laplace, *«Monnaie et financement de l'économie.», Edition* Dunod, Paris, 2007, p.8-9
[29] Ibid., p.18.
[30] François Combe, Thierry Tacheix, Op.cit, p33-34.

- C'était lourd et peu maniable ;
- Assez facile à falsifier ;
- Altération au fur et à mesure des échanges[31].
- Les formes marchandise et métallique de la monnaie ne sont plus utilisées dans nos économies.

3-2-Les formes actuelles

Nous distinguons aujourd'hui trois formes de monnaie :

3-2-1-La monnaie fiduciaire

Elle comprend, d'une part la monnaie divisionnaire matérialisée par des pièces de monnaie, et d'autre part les billets de banque. Son utilisation repose sur la confiance accordée par les utilisateurs dans les institutions qui l'émettent. Le mot fiduciaire vient du latin "***fiducia"*** qui signifie confiance. On nome également cette forme de monnaie de la "monnaie manuelle" car sa circulation se fait de main en main.

A- La monnaie divisionnaire (les pièces métallique)

Elle est constituée de pièces émises par le trésor public et mises en circulation par la Banque Centrale. Cette monnaie est parfois considérée comme une forme dégénérée des anciennes pièces d'or et d'argent.

Ses avantages sont :

- Stockage et conservation aisés ;
- Rareté relative ;
- Inaltérabilité (elles peuvent ne pas être modifiées).

Mais d'un pouvoir libératoire limité, on ne peut régler des sommes importantes exclusivement en pièces, elles sont utilisées pour les échanges de faibles montants.

B- Les billets

Les billets appelés aussi papier-monnaie, composée de l'ensemble de billets émis par la Banque Centrale, leur valeur est fortement dépendante de degré de la confiance accordée par les porteurs de billets.

[31] Marie de Laplace, Op.cit, p18

La monnaie fiduciaire avait cependant quelques inconvénients :

- Encombrement : les pièces sont lourdes, difficiles à transporter pour de long voyage ;
- Risque de perte ou de vol ;
- Leur valeur est limitée par rapport au développement de plus en plus important de commerce.

La monnaie fiduciaire a un pouvoir libératoire illimité : elle donne la possibilité de se libérer d'une dette avec une quantité de monnaie, dans un espace géographique donnée[32].

3-2-2 La monnaie scripturale

La monnaie scripturale est une dette du système bancaire à l'égard des particuliers.

A- La nature de la monnaie scripturale

La monnaie scripturale ou encore la monnaie de banque, vient du latin ***"scriptum"*** qui signifie écriture, c'est donc une monnaie d'écriture. Elle est constituée par les sommes inscrites sur les comptes à vue ou dépôts détenus auprès des intermédiaires financiers. Ces dépôts sont des créances détenues par les agents non financiers sur le système bancaire. Ces comptes bancaires ou comptes courants peuvent prendre la forme de comptes ouverts dans les banques commerciales ou comptes chèques postaux. Les sommes qui y sont inscrites sont directement utilisables pour régler les dettes.

Le développement de la monnaie scripturale s'explique par le fait qu'elle présente un triple avantage par rapport aux monnaies fiduciaires :

- Elle permet le règlement d'échange sans déplacement physique des personnes ;
- Elle offre des garanties plus fortes contre la perte ou le vol ;
- Elle entraine des écritures dans la comptabilité bancaire qui sont sources de preuves en cas de contestation.

La monnaie scripturale est une écriture comptable qui circule dans l'économie grâce à plusieurs instruments de paiements.

[32] Rumy Michel, *" Économie Monétaire"*, Edition Ellipses, Paris, 2004, p15.

B- Les instruments de circulation de la monnaie scripturale

La monnaie scripturale circule entre les agents économiques à l'occasion des paiements. Il existe plusieurs instruments qui servent à transférer la monnaie scripturale d'un compte à un autre. Ils représentent les instruments de mobilisation de la monnaie scripturale. Parmi ces instruments nous citons :

❖ **La lettre de change :** appelée également traite, est un écrit par lequel le créancier (le tireur) ordonne au débiteur (le tiré) de lui payer une certaine somme à une échéance déterminée, le créancier peut, par le procédé de l'endossement, la transmettre à une tierce personne[33].

❖ **Le billet à ordre :** est un écrit par lequel un débiteur (le souscripteur) s'engage à payer au bénéficiaire une certaine somme à une échéance déterminée, la mention "à ordre" rend le billet endossable et lui permet de circuler entre plusieurs intervenants[34].

La lettre de change et le billet à ordre sont de moins en moins utilisés au profit des instruments suivants[35]:

❖ **Le chèque :** c'est un ordre de paiement écrit qu'une personne physique ou morale, appelée le tireur, et détentrice d'un compte en banque remet à une autre personne, appelée bénéficiaire, pour payer un achat ou régler une dette. L'établissement bancaire qui gère le compte du tireur du chèque est le tiré.

❖ **Le virement bancaire :** il consiste à opérer le transfert de fonds à l'initiative du débiteur sans intervention du créancier.

❖ **L'avis de prélèvement automatique :** il est à l'initiative du créancier qui opère un prélèvement dans le cadre d'une autorisation donnée par le titulaire du compte. Cet instrument est utilisé pour le paiement des impôts et de certaines factures.

❖ **Le titre interbancaire de paiement (TIP) :** le débiteur donne son accord pour le paiement de chaque opération mais le titre fait ultérieurement l'objet d'un traitement informatique.

❖ **La carte de paiement (ou carte bancaire ou encore carte de crédit):** est l'instrument le plus dématérialisé. Lors de paiement, les coordonnées bancaires du payeur sont saisies par lecture d'une piste magnétique de sa carte. Elle permet de pouvoir automatiquement débiter

[33] François Combe, Thierry Tacheix, Op.cit, p39.
[34] Ibid. p40.
[35] Ibid. p.41.

son compte et créditer celui du bénéficiaire de façon immédiate ou différée selon le type de contrat qui lie la banque et le détenteur de la carte.

La monnaie scripturale peut présenter des inconvénients tels que :

- Le facteur temps pour la réalisation des opérations de paiement et d'encaissement, qui sont parfois lentes ;
- Le processus est parfois complexe et coûteux.

3-2-3-La monnaie électronique ou la monétique :

L'apparition des nouvelles technologies de l'information et de la communication (TIC) comme le **minitel**[36] et l'internet autorise le développement d'une nouvelle forme de monnaie**.** Celle-ci constitue la troisième mutation en matière de modes de paiement.

La monnaie électronique correspond à l'ensemble des techniques informatiques, magnétiques et télématiques assurant le transfert de sommes d'un compte vers un autre sans recourir à un support papier.

La monnaie électronique est une solution de rechange numérique à l'argent comptant. Il s'agit d'une valeur monétaire stockée sous une forme électronique par divers moyens, comme un téléphone portable, une tablette, une carte sans contact (ou une carte à puce), un disque dur ou un serveur, et transférable par voie numérique.

Ce système repose sur un chargement, par un émetteur, d'unités électroniques sur le microprocesseur d'une carte contre le débit du compte du porteur.

Alors que les monnaies fiduciaires et scripturales sont matérielles, la monnaie électronique est virtuelle. Si la monnaie traditionnelle est parfaitement palpable, la monnaie électronique ne permet plus de savoir, sauf à recourir d'un lecteur adéquat, quelle somme est stockée dans la puce.

Les cartes prépayées, qui fonctionnent grâce à des réseaux de paiement comme Visa ou MasterCard, et les soldes de comptes administrés par des fournisseurs comme PayPal constituent des formes de monnaie électronique. Toutes deux peuvent servir à régler divers achats dans de multiples commerces.

[36]Minitel est un terminal informatique compatible avec la norme vidéotex (affichage de 25 lignes de 40 colonnes, et en 80 sur certains modèles) équipé d'un clavier, d'un écran de visualisation et d'un modem incorporé.

D'autres monnaies électroniques sont décentralisées, dans le sens où elles sont dépourvues d'un émetteur particulier, et la valeur n'est pas exprimée dans une quelconque monnaie nationale.la plus connue d'entre elles est **le bitcoin[37],** une monnaie virtuelle servant à effectuer des transactions directes entre des usagers reliés par un réseau informatique.

Certaines personnes apprécient la monnaie électronique parce qu'elles la considèrent comme un moyen de paiement rapide, commode et confidentiel à l'instar de l'argent comptant.

La monnaie électronique répond aux besoins des consommateurs qui désirent préserver la confidentialité de leurs renseignements personnels ou bancaires lorsqu'ils font des achats en ligne.

Dans la vie de tous les jours, certains préfèrent utiliser de la monnaie électronique plutôt que de devoir transporter et compter des billets de banque et des pièces de monnaie. Les commerçants, quant à eux, sont à même de réaliser des économies, car ils n'ont plus à rendre la monnaie ou à traiter des espèces.

Les progrès techniques contribuent aussi à stimuler l'innovation.par exemple, l'adoption généralisée d'Internet et des téléphones intelligents a rendu possible la création de monnaie électronique grâce auxquelles les détaillants et les consommateurs peuvent se passer des lecteurs de cartes, des terminaux et d'autres dispositifs liés à l'infrastructure de paiement.

SECTION 2 : LA MASSE MONÉTAIRE ET LA CRÉATION DE LA MONNAIE

La monnaie est un instrument indispensable à l'activité économique puisqu'elle facilite les transactions entre les agents économiques et elle permet d'effectuer un paiement immédiat.

Les besoins des agents économiques de ces moyens de paiement entrainent un besoin de création monétaire. Créer la monnaie signifie mettre en circulation une nouvelle quantité de monnaie qui entraine un accroissement de la masse monétaire.

[37] A revoir d'une manière détaillée dans chapitre 4.

1-La masse monétaire

1-1 -la définition de la masse monétaire

La masse monétaire regroupe l'ensemble de la monnaie détenue par les ménages, les entreprises et administrations publiques (Etat) dans un pays ou une zone monétaire.

La masse monétaire représente la quantité de la monnaie qui circule dans l'économie à un moment donnée. Celle-ci est mesurée grâce à des indicateurs statistiques (agrégats) qui sont fixés par la Banque Centrale Européenne (BCE). Cela correspond à tous les moyens de paiement qui peuvent être transformés en liquidité.

Elle est composée de l'ensemble des billets, des comptes de dépôts et de tous les placements que l'on peut transformer en liquide.

1-2 -La contre partie de la masse monétaire

La contre partie de la masse monétaire constituent la source de la création monétaire au profit des agents non financiers. On distingue trois contre parties de la masse monétaire :

- **Les avoirs extérieurs nets** : mesure l'incidence sur le stock de la monnaie des transactions courantes et en capital entre les agents non financiers résidents et les non résidents.
- **Les créances nettes sur l'Etat** : retrace l'endettement net de l'Etat vis-à-vis du système bancaire dans son ensemble.
- **Les crédits à l'économie** : décrit les financements accordés aux agents économiques non financiers par les établissements de crédit.

1-3 -La composition de la masse monétaire

Pendant une longue période, la monnaie était exprimée en fonction d'une certaine quantité de métaux précieux selon le bimétallisme ou le monométallisme. La masse monétaire était égale aux réserves métalliques dans les coffres des banques centrales, système qui a définitivement disparu.

De nos jours, les composantes de la masse monétaire sont des agrégats :

1-3-1-Définition des agrégats

Sont des indicateurs statistiques regroupant dans des ensembles homogènes les moyens de paiement détenus par les agents d'un territoire donné[38].

Les agrégats sont des grandeurs statistiques mesurant la quantité de monnaie en circulation dans l'économie. Ils sont définis par les autorités monétaires.

En d'autres termes, un agrégat est une catégorie de monnaie et d'actifs liquide représentant une mesure comptable de monnaie en circulation mise à la disposition des agents non financiers pour assurer l'ensemble de leurs transactions.

1-3-2-La construction des agrégats monétaires

Pour définir les agrégats monétaires, il convient de distinguer les actifs monétaires[39] des actifs non monétaires[40].

Les catégories d'actifs retenus sont déterminées en fonction de leur caractère monétaire ou leur degré de liquidité[41], cette mesure dépend des critères fondamentaux suivants :

- **La transférabilité :** la possibilité de transférer des fonds placés dans un actif en ayant recours à des instruments de paiement comme le chèque, le virement,…
- **La convertibilité :** la possibilité de convertir un actif financier en numéraire ou en compte à vue à moindre coûts.
- **L'échéance :** permet de distinguer entre les actifs par rapport à l'intervalle de temps entre la date de contrat et celui de remboursement.
- **Le délai préavis :** c'est l'intervalle de temps entre le moment de la demande de conversion et la date à laquelle il est autorisé à convertir l'instrument en liquidité.

Les agrégats sont classés par degré de liquidité et l'économie retient ceux suivants :

- **M_0 (la base monétaire) :** représente la monnaie fiduciaire émise par la BC, elle comporte les billets et pièces (B_0) + les réserves (R) des banques ordinaires placées au niveau de la BC. **$M_0 = B_0 + R$.**

[38] WIKIPEDIA en ligne sur (http : //www.fr.m.wikipedia.org) consulté le 11/10/2019.

[39] C'est des actifs tangibles, ce sont les formes monétaires et les supports monétaires dont l'utilisation dans l'échange n'exigent aucune conversion ou transformation préalable.il s'agit de la monnaie manuelle et monnaie scripturale.

[40] C'est des éléments d'actif dont la valeur exprimée en unités monétaires est variables, tels que les stocks, les placements en actions et les immobilisations corporelles et incorporelles.

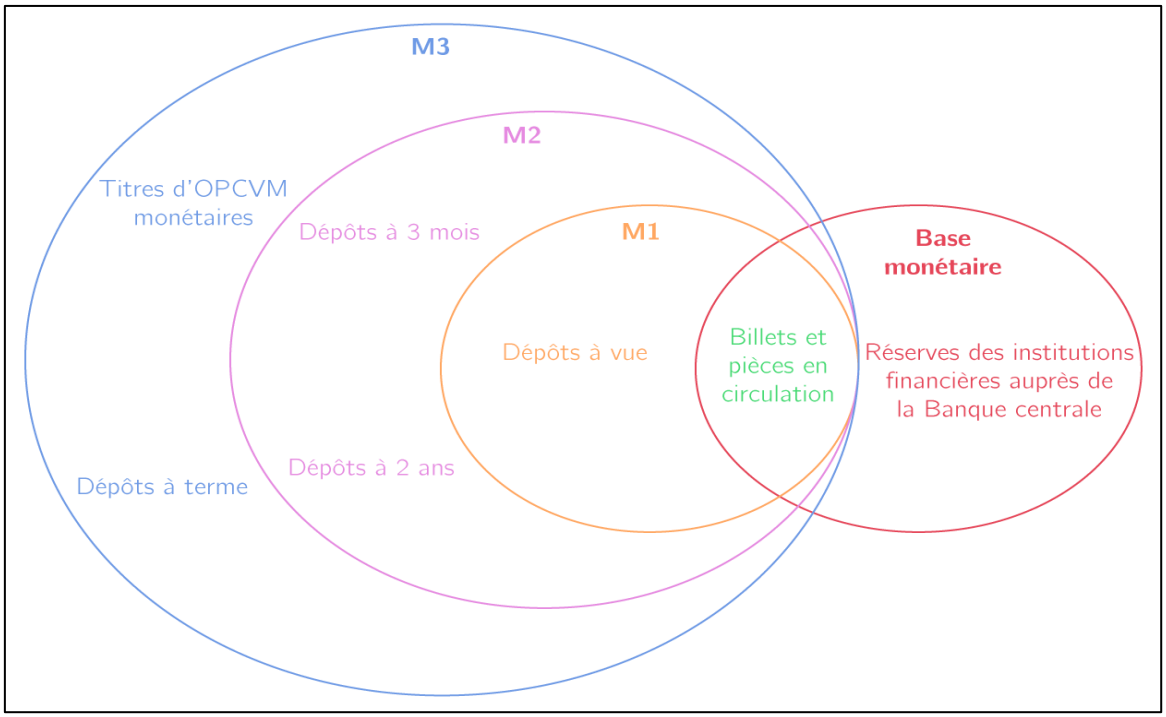
[41] La liquidité fait référence à la capacité d'un actif à être aisément transformable en moyen de paiement sans perdre de valeur.

- **M_1 (la disponibilité monétaire):** regroupe les billets et pièces (B_0) et les dépôts auprès des banques, CCP et le trésor public.

  M_1 = monnaie fiduciaire + monnaie scripturale.

- **M_2 (la masse monétaire) :** contient M_1 + la quasi-monnaie placée auprès des institutions financières et bancaires (IFB) tels que les comptes sur livrets, dépôts à terme et bon de caisse.
- **M_3 (la liquidité de l'économie) :** contient M_2 + la quasi-monnaie placée auprès des institutions financières non bancaires (IFNB) tels les titres d'OPCVM monétaires, pensions et titre de créances de durée inférieure ou égale à deux ans[42].

Figure N° 1 : Les Agrégats Monétaires



La source : la BCE (https://www.ecb.europa.eu)

[42] 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, 2014/2015, p27.

1-3-3- l'intérêt des agrégats monétaires

Les agrégats monétaires permettent aux autorités monétaires de :

- ✓ Mesurer la masse monétaire afin de contrôler l'évolution et la croissance ;
- ✓ Guider la BC en terme de mise en œuvre de la politique monétaire du pays ;
- ✓ Administrer la masse monétaire ;
- ✓ Déterminer les opérations qui sont à l'origine de la création monétaire.

2-La création monétaire

2-1- La définition de la création monétaire

La création monétaire est l'opération qui consiste pour une banque ou plus généralement un établissement de crédit à mettre à la disposition d'un agent économique non financier une certaine quantité de moyens de paiement utilisables sur les marches de biens et service[43]. Les banques ont l'initiative de la création monétaire.

Par la création monétaire, la banque émet une créance sur elle-même. L'acceptation de cette créance par le public en fait un moyen de paiement.

Donc la création monétaire est l'augmentation de la masse monétaire via la monétarisation des créances. C'est une opération qui se réalise entre un agent monétaire et un agent non monétaire, c'est-à-dire une transformation des créances sur les agents non bancaires (ménages, entreprises, Etat,…) sans pouvoir libératoire immédiat sur les marches des biens et services, en moyen de paiement immédiatement utilisable pour effectuer des règlements

2-2-Les principes de la création monétaire

La création monétaire s'effectue par l'intermédiaire d'nt à un crédit bancaire consistant à transformer des créances en moyens de paiement. L'émission des billets par la BC est la forme la plus évidente de la création monétaire, pourtant elle est la moins importante en termes de valeur. Il apparait néanmoins que cette création correspond plutôt à des écritures en comptes à cause de la composition essentiellement scripturale de la masse monétaire.

En effet, dans les économies monétaires modernes, les principaux responsables de la création monétaire sont les établissements de crédit. Selon l'adage "*les crédits font les dépôts*», tout crédit s'ajoute au volume de monnaie existant. Un crédit bancaire permet à un agent économique de disposer d'une capacité de paiement supplémentaire.

[43] Berger, Icard. A," *la monnaie et ses mécanismes*" collection Que sais-je ? Paris, 1995, p.18.

Lorsqu'un dépôt est effectué au sein d'une banque commerciale pour une certaine durée (une année par exemple). Cette banque peut prêter cette somme pour une durée inferieur. Les banques s'aperçurent toutefois que leurs stocks de monnaie ne descendaient jamais en dessous d'un certain seuil puisque une partie des sommes prêtée revenait toujours dans leurs caisses sous forme de dépôts.

Lorsque le trésor public, banquier de l'Etat, veut financer le déficit budgétaire, il peut émettre des bons de trésor qui seront achetés par les banques. Ces dernières acquièrent une créance sur le trésor public en créant de la monnaie. En revanche, si elles prêtent des ressources qu'elles disposent déjà, il n'y a pas création. Ce principe est lié aux crédits internes auprès de l'Etat.

Ces deux opérations, crédits auprès de l'économie et crédits auprès de l'Etat constituent la source interne de la création monétaire des banques.

A celle-ci s'ajoute une source extérieur de la création monétaire ; crédit extérieur lié aux mouvements de capitaux avec l'étranger, les banques avec l'intermédiaire de la BC cédant des devises étrangères sur la marché de change, c'est-à-dire des avoirs en compte dans les banques étrangères (les exportateurs) ainsi que des bénéficiaires de créances sur l'étranger qui doivent transformer leurs avoirs en monnaie locales, inversement, elles procurent à leur clientèle les devises étrangères nécessaires pour effectuer des règlements hors du territoire national.

2-3-Les acteurs de la création monétaire

La Banque Centrale, les banques commerciales et le trésor public participent à des degrés différents à la création monétaire.

2-3-1-La Création monétaire par la Banque Centrale

La Banque Centrale est à la fois un institut d'émission (elle émet la monnaie légale), la banque des banques (elle permet la compensation, le refinancement, la régulation de la masse monétaire et le contrôle des banques), et le gérant des réserves publiques (défense de taux de change). Elle crée la monnaie centrale à trois occasions[44] :

❖ *Transforme des créances détenues par les banques en monnaie centrale :* c'est-à-dire en assurant le refinancement des banques sous liquides, si une entreprise emprunte de l'argent à une banque, cette dernière a une créance sur l'entreprise, la banque peut vendre sa créance à

[44] Rumy Michel. Op.cit.p.47

la BC. Cette dernière va créer de la monnaie au profit de la banque commerciale. La dette de l'entreprise est alors transférée de l'actif de la BC qui fait payer aux banques commerciales un taux d'intérêt directeur[45].

Ces taux influencent le coût de crédit que les banques accordent à leurs clients.

❖ *Transforme les devises reçues par les agents économiques en monnaie centrale :* lorsqu'elle acquière des devises, la BC procède également à de la création monétaire (les opérations sur or et devises). Les opérations d'achats et de ventes de devises de la BC sur le marché des changes peuvent avoir un effet sur la masse monétaire. Les créances extérieures nettes, si elles sont positives, sont génératrices de création de monnaie.

❖ *Achat de titre de la dette directement à l'Etat :* en faisant des avances au trésor public (le concours de la BC à l'Etat) en lui achetant des bons de trésor pour financer les besoins de trésorerie et une partie du déficit budgétaire de l'Etat (planche à billet).

La BC se contente d'acheter aux banques de second rang les bons de trésor qu'elles ont acheté sur le marché monétaire.

2-3-2- la création de la monnaie scripturale par les banques commerciales

Les banques ordinaires créent de la monnaie scripturale à l'occasion d'une opération de crédit à court terme et moyen terme[46].

Un crédit consiste à transformer une créance (reconnaissance de dette) en monnaie, lorsqu'un client obtient de sa banque un prêt ou un crédit, son compte est alors crédité de la somme. La banque crée ainsi de la monnaie scripturale par une inscription au crédit de compte à vue de la personne qui a obtenue le prêt, donc il y a une création supplémentaire.

Lorsqu'un client rembourse le prêt, il y a destruction de monnaie.

2-3-3- Le rôle du trésor public dans la création de la masse monétaire

Le trésor public a deux rôles complémentaires et indissociables qui sont la gestion de la trésorerie de l'Etat et une fonction monétaire[47].

➢ Le trésor public est le gestionnaire de trésorerie et des déficits de l'Etat.

[45] C'est un taux d'intérêt fixé par la BC, auquel elle accorde des crédits à court terme aux banques commerciales.
[46] Rumy Michel. Op.cit.p.32.
[47] François Combe, Thierry Tacheix, Op.cit, p.65.p.66

La loi de finance définit les dépenses et les recettes de l'Etat pour l'année civile, ceci conduit à gérer les flux de trésorerie ainsi que les éventuels déséquilibres budgétaires annuels. Comme les recettes et les dépenses ne sont pas parfaitement synchronisées, le trésor public est obligé de laisser les flux de trésorerie en retardant ou différant certains paiements.

Si le budget est en déficit, le trésor public doit le financer, quatre sources de financement peuvent être envisagées :

- ✓ Il peut procurer des ressources en faisant appel à l'épargne du public à travers l'émission de bon de trésor ;
- ✓ Il peut emprunter auprès des banques et des intermédiaires financiers non bancaires en leur vendant des bons en fonction du volume de ses besoins. L'appel au public et aux intermédiaires financiers représente un financement « à travers le marché » ;
- ✓ Il peut financer le déficit en se procurant des ressources « hors marché ». Il peut emprunter à deux organismes qu'il gère : les CCP et les collectivités locales ;
- ✓ Il peut céder des actifs qui appartiennent à l'Etat (vente de biens et privatisation).

Le trésor public exerce une fonction monétaire directe et indirecte. Il crée sa propre monnaie, en quantité très faible, à travers l'émission de monnaie divisionnaire. C'est une fonction de création monétaire directe. Le montant de cette monnaie divisionnaire en circulation a pour contrepartie une dette de l'Etat.

Le tableau qui suit récapitule les différents acteurs qui créent de la monnaie et les circonstances qui sont à l'origine de cette création monétaire :

Tableau N°1 : Les acteurs de la création monétaire

Acteur de la création monétaire	Circonstance à l'origine de la création monétaire
La Banque Centrale	- Emission des billets. - Concours aux banques secondaires. - Avances au trésor public. - Achat des devises.
Les banques commerciales	- Octroi de crédits - Achat de bons de trésor. - Achat de titres de créances à leurs clients. - Achat des devises
Trésor public	- Frappe de monnaie. - Création de monnaie scripturale en créditant les comptes des titulaires de comptes courants postaux. - Emission des bons de trésor.

Source : établi par nos soins

SECTION 3 : LE SYSTÈME MONÉTAIRE ET LE SYSTÈME DE PAIEMENT ACTUEL

La monnaie, ainsi que la montre l'histoire, peut être fragile, que son offre passe par des moyens privés, soit assurée de manière concurrentielle ou soit le fait d'un émetteur souverain qui en détient le monopole. La qualité de la monnaie émise par les banques dépend des actifs qui l'étayent. Les banques ont pour but de transformer les risques ; par conséquent la confiance dans une monnaie émise de manière privée peut disparaitre du jour au lendemain.

La recherche d'un cadre institutionnel solide soutenant la confiance dans la monnaie a finalement abouti à la création des banques centrales telles que nous les connaissons aujourd'hui. Elles ont pour but d'améliorer les échanges commerciaux en fournissant un moyen de paiement efficace et de qualité, en centralisant un certains nombre d'opérations de compensation et de règlement.

1 Les rôles des banques centrales

A l'ère moderne, le système qui a fait ses preuves dans l'instauration d'une confiance résiliente est celui des banques centrales indépendantes. Il passe par l'établissement d'objectifs (en matière de politique monétaire et de stabilité financière) ; par une indépendance opérationnelle, administrative ainsi qu'au plan des instruments utilisés ; et le principe de responsabilité démocratique, afin de garantir un soutien et une légitimité politique suffisamment larges. Les banques centrales indépendantes sont largement parvenues à préserver l'intérêt économique et politique de la société à disposer d'une monnaie stable. Dans cette configuration, la monnaie peut être précisément définie comme une "convention sociale indispensable, soutenue par une institution au sein de l'Etat qui jouit de la confiance du public"[48].

Dans la quasi-totalité des économies actuelles, l'offre de monnaie est le fait d'un partenariat public-privé entre la banque centrale et les banques privées, la première se situant au cœur du système.

Dans le cadre de leur mandat consistant à assurer la stabilité de la monnaie en tant qu'unité de compte et moyen de paiement, les banques centrales jouent un rôle actif dans la supervision, la surveillance et, dans certains cas, l'offre, d'infrastructures de paiement pour leur monnaie. Les banques centrales ont notamment pour rôle de garantir le bon fonctionnement du système de paiement et de veiller à ce que l'offre de réserve réponde correctement à l'évolution de la demande.

Grâce au rôle actif des banques centrales les systèmes de paiement, dans leur diversité, sont aujourd'hui devenus sûrs, efficaces en terme de couts, extensibles et à même de garantir qu'un paiement, une fois effectué, est irrévocable.

Dans les économies complexes aujourd'hui, le volume de paiement est élevé, représentant plusieurs fois le PIB. Pour autant l'augmentation de l'utilisation de l'instrument ne conduit pas à une augmentation proportionnelle des coûts. Il s'agit d'un point important car une l'une des caractéristiques essentielles d'une bonne monnaie et d'un bon système de paiement est l'étendue de son utilisation tant par les acheteurs que par les vendeurs : plus il existe d'utilisateurs d'un système de paiement en particulier, plus un individu est incité à y recourir lui-même.

[48] Rapport économique annuel 2018, P4 .consulté en ligne sur (www.bis.org) le 29/11/2019(Bank for international settlements).

Dans les économies modernes, la monnaie est majoritairement constituée de dépôts bancaires. Pour l'essentiel, la monnaie est donc créée, détruite et transférée par les banques. Cette monnaie dite « de banque » a plusieurs caractéristiques[49] :

- Pour posséder la monnaie et l'utiliser, il faut disposer d'un compte bancaire, nécessaire à l'inclusion financière au sein d'une société ;
- Toute transaction monétaire s'accompagne d'un mouvement de comptes bancaires. Elle est identifiable et traçable. Elle peut être surveillée et règlementé ;
- La monnaie est une créance sur une personne morale identifiable, en l'occurrence la banque ;
- La monnaie de banque est une monnaie « privée ». elle est donc vulnérable à une perte de confiance dans les banques qui l'ont émet ;
- Mais elle bénéficie d'un soutien de la banque centrale par le biais de mécanismes d'assurance et de dépôts ou d'un accès au refinancement ;
- Par ailleurs, c'est la banque centrale qui émet la monnaie servant de « base » au système, ce qui lui confère cours légale ;

De nombreux instruments permettent aujourd'hui d'utiliser et de mobiliser la monnaie de banque. S'agissant des paiements de détail, des progrès ont donné naissance à de nouveaux supports : cartes bancaires, virements par internet, monnaie stockées sur téléphones mobiles, qualifiés de « monnaie électronique ».

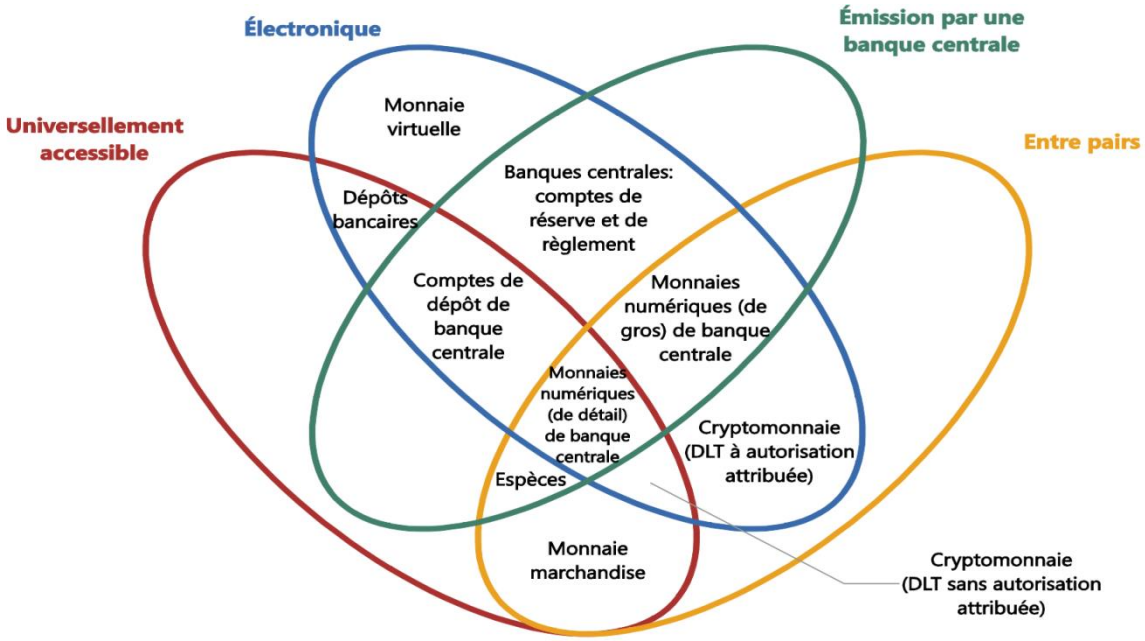
Il ne s'agit pas de monnaie mais d'instruments de paiement qui permettent de mobiliser et d'utiliser la monnaie de banque.

2- La « corolle des monnaies » : une taxonomie des monnaies

Si la plupart des transactions passent aujourd'hui par des moyens de paiement en définitive adossées aux banques centrales, une riche panoplie de moyens de paiement publics et privés s'est, au fil du temps, développée. La « corolle des monnaie » en fournit une taxonomie détaillée[50].

[49] Jean-Pierre Landau, Alban Genais, Op.cit.
[50] Rapport économique annuel 2018, Op.cit.p5.

Figure N° 2 : La Corolle Des Monnaies



Source : Rapport trimestriel BRI, Septembre 2017

La corolle des monnaies distingue quatre propriétés clés des monnaies : L'émetteur, la forme, le degré d'accessibilité et le mécanisme de transfert de paiement.

L'émetteur peut être une banque centrale, une banque, ou bien personne en particulier, comme cela était le cas lorsque la monnaie prenait la forme d'un produit de base.

La monnaie peut revêtir une forme physique (par exemple, une pièce de métal ou un billet de banque), ou numérique.

Elle peut être largement accessible (c'est le cas des dépôts des banques commerciales) ou d'accès réduit (réserves des banques centrales).

La dernière propriété concerne le mécanisme de transfert, qui peut être pairs ou passer par un intermédiaire central- comme c'est le cas pour les dépôts.

3-Les monnaies historiques : Usages classiques et nouveaux usages

3-1-L'évolution des usages classiques

A l'heure de la décentralisation et des innovations technologiques, l'acte de paiement a aussi évolué en ce qui concerne les monnaies traditionnelles : en effet, le commerce à distance a modifié cette relation directe et de nouveaux acteurs sont apparus. Ainsi, de nouvelles solutions de paiement se sont multipliées dans un monde où les moyens de paiement traditionnels (espèce, carte bancaire ou chèque) avaient créé une relation de confiance au fil du temps.

La carte bancaire a acquis une confiance majeure auprès des utilisateurs en prouvant sa robustesse, sa facilité d'utilisation et surtout sa sécurité liée à une innovation technologique, la carte à puce. Ce moyen de paiement qui a pu connaitre des difficultés dans son développement, notamment à l'international, est néanmoins devenu indispensable et créateur de confiance dans les transactions et les échanges internationaux.

Selon le rapport de la BCE sur les moyens de paiement, le nombre total de paiements scripturaux dans l'UE a augmenté de 4,2% en 2012 par rapport à 2011. Au niveau européen, les paiements par carte représentent 42% de l'ensemble des opérations, alors que la part des virements se monte à 27% (augmentation de 3% atteignant 25,7 milliards d'euros)[51].

Le nombre de cartes de paiement a augmenté de 1,5% dans l'UE, s'établissant à 738 millions en 2012, ce qui équivaut à 1,46 carte de paiement par habitant. Le nombre de transactions par carte a augmenté de 7,3% s'établissant à 39,8 milliards, pour une valeur de 2 000 milliards d'euros, représentant une valeur moyenne de 51 euros par transaction. En moyenne, un européen effectuait 79 paiements par carte en 2012, un français, 129, un Danois, 224, un Allemand, 39 et un Bulgare moins de 5.

L'utilisation du chèque continue de diminuer avec 4,5% des opérations réalisées en Europe 4,3 milliards de chèque émis en 2012. Les français conservent leur première place avec 66% des paiements par chèque émis en Europe qui sont effectués en France. A l'inverse, le chèque a quasiment disparu en Allemagne, ou en Belgique, où moins d'un chèque par an est émis par habitant[52].

[51] Ces statistiques concernent l'UE.

[52] Pierre Antoine Gailly,"*Les nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux*», les éditions des journaux officiels, avril 2015, consulté en ligne sur (www.lecese.fr) le 28/10/2019.

3-2-Les nouveaux usages et technologies nouvelles

Le nombre croissant de transactions sur internet et l'importance de la fraude ont nécessité la création d'outils permettant de sécuriser les transactions. D'après la Fevad[53], "les ventes sur internet mobile (Smartphone et tablettes, sites mobiles et applications hors téléchargement d'application et hors ventes sur les places de marché) poursuivent leur développement avec +97% au 4ème trimestre 2013 par rapport au 4ème trimestre 2012"[54]. Afin de permettre aux internautes de payer sur internet, plusieurs solutions existent qui permettent de sécuriser les achats en ligne en ne transmettant pas les données de la carte bancaire, qui ont été préalablement enregistrées par l'utilisateur comme:

- **PayPal :** avec plus de 100 millions de comptes actifs dans le monde, c'est le leader des paiements en ligne.
- En France par exemple, des solutions de paiement sur internet sécurisé ont fleuré ces dernières années avec des initiatives comme Kwixo (Crédit Agricole), Buyster ou encore Paylib (BNP Paribas, Société Générale et la Banque Postale). En proposant une alternative à l'américain PayPal, Paylib peut rassurer certains clients réticents car le service est directement géré par des banques et les opérations apparaîtront dans le relevé de compte au même titre qu'un virement classique.

Deux nouvelles technologies sont en train de se développer : le paiement sans contact (technologie NFC)[55] et les portefeuilles en ligne (e-Wallet)[56]. Ces derniers tentent d'installer de nouvelles habitudes de consommation en dépassant la simple transaction. En effet, les fournisseurs de ces solutions vendent également des services de gestion de la clientèle (fidélité, connaissance du client…).

Tous ces nouveaux moyens de paiement reposent sur l'utilisation de monnaies classiques. Il s'agit avant tout pour de nouveaux acteurs de s'insérer dans un marché réputé porteur et pour les acteurs en place de ne pas être distancé. Ces différents acteurs font évoluer l'acte de

[53] La Fevad (Fédération e-commerce et vente à distance) est un syndicat professionnel français créé en 1957, a pour vocation de fédérer l'ensemble des acteurs du e-commerce et de la vente à distance, quelque soient le secteur et le support de communication utilisés. Aujourd'hui la Fevad regroupe plus de 600 entreprises et plus de 1000 sites internet, dans le domaine de la vente aux particuliers, de la vente aux professionnels ou encore celui de la vente entre internautes.

[54] Pierre Antoine Gailly, Op.cit.

[55] La technologie NFC (Near Field Communication : la communication en champ proche) consiste à rapprocher sa carte bancaire ou Smartphone d'un terminal sans contact NFC, pour effectuer une transaction. Cette dernière est immédiate et ne demande aucune confirmation ; ni code bancaire, pour les petits montants.

[56] E-Wallet s'agit d'un compte alimenté à partir de son compte bancaire. L'exemple le plus cité est celui de Google qui a lancé son portefeuille en ligne et qui continue d'investir dans l'industrie du paiement.

paiement en proposant des services nouveaux aux utilisateurs (rapidité et facilité d'emploi notamment) et présumés moins couteux. En outre, un nouvel écosystème se crée : de nouveaux acteurs proposent des nouveaux modes d'initiation et de nouveaux services en matière de paiement.

CONCLUSION

La monnaie favorise l'activité économique en facilitant les échanges entre les agents économiques, les fonctions et les formes de monnaie s'appuient sur les instruments de paiement qui se dématérialisent, et sur la confiance qu'ont les agents économiques dans le système financier et bancaire qui régule la circulation monétaire.

Depuis son appariation, la monnaie n'arrête pas de connaitre de nouveaux moyens de paiement grâce aux innovations technologiques et à l'essor des moyens de télécommunication. D'ailleurs ces dernières années nous assistons à l'émergence de monnaie d'un genre nouveau, reposant sur des procédés cryptographiques et gérées en pair à pair selon un consensus distribué, appelée crypto-monnaie.

De nos jours de nombreuses transactions se font dans une partie du monde, par le biais de cette monnaie qui pourrait remplacer la monnaie traditionnelle.

Chapitrell:
La Genèse
des crypto-monnaies

CHAPITRE II : LA GENÈSE 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 réglementées 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[57]. 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 start-ups[58] 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.

Alors dans ce chapitre, organisé aussi en trois sections, nous essayons de répondre sur des questions soulevées par les crypto-monnaies ; d'abord nous verrons dans la première section que sont les crypto-monnaie ? Leur historique ainsi que leur nature. La seconde portera sur les différents concepts qui leur sont liés. Et enfin, pour la troisième section, nous présenterons l'écosystème de ces monnaies.

[57] Jean-Paul Delahaye, ″Les preuves de travail″ revue Pour la science, N°60, Avril 2014, en ligne consulté sur (www.pourlascience.fr) le 26/10/2019.

[58] Start-up (entreprise en démarrage en français) est une nouvelle entreprise innovante, généralement à la recherche d'importants fonds d'investissement avec un très fort potentiel éventuel de croissance économique, et de spéculation financière sur sa valeur future.

SECTION 1 : QU'EST CE QU'UNE CRYPTO-MONNAIE ?

Depuis leur apparition les crypto-monnaies génèrent beaucoup de fantasme. Pourtant, pour beaucoup, le concept même de crypto-monnaie est souvent abstrait. Alors qu'elles peuvent s'avérer être un formidable investissement, il serait malavisé de miser sur les crypto-monnaies sans en connaitre tous les mystères.

1-Historique

Ce qui nous amène à la préhistoire des monnaies chiffrées ou cryptées. En 1982, soit une décennie avant le développement du commerce électronique, dans un papier nommé ″Blind Signatures for Untraceable Payements″ (Signature aveugle), David Chaum décrit le premier système chiffré pour permettre des paiements intraçables[59]. Il y décrit comment parvenir à des paiements qui reposent sur la cryptographie et qui empêchent au tiers de savoir qui paye, à quel moment et quel montant. Ce système permettrait aux individus d'avoir des preuves de paiement et d'avoir à enrayer les moyens de paiement détournés ou volés.

En 1990, le même David Chaum écrit un autre papier nommé ″Untraceable Electronic Cash″ dans lequel il explique que l'utilisation des cartes de crédit est devenue un acte de foi de la part de leurs détenteurs car ils n'ont aucune protection contre la surveillance et contre la fraude. Dans son papier explique que l'argent liquide dispose d'un avantage certain sur la carte de crédit en ce qui concerne le respect de la vie privée. Partant de ce constat, il décide de créer un premier système de monnaie électronique anonyme qui ne va pas bénéficier d'une acceptation globale et va se solder par un échec. Toutefois, l'idée de transactions protégeant l'anonymat, en plus d'être nées, a été mise en application pour la première fois.

En 1996 est créé e-Gold[60], considéré comme une devise électronique ayant pour but de créer une monnaie mondiale numérique et convertible en or. Cette monnaie permet de faciliter les paiements sur internet. Elle est soupçonnée d'être utilisée dans de nombreuses activités illégales, les créateurs ont donc été mis en examen pour blanchiment d'argent, transferts illégaux, etc. accusation remplacées par l'accusation d'opérer sans licence bancaire locale. Ainsi est née la première monnaie électronique non émise par un Etat et qui pouvait se changer contre une réserve de valeur communément acceptée à travers le monde, à savoir l'or.

[59] David Chaum, ″Blind signatures for Untraceable payements″,1983, en ligne, consulté sur (www.taler.net) le 20/10/2019.
[60] Site internet e-Gold en ligne (www.e-gold.com) consulté le 20/10/2019.

En 1998, un cypherpunk[61] (voir annexes) du nom Wei Dai écrit le ″B-money proposal″[62]. Dans cet article publié sur la liste de diffusion cypherpunk, tout en expliquant ne pas savoir comment les mettre en place, il décrit deux protocoles de création et gestion monétaires non traçables sans avoir besoin d'aide extérieure[63], de tiers de confiance ou autre personne faillible. Il décrit dans son article un système basé sur la preuve de travail (proof of work)[64] comme mode de création monétaire, en s'appuyant sur l'hypothèse que tous les participants seraient aussi les gardiens du système.

C'est dans ce contexte, à travers ces théories, que vont apparaître les premières monnaies chiffrées ou plus communément appelées crypto-monnaie. Le Bitcoin est la tête de ces nouvelles monnaies numériques basées sur la cryptographie. En effet, en 2008, une ou plusieurs personnes utilisent le pseudonyme ***Satoshi Nakamoto,*** publient sur la liste de la diffusion cypherpunk un article appelé le ″white paper″ (ou livre blanc)[65] par la communauté Bitcoin. Cet article a pour objectif de décrire le fonctionnement du protocole Bitcoin, le Bitcoin étant à la fois un moyen d'échange et un système de paiement. Les différences majeures entre le Bitcoin et les autres monnaies électroniques et/ou virtuelles, qui existaient précédemment, sont que ces autres monnaies, qu'elles soient étatiques ou privées, sont émises par des autorités centrales à savoir les Etats, les banques centrales ou non, et les compagnies privées. Ce qui donne un monopole de contrôle sur la monnaie à ces entités.

Le système Bitcoin, comprenant la monnaie et le moyen de paiement, est apparu le 03 janvier 2009 avec la création des premières bitcoins. Dans son article réellement nommé ″Bitcoin :A peer-to-peer Electronic Cash system″, Satoshi Nakamoto décrit tous les mécanismes de fonctionnement du protocole Bitcoin, et donc de la première crypto-monnaie, qui fonctionneront par la suite pour la plupart sur le modèle du Bitcoin. C'est une innovation que

[61] Cypherpunks (mot-valise composé à partir des mots anglais cipher : *chiffrement,* et punk sur le modèle de cyberpunk) forment un groupe informel de personnes intéressées par la cryptographie. Leur objectif est d'assurer le respect de la vie privée par l'utilisation proactive de la cryptographie.

[62] B-money : était l'une des premières propositions de Wei Dai pour un système de paiement électronique anonyme et distribué. En ligne sur (en.bitcoin.it) consulté le 20/10/2019.

[63] http://www.bitcoin.org consulté le 22/09/2019.

[64] Preuve de travail ou en anglais ″proof of work″, est un des concepts les plus important en, ce qui concerne le chiffrement, et plus particulièrement celui des monnaies numériques. On demande à l'ordinateur d'effectuer une tâche qui nécessite de la puissance de calcul afin de créer la preuve de travail (Son fonctionnement et son utilité seront expliqués par la suite).

[65] Un white paper, ou livre blanc, est un recueil d'information factuelle concernant un projet. Le rôle du livre blanc en marketing est de convaincre de l'intérêt d'un projet. Dans le monde des crypto-monnaies, il est généralement publié par l'initiateur d'un projet entre le moment où le projet est annoncé et le lancement De l'ICO (la levée de fons en crypto-monnaies).

l'on pourrait qualifier de révolutionnaire, qui va et qui change déjà l'approche traditionnelle que l'on a du paiement et de la monnaie[66].

2-Définition

Avant de donner une définition de la crypto-monnaie, il est nécessaire de définir le principe de base de sa création, à savoir la cryptographie.

2-1-Définition de la cryptographie

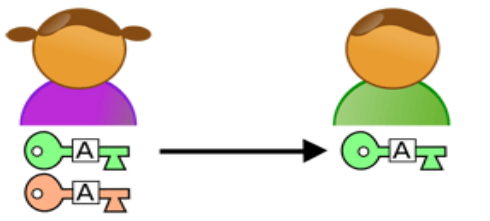
La cryptographie est une technique basée sur des caractères (chiffres, lettres,…) permettant de protéger des messages en les rendant inintelligibles (en les chiffrant).

Le mot ″cryptographie″ vient des mots en grec ancien ***″Kruptos″*** (caché) et ***″graphein″*** (écrire).

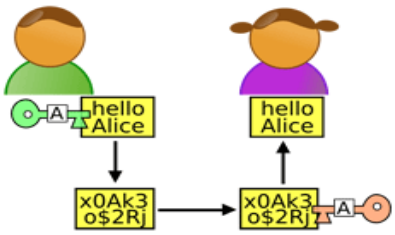
En cryptographie classique, dite, symétrique, le chiffrement est la transformation, par le biais d'une clé, d'un message compréhensible (un texte clair) en message incompréhensible (un texte chiffré) pour celui qui ne possède pas la clé de déchiffrement.les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message.

En cryptographie asymétrique[67], chacun a sa clé, ce qui évite de devoir envoyer de manière confidentielle la clé de déchiffrement à son correspondant. Cette cryptographie est utilisée par toute les crypto-monnaies. Aller dans un sens est facile et dans l'autre sens quasiment impossible.

Figure N°3 : Le Principe De La Cryptographie Asymétrique



Principe de la cryptographie asymétrique.
Alice génère deux clés : la clé publique (verte) qu'elle envoie à Bob et la clé privée (rose) qu'elle conserve précieusement sans la divulguer à quiconque.



Bob chiffre son message avec la clé publique d'Alice et lui envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

Source: WIKIPEDIA (fr.wikipedia.org)

[66] Chris Campbell, *"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.
[67] La cryptographie asymétrique est déjà utilisée depuis longtemps par les banques et l'internet pour coder des données et des messages ; par exemple des mots de passe.

La cryptographie asymétrique est basée sur la distinction données publiques/privées et sur deux clés : la clé publique, qui permet de chiffrer (rend le message inintelligible) et qui peut être mise à disposition de tous, et la clé privée, qui permet de déchiffrer et qui doit rester absolument secrète. C'est exactement ce système de public Key/private Key qui est utilisé dans les crypto-monnaies.

Ce système a deux avantages majeurs, la confidentialité du message est assurée par l'utilisation de la clé publique pour chiffrer et de la clé privée pour déchiffrer celui-ci.

Autre avantage : celui de l'authenticité de l'expéditeur, qui utilise la clé publique du destinataire pour coder un message que seul le destinataire pourra décoder, car lui seul possède la clé privée correspondant à sa clé publique[68].

2-2-Définition des crypto-monnaies

La crypto-monnaie[69], selon la personne à qui vous demandez, est considérée comme une monnaie, un actif ou un bien, tout comme l'or. La crypto-monnaie, comme le bitcoin, est une forme d'argent numérique qui peut servir à l'achat de biens ou services et remplacer une monnaie classique. Une crypto-monnaie est un bien numérique conçu pour servir de moyen d'échange dans la cyberéconomie[70].

Une crypto-monnaie, ou monnaie cryptographique, monnaie numérique, monnaie digitale ou encore monnaie virtuelle (dénomination *à priori* péjorative) est une monnaie dont le fonctionnement et la sécurité sont fondés sur la cryptographie[71]. Pour être échanger sur internet, et qui, pour certaines crypto-monnaies, sont gérées de manière décentralisée[72].

Trois caractéristiques définissent donc conjointement les crypto-monnaies :

- Ce sont des monnaies virtuelles, c'est-à-dire des représentations numériques de valeur purement fiduciaires : elles ne sont ni émises, ni garanties, ni par une banque centrale, ni par une institution de crédit ou monétaire ;

[68] Enée Bussac, *"Bitcoin, Ether & Cie : guide pratique pour comprendre, anticiper et investir."*, Dunod, 2018, P.9.
[69] le terme crypto actif (crypto asset en anglais) est de plus en plus utilisé. Le terme donne une dimension plus grande aux crypto-monnaies. La plupart n'ont pas pour but d'être simplement une monnaie, elles constituent à la fois un actif financier reflétant la valeur de société émettrice et un outil permettant d'utiliser un service, comme un réseau d'ordinateur pour faire tourner des contrats intelligents (smart contract en anglais).
[70] BMO. Nesbitt burns Inc., *"Introduction au bitcoin et aux autres crypto-monnaies"*, Rapport publié par la banque de Montréal, Canada, octobre 2017, consulté en ligne sur (www.nesbittburns.bmo.com) le 01/07/2019.
[71] Enée Bussac, Op.cit.p10.
[72]Jean-Pierre Landau, Alban Genais, Op.cit.

- Elles utilisent la cryptographie, elles sont conçues et adaptées pour transmettre de la valeur sur internet dans un environnement totalement ouvert et public, et en toute sécurité ;
- La plupart, mais pas toutes, fonctionnent dans un système décentralisé, où l'information est intégralement, simultanément et également distribuée entre tous les participants. Les transactions sont décidées et validées par un **consensus**[73].beaucoup, mais pas toutes, sont adossées à la technologie **Blockchain**[74].

La crypto-monnaie n'existe que sous forme électronique et n'est pas rattachée à un territoire[75].

Toutes les crypto-monnaies se distinguent les unes des autres essentiellement par leur valeur (déterminée par la loi de l'offre et de la demande et relativement volatile), leur rythme de création (de nouvelles unités monétaires sont créées à une fréquence prédéfinie), le fonctionnement de leur blockchain et leur projet.

Chaque crypto-monnaie est utilisable sur un réseau informatique et est caractérisée par un symbole (ticker) généralement de trois lettres majuscules (BTC pour le bitcoin).

La crypto-monnaie est couplée à un système de paiement qui permet de régler des transactions de pair à pair (peer-to-peer)[76]. Elle a un fonctionnement décentralisé et est régie par un protocole initial qui stipule le rythme et les règles de création et d'attribution de nouveaux coins[77].

Le modèle des crypto-monnaies préserve une forme d'anonymat, puisque l'identité des possesseurs des clés publiques n'est pas nécessaire, seule une preuve de possession de la clé privée (la signature électronique de la transaction) est demandée pour dépenser des devises[78].

[73] A revoir par la suite.
[74] Elément détaillé dans la section suivante.
[75]Enée Bussac, Op.cit.p11.
[76] Peer-to-peer ou pair à pair est l'un des principes de fonctionnement des crypto-monnaies (principe expliqué dans les sections qui suivent.)
[77] Un coin (littéralement pièce de monnaie) est une monnaie cryptographique, toujours lié à une plateforme ou système où cette monnaie sert de moyen de paiement, le bitcoin par exemple.
[78] Jean-Guillaume Dumas, Pascal la Fourcade, *"Les crypto-monnaies, une réalité virtuelle"*, Dunod, 2015, P10.

Le nombre d'unités en circulation et la masse monétaire maximales sont définis à l'avance et visible par tous, jusqu'à preuve du contraire, une crypto-monnaie ne peut pas être contrefaite ou usurpée[79].

3-La double innovation des crypto-monnaies

Hormis les pièces et billets de banque, toute monnaie est aujourd'hui dématérialisée et digitale. Elle existe uniquement sous forme électronique. Il en va de même des actifs et titres financiers. Les crypto-monnaies n'apportent, de ce point de vue, aucun changement.

La révolution est ailleurs et plus profonde, à la fois technologique et monétaire[80]. Ces deux éléments sont présents dans la plupart des crypto-monnaies.

3-1-L'innovation technologique

Beaucoup de technologies de base utilisées par les crypto-monnaies, comme les registres distribués, les techniques cryptographiques et les signatures électroniques existent depuis plusieurs décennies. L'innovation vient de la combinaison de ces diverses techniques dans un projet ambitieux et cohérent.

3-1-1-L'innovation dans les procédures et dans les registres ″la blockchain″

- ✓ la technologie des registres distribués (DLT : Distributed Ledger Technology) : système numérique qui enregistre des transactions d'actifs et leurs détailles dans plusieurs emplacements à la fois ;
- ✓ la blockchain, elle-même qui est une forme particulière de registre distribué ;
- ✓ Les procédures de consensus.

Ces trois composants ne sont pas nécessairement liés et présents dans toutes les crypto-monnaies, on les trouve intégralement dans Bitcoin et Ethereum, mais dans d'autres crypto-monnaies, par exemple Ripple, la 3ème plus importante crypto-monnaie, a des registres distribués et des règles de consensus, mais pas de blockchain. La crypto-monnaie IOTA ne s'appuie pas sur une blockchain et la décentralisation n'est pas totale.

3-1-2-La digitalisation de la valeur

C'est une deuxième innovation que les crypto-monnaies contribuent à promouvoir**.** Il s'agit de la capacité à présenter numériquement de la valeur et à la transférer en toute sécurité entre individus sans aucun intermédiaire.

[79]Crypto-encyclopédie, en ligne sur (www.cryptoencyclopedie.comm) consulté le 23/10/2019.
[80] Jean-Pierre Landau, Alban Genais, Op.cit.

3-2-L'innovation monétaire

3-2-1-Les crypto-monnaies

Les crypto-monnaies sont fondamentalement différentes. Comme la monnaie de banque, elles n'ont aucune valeur intrinsèque, et sont totalement dématérialisées et digitales. Mais chacune de leurs autres caractéristiques se situe à l'opposé des monnaies existantes :

- Elles se créent et circulent indépendamment de toute banque et sont détachées de tout compte bancaire ;
- Elles ne représentent pas une créance sur quelconque, personne physique ou morale ;
- Il s'agit de monnaie purement privée, sans cours légal, et ne bénéficient d'aucun soutien public, direct ou indirect.

Au-delà de la prouesse technologique et de l'apparente proximité avec les monnaies électroniques, il est important de mesurer que les crypto-monnaies constituent une expérience monétaire sans réel précédent. Les formes de monnaie ont constamment évolué dans l'histoire, sous l'effet de la technologie, des institutions ainsi que des conventions sociales. Néanmoins, toutes les monnaies qui se sont développées et imposées dans les économies capitalistes possédaient l'une ou l'autre – ou plusieurs- des caractéristiques suivantes :

- ✓ Soit une valeur intrinsèque (les monnaies et pièces en métal précieux) ;
- ✓ Soit une contrepartie sous forme d'actif physique ou financier servant à gager leur valeur, c'est le cas de l'étalon-or ;
- ✓ Soit un soutien public, avec cours légal et refinancement par la banque centrale.

Les crypto-monnaies aujourd'hui n'ont aucun de ces trois attributs. Ce sont des objets monétaires totalement nouveaux. Pour cette raison, elles sont qualifiées de ″virtuelles″.

3-2-2-Les régimes d'émission

Les créateurs de crypto-monnaies ont accordé beaucoup d'importance et d'attention à leur régime d'émission. Ces régimes, assez divers, combinent un mélange de rigueur, d'ambigüité et d'innovation aux conséquences parfois incertaines[81] :

- ✓ La rigueur provient d'un encadrement de la quantité de monnaie émise. Celle-ci est souvent plafonnée, soit en montant final (Bitcoin), soit en taux de croissance (Ether), soit en montant initial (Ripple) ;

[81] Jean-Pierre Landau, Alban Genais, Op.cit.

- ✓ L'ambigüité vient des conditions dans lesquelles certains fondateurs se ″réservent″ à l'émission, une fraction du stock de crypto-monnaies. Quand cette fraction est significative, les fondateurs contrôlent directement l'émission effective de la monnaie en cause, dont la valeur dépendra des conditions de libération de la réserve ;

De nouveaux régimes d'émission des crypto-monnaies se déploient. Certaines sont totalement adossées à ″un panier″ de monnaies avec cours légal, dont elles forment une représentation digitale. C'est le cas de Saga, créée en mars 2018 et adossée aux droits de tirage spéciaux (DTS), la monnaie interne du Fonds Monétaire International (FMI). C'est aussi le cas de Tether, créée en 2016 et théoriquement adossée au pair au dollar pour une capitalisation de 2,5 milliards de dollars. D'autres sont plus ambitieuses et visent à stabiliser automatiquement le taux de change de la monnaie virtuelle par rapport à l'une des grandes monnaies fiat[82]. Ce sont les projets dits de ″stablecoin″[83]. Pour ce faire, l'émission et la destruction de monnaies sont contrôlées par un algorithme qui réagit aux variations de cours[84].

4-Une diversité des crypto-monnaies

En Octobre 2019, nous recensons 2346 crypto-monnaies[85], et ils en apparaissent 2 ou 3 nouvelles chaque jour. La liste régulièrement mis à jour.

En réalité, seule une douzaine de crypto-monnaies semblent disposer d'un réel potentiel à un moment donnée. A la fin du mois d'Octobre 2019, ces crypto-monnaies sont les suivantes : Bitcoin(BTC), Ethereum(ETH), Ripple(XPP), Tether(USDT), Bitcoin cash (Bch), Litecoin(LTC), Binance coin(BNB), EOS, BitcoinSV(BSV), Stellar(XLM), Tron(TRX), Cardano(ADA).

Le Bitcoin constitue la 1ère génération de la crypto-monnaie basée sur la blockchain.

L'Ethereum, la 2ème génération, n'est pas seulement une monnaie, mais davantage un environnement de développement à part entière et qui a donnée le feu vert au phénomène des crypto-monnaies, et a prouvé que leur technologie sous-jacente disposait d'un potentiel bien plus large que celui du simple Bitcoin, permettant : le stockage non seulement de la crypto-

[82] Une monnaie fiat est une monnaie fiduciaire décrétée par l'Etat, une monnaie qui a cours légal, tels que :le dollar, l'euro , la livre ,…

[83] Un stablecoin est un coin qui réplique la valeur d'un actif financier (par exemple une monnaie fiat), c'est une valeur refuge, un outil utilisé par les investisseurs pour se protéger contre les variations du marché (il le vende quand le marché monte et l'achète quand le marché baisse.)

[84] Jean-Pierre Landau, Alban Genais, Op.cit.

[85] Ressource électronique sur (http://coinmarketcap.com) consulté le 31/10/2019.

monnaie, mais aussi le stockage de ce qu'on appelle des smart contract (contrats intelligents, soit une application particulière de la blockchain).

A partir de 2017, la plus puissante blockchain au monde s'annonce avec EOS, c'est la 3ème génération de la crypto-monnaie et qui offre une capacité à supporter des millions d'échanges par seconde.

4-1-Pourquoi y a-t-il autant de crypto-monnaie ?

Il existe des milliers de crypto-monnaies en dehors du bitcoin. Elles sont toutes à la fois une monnaie et un système de paiement, fonctionnent sur une blockchain, ont un projet et des modalités de création et de détermination du consensus. La création de crypto-monnaies est faite dans le but résoudre tel ou tel problème, améliorer tel ou tel processus, ou comprendre les besoins spécifiques de telle ou telle industrie. Les nouvelles crypto-monnaie sont créées soit par une fork[86], hard ou soft, soit par un ICO[87].

Derrière chaque monnaie se cache un projet, chacune s'adresse à un public particulier.

Une différence fondamentale entre les monnaies fiduciaires et les crypto-monnaies : les premières sont rattachées à un territoire, et les secondes à un usage. Comme il y a énormément d'usage et de publics potentiels, le nombre des crypto-monnaies, est appelé à exploser une fois que le grand public les aura adoptées et qu'elles auront un cadre légale.

4-2-Les familles de coins

Pour la plupart, l'utilisation du coin comme outil de transaction entre deux entités ne constitue pas le projet central de la société qui les émet. Le coin est plutôt le carburant qui permet d'utiliser le service proposé. Nous pouvons aussi voir les coins comme une action d'une entreprise qui a un projet.

Ce que cherchent à faire la plupart des créateurs de coins, c'est soit une utilisation sur leur plateforme, soit une application dans le monde réel.

[86] Un fork (bifurcation en français) est un événement qui se produit au sein d'une crypto-monnaie lorsque le consensus de la communauté qui participe à la blockchain associée est rompu, et qui donne naissance à une nouvelle crypto-monnaie.

[87] ICO (Initial Coin Offering : levée de fonds en crypto-monnaie) A revoir dans les sections suivantes.

Enée Bussac[88] les a regroupées dans 5 grandes familles et 25 sous familles[89]. Sachant qu'un coin peut appartenir à plusieurs sous familles et parfois à plusieurs familles[90].

Les 5 grandes familles sont :

- **Les coins purs :** qui n'ont vocation qu'à être une monnaie ;
- **Les financières :** celles qui ont vocation à assurer certaines fonctionnalités des banques et des bourses.
- **Les technologiques :** celles qui mettent à disposition de leur communauté un super ordinateur constitué de milliers ou millions d'ordinateurs en réseau, permettant de développer et d'héberger des applications ou des contrats intelligents par exemple ;
- **Les communautaires :** celles qui permettent d'améliorer des processus du monde réel, en se concentrant ou pas, sur une industrie ou un secteur en particulier.

4-2-1-Les coins purs

- Le cash numérique, qui remplace la monnaie fiduciaire pour acheter des biens et services online et offline ;
- Les anonymes, pour effectuer des transactions de manière anonyme ;
- Les sécuritaires, qui mettent l'accent sur l'aspect sécuritaire des transactions ;
- Les rapides, pour réaliser des transactions en quelques secondes ;
- Les people coins, laissent la communauté détentrice du coin décider de son évolution ;
- Les discounts, proposent des frais de transaction quasi-nuls.

4-2-2-Les coins financiers

- Les places de marché, permettent l'achat et la vente décentralisés de monnaies ou autres actifs numériques ;
- Les bancaires, proposent des services traditionnellement assurés par les banques, comme le transfert de monnaie entre entreprises ou filiales d'entreprises ;
- Les gestionnaires d'actifs, permettent de gérer des actifs et documents numériques de manière décentralisée ;
- Les solutions de paiement, proposent des solutions de paiement de plusieurs crypto-monnaies avec possibilité de conversion en monnaies fiduciaires ;

[88] Enée Bussac, auteur de l'ouvrage "*Bitcoin, Ether & Cie*", est créateur de Nouvelor, site d'information sur les crypto-monnaies.
[89] Cette classification est faite sur la base des 131 premiers coins en capitalisation boursière (au 31/12/2017).
[90] Les familles et sous familles des crypto-monnaies sont issues de la réflexion de l'auteur, et sont amenées à changer avec l'évolution du marché

- Les solutions de prêt, utilisent les crypto-monnaies comme support de prêt.

4-2-3-Les coins technologiques

- Les blockchains, apportent la technologie de la blockchain à des entreprises du monde réel pou gérer ou créer des actifs financiers, des processus, des documents ou des contrats ;
- Les plateformes d'applications, mettent des réseaux d'ordinateurs à disposition pour développer, tester et faire tourner des applications;
- Les smart contratcts, permettent à des entreprises ou développeurs de mettre en place des contrats intelligents pour améliorer leur efficacité, rendre moins chère leur exécution et servir de base dapps[91] ;
- Les Storage clouds[92], mettent des réseaux d'ordinateurs à disposition pour stocker des données ;
- Les IOT, servent de moyen de paiement et de communication entre machines connectées.

4-2-4-Les communautaires

- Les plateformes de contenu**,** permettent la mise à disposition et la vente de contenus notamment artistiques ;
- Les reward Systems, mettent en place des systèmes incitatifs pour encourager certains comportements, comme l'évaluation de services ou la lecture d'articles par exemple ;
- Les joueurs, proposent des plateformes de jeux et des casinos décentralisés ;
- Les réseaux sociaux, proposent des réseaux décentralisés et une monnaie que les membres peuvent s'échanger ;
- Les CrowdFunding, permettent de récolter des fonds pour financer un projet.

4-2-5-Les coins "monde réel"

- Les publicitaires, inventent un nouveau modèle de publicité décentralisée via la blockchain ;
- Les sectorielles, ciblent un secteur particulier ;
- Les research, permettent à la recherche d'avancer de manière plus efficace et collaborative ;
- Les prédictives, prédisent le futur à partir de nombreuses informations.

[91] Dapp est une application décentralisée fonctionnant sur un réseau lui-même décentralisé, comme celui de l'Ethereum.

[92] Storage cloud : stockage en nuage, est un modèle de stockage de données informatiques.

Certaines familles, comme les coins purs, sont amenées à perdurer, d'autres disparaîtront peut-être et d'autres apparaîtront avec notamment l'arrivée des coins émis par les Etats et les entreprises. Les stablecoins uniquement représentés à l'heure actuelle par Tether, qui réplique le dollar US et DGX, qui réplique l'or, sont amenés à devenir une famille de coins à part entière dans un futur proche[93].

SECTION 2 : CONCEPTS ET ÉLÉMENTS CLÉS DE LA CRYPTO-MONNAIE

Ce qui rend l'approche des crypto-monnaies complexe pour un grand nombre de gens, ce sont les multiples termes apparus avec ce phénomène, des termes souvent liés à l'informatique, qui constituent des éléments clés d'une crypto-monnaie.

Nous proposons donc d'expliquer quelques concepts essentiels au premier abord de ce domaine[94].

1-Un système de signature numérique (clé privée/clé publique)

Dans le monde réel, lorsqu'une personne signe un chèque ou un contrat, cette opération est authentifiée par sa signature, qui est unique à elle et qui est censée être infalsifiable. Elle est également authentifiée par le numéro de compte de cette personne, l'indicatif de sa banque, etc. Dans le monde des ordinateurs, nous avons un équivalent avec la signature numérique. Une signature numérique est associée à notre compte et une autre signature numérique est associée à chaque transaction.

Plus précisément en matière de cryptographie, l'astuce repose sur un couple : clé privée/clé publique.

1-1-Une clé privée absolument unique

La clé privée est une signature numérique secrète, soit un chiffre de 256 bits auquel personne d'autre que le détenteur de compte n'est censé avoir accès. Il est impossible de la falsifier.

Cette clé lui est fournie de manière aléatoire au moment où il acquiert un portefeuille (Bitcoin par exemple). Cette clé n'intervient pas dans les transactions. Elle est le sésame (mot de passe) qui nous donne accès à notre Wallet (portefeuille) en Bitcoin.

[93] Enée Bussac, Op.cit, P29.
[94] Tous les termes incompréhensibles liés aux crypto-monnaies sont expliqués dans le lexique.

La question qui se pose est : 256 bits est-ce un cryptage suffisamment sûr ? En réalité, le nombre de combinaisons possibles, soit 2^{256} est un nombre si énorme qu'il est quasi impossible de se le représenter mentalement. Autant le dire, il y a fort peu de chances que la clé privée puisse être retrouvée. Cette signature numérique qui nous identifie est donc infalsifiable.

1-2-Une clé publique dérivée de la clé privée

La force de ce système, c'est que, à partir de la clé privée, une deuxième signature est déduite, elle-même unique, appelée la clé publique.

La clé publique peut-être déduite de la clé privée. Toutefois l'inverse est impossible.

Ainsi dans le cas d'un échange de message sur une messagerie cryptée, c'est notre clé publique et celle de notre destinataire qui va favoriser un échange sûr. Alors :

- Pour accéder à nos messages, nous ferons usage de notre clé privée ;
- Pour échanger des messages, nous ferons usage de notre clé publique et celle de notre destinataire ;
- Notre destinataire ne pourra lui-même accéder à ses messages que grâce à sa clé privée[95].

La clé privée permet de signer les transactions et la clé publique, qui assimilable à un numéro de compte, autorise qui le souhaite à vérifier rapidement que la signature est correcte, c'est-à-dire que la transaction provient bien de celui qui possède la clé privée associée[96].

En faisant intervenir les deux clés publiques sur une transaction en Bitcoin par exemple, il va être possible à certains ordinateurs puissants de vérifier que cette clé publique associée au message est correcte. Tel va être le travail des mineurs.

2- Le registre des transactions : La Blockchain

L'autre problème qu'a voulu résoudre Nakamoto en créant le Bitcoin était d'éviter qu'une même transaction puisse avoir lieu deux fois de suite. Il a donc imaginé un système qui puisse faire en sorte qu'une somme d'argent ne puisse se trouver qu'à un seul endroit, et à un moment donné.

[95] Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P135.P136

[96] Jean Paul Delahay, "*les monnaies cryptographiques et les systèmes à blockchain*" consulté en ligne sur (inference-reviw.com) le 28/10/2019.

La solution trouvée par Nakamoto consiste en premier lieu à établir l'équivalent d'un livre de comptes géré de manière chronologique. Chaque opération est consignée dans un registre, avec un numéro chronologique correspondant à chaque transaction. Chaque transaction correspond à un bloc. D'où le nom de Blockchain ou "chaîne de blocs".

Une sécurité supplémentaire est apportée par le fait que chaque bloc intègre le hash du bloc précédent. Ainsi la transaction suivante comporte son propre hash (voir le lexique) mais aussi le hash de bloc (transaction) précédent.

Ainsi donc, chaque transaction opérée à un moment donné est unique. Elle est unique par :

- ✓ Le numéro de séquence de la transaction dans la blockchain ;
- ✓ Les clés publiques (signature numérique) impliquée dans la transaction ;
- ✓ Le hash de la transaction actuelle ;
- ✓ Le hash de la transaction précédente.

Telle est la blockchain. Un livre de compte qui contient à tout moment l'historique complet de toutes les transactions précédentes depuis la toute première[97].

Alors, par définition, la blockchain est une technologie à la même échelle qu'internet qui permet de stocker des données numériques, pour un coût minime, de manière décentralisée et sécurisée. Il s'agit d'une sorte de livre de compte ou de registre qui contient la liste de tous les échanges effectués entre utilisateurs du réseau. Ce registre décentralisé est infalsifiable. (Nous verrons le fonctionnement de la blockchain dans le chapitre IV.

La blockchain peut être comparée à un grand registre décentralisé accessible en ligne et partagé par un grand nombre d'utilisateur[98].

Il y a souvent confusion entre blockchain et Bitcoin (système).Le Bitcoin est une application particulière de la blockchain, qui repose sur une valeur monétaire : c'est une crypto-monnaie.

Dans le cas du Bitcoin, la technologie Blockchain est utilisée pour assurer la traçabilité des transactions, puisque chaque bitcoin a un code de cryptage propre. Ainsi un utilisateur ne peut

[97] Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P144.

[98] Gilles Quoistiaux, "*Bitcoin et crypto-monnaie*", Edition MARGADA, Bruxelles, 2019, P19.

se servir de ses bitcoins qu'auprès d'un seul destinataire correspondant à une seule transaction donnée[99]. C'est le réseau Peer-to-Peer (P2P) qui rend la blockchain infalsifiable.

❖ **Le réseau Peer-to-Peer (P2P : Pair à Pair)**

Le P2P désigne un type de réseau à l'intérieur duquel chaque ordinateur dispose de droits équivalents. Le P2P favorise la mise en relation de plusieurs internautes, c'est-à-dire d'amener les internautes connectés entre eux à s'échanger leurs propres fichiers[100].

Le pair à pair est un modèle d'échange où chaque entité du réseau est à la fois client et serveur, contrairement au modèle client/serveur. Dans un réseau P2P, les nœuds interconnectés (pairs) partagent les ressources entre eux sans avoir recours à un système administratif centralisé[101].

3-Le minage/Le consensus

Le minage (mining, ou fait de miner) est une activité qui permet de créer un consensus dans un système décentralisé, mais qui ne consiste pas à créer de la crypto-monnaie (par exemple des bitcoins), avec son ordinateur.

Dans les blockchain **Proof Of Work** (POW : preuve de travail) des crypto-monnaies, le minage est le fait de contribuer à la continuité du réseau en créant et ajoutant à la blockchain des blocs de transactions selon des conditions spécifiées dans le protocole de la crypto-monnaie (qui détermine notamment de quoi doit être constitué un bloc, à quelle fréquence les blocs doivent être crées, quel algorithme de consensus est utilisé et quelle récompense est accordée au mineur qui détermine le consensus) et l'algorithme de consensus (qui détermine qui "a raison", c'est-à-dire selon quel critère un mineur est choisi pour ajouter son bloc à la chaîne et ainsi déterminer le consensus).

Nous comptons trois types de participants dans le réseau d'une blockchain POW :

- **Les utilisateurs (users, aussi qualifiés de light nodes)** : qui forment la grande majorité des participants. Ils veulent recevoir et envoyer des paiements ou des données sans devoir s'occuper de la structure du système. Quand ils veulent procéder à une transaction, ils envoient l'information nécessaire de leur wallet à des nœuds et les

[99] Blog les Echos.fr, "*comprendre la blockchain en 5 points*" publié le 19/01/2016, consulté sur (lesechos.fr) le 28/10/2019.
[100] Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P144.
[101] WIKIPEDIA, Op.cit consulté le 28/10/2019.

mineurs du système la font suivre afin de la présenter pour vérification à d'autres nœuds et mineurs afin d'aboutir à un consensus.

- **Les nœuds (nodes ou full nodes)** : reçoivent des informations d'utilisateurs et d'autres nœuds, les vérifient et les transmettent encore à d'autres. Ils sauvegardent la blockchain entière afin de garantir la décentralisation du système.
- **Les mineurs** : contrôlent et vérifient les transactions que les utilisateurs souhaitent effectuer en se pliant au protocole de la monnaie et à l'algorithme de consensus. Ils perçoivent des frais sur chaque transaction pour rémunérer leur travail, en plus de la récompense fixe attribuée à chaque validation de bloc (ils sont rémunérés en un nombre de coins)[102]. Ce que nous appelons preuve de travail.

❖ **La preuve de travail**

Le travail des mineurs, en fonction de paramètres divers liés à la transaction et notamment sa propre signature, va consister à générer, grâce à la fonction SHA-256 (voir le lexique), un hash commençant par un certain nombre de zéros. Une fois qu'il a trouvé ce hash, le mineur peut soumettre sa preuve de travail, et n'importe qui pourra vérifier qu'elle est correcte. Le mineur diffuse donc son bloc aux autres membres de la communauté. S'il a été plus rapide que les autres mineurs, la nouvelle version de la blockchain qu'il vient de créer devient l'officielle et au passage, il récolte de nouveaux bitcoins (dans le réseau Bitcoin par exemple). Il récolte aussi une commission, soit un pourcentage minime de la transaction qu'il a validée[103].

4-Le smart contract

Littéralement "**contrat intelligent**".

Un smart contract est un concept crée en 1993 par Nick Szabo[104]. Un concept né avec l'environnement Ethereum[105], qui intègre dans sa boite à outil un langage de programmation, solidity, dédié à l'écriture de ces contrats intelligents et à leur inscription sur la blockchain[106].

[102] Enée Bussac, Op.cit, P57.P58.

[103] Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P148.

[104] Enée Bussac, Op.cit, P52.

[105] Ethereum, crée par Vitalik Buterin aidé par Nick Szabo, a constitué la 1ère évolution majeur des crypto-monnaies. Il est ainsi considéré que le Bitcoin représente la 1ère génération de crypto-monnaie et que l'Ethereum et les monnaies basées sur lui ont constitué la seconde génération.

[106] Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P156.

Les contrats intelligents sont des protocoles informatiques qui permettent de vérifier et d'exécuter en temps réel un contrat juridique ou financier, ou tout type d'accord que plusieurs contreparties peuvent codifier avec peu, ou pas du tout, d'interventions humaines.

Un smart contract est un contrat dit auto-exécutant. Il implique deux points fondamentaux :

- ✓ Grâce à la blockchain et à son réseau de participants, le contrat pourra s'exécuter de manière automatique ;
- ✓ En cas de litige, les participants à la blockchain serviront d'arbitres pour la résolution du conflit.

SECTION 3 : L'ÉCOSYSTÈME DES CRYPTO-MONNAIES

Le monde des crypto-monnaies est un marché pur, c'est encore un magma où se forme la valeur donc le cours de chacune.la technologie de la blockchain, la recherche de consensus, la possibilité offerte à chacun de contribuer à l'essor de ces monnaies par le minage, etc., apportent de vrais avantages en terme de "démocratie" et d'économie de coûts et de temps, mais nous ne sommes pas encore capable de fixer une valeur à ces avantages et c'est précisément ce qui entrain de se passer sur les marchés.

Il y a beaucoup de vrais projets avec la vraie valeur ajoutée derrière plusieurs de ces monnaies comme Ethereum, Salt ou Tenx par exemple, c'est pour cela que l'investisseur avisé qui a une optique de long terme se doit de bien regarder ce qu'il y a derrière chaque monnaie dans laquelle il souhaite investir, où il sera hautement récompensé.

1-Les Wallets

1-1-Définition

Un wallet, comme son nom l'indique, est un portefeuille où les coins sont stockés. Enfin, pas tout à fait, les coins sont virtuels. Quand nous achetons un coin ou une partie de coin, nous acquérons en fait le droit de l'utiliser et pour ce faire, il est attribué à une de nos public addresses qui est communiquée au vendeur et à la blockchain. Une fois que nous avons acheté notre coin, notre private key est ce qui nous donne le contrôle de la public address à laquelle est rattaché ce coin et donc du coin. C'est aussi ce que stock un wallet : notre private key (clé privée) qui nous donne le contrôle de nos public addresses (clés publiques). Si nous perdons

notre private key, nous perdons le contrôle de nos coins. Il n'y a aucun moyen de les retrouver car il n'y a pas de système ou autorité centrale régulatrice[107].

1-2-Les types de wallets

Il existe plusieurs types de wallets, autrement dit de manière de stocker une clé privée, de la plus sûr, qui est aussi la moins pratique, à la moins sûr, qui aussi la plus pratique :

1-2-1-A l'ancienne sur papier

C'est peut être la manière la plus sûr, car complètement offline, mais cela demande une bonne organisation.

1-2-2-Sur un hardware wallet

Un hardware wallet est un périphérique informatique qui ressemble à une petite tablette ou une clé USB. Il stocke et encrypte une clé privée, et offre diverses fonctions comme le transfert de coins, la génération des clés publiques et l'affichage du solde des coins contrôlés. Comme un hardware wallet est un objet physique, il peut être débranché de l'ordinateur. Il est pratiquement inviolable par des hackers et inutilisable sans le code d'accès, il reste une solution très sûre et relativement pratique.

1-2-3-Sur un desktop wallet

Un desktop wallet est une application installée sur un ordinateur, une tablette ou un smartphone, et qui remplit les mêmes fonctions qu'un hardware wallet. Comme le desktop wallet est installé sur un périphérique *à priori* connecté à internet, le risque est plus grand que celui-ci soit piraté, même si cela reste très peu probable étant donné le niveau d'encryption des données, mais il est plus pratique, car toujours sur un ordinateur/tablette/smartphone, et il coûte, *à priori*, moins cher qu'un hardware wallet.

1-2-4-Sur un exchange wallet

Le propriétaire des coins peut laisser ses dernières sur un exchange, qui propose toujours des services de stockage, d'affichage des soldes, d'envoi et réception de coins, etc. Dans ce cas c'est l'exchange qui gère la clé privée et pas le propriétaire des coins (les clés publiques aussi sont générées par l'exchange), ce qui fait que le propriétaire des coins est à la merci de cet exchange et qu'il ne possède pas vraiment ses coins. Il possède le contrôle de coins qui sont contrôlés eux-mêmes *in fine* par l'exchange car c'est ce dernier qui détient la clé privée.

[107] Enée Bussac, Op.cit, P103.

2-Les exchanges (places de marché)

2-1-Définition

Les exchanges sont des plateformes dédiés au trading de crypto-monnaies proposant des fonctions de vente, achat et wallet (stockage, envoi et réception de crypto-monnaies). **Coin Market Cap**[108] en répertorie plus de 10 000 début Mai 2018. Absolument fondamentaux dans le monde des crypto-monnaies, très rentables et autrefois surchargés, les exchanges sont les grands gagnants et les pivots du marché des crypto-monnaie : ils encaissent des commissions sur les transactions, dont les volumes ont augmenté exponentiellement en 2017. Le marché a atteint les 200 milliards de dollars tout début novembre, 300 fin novembre et 800 fin décembre pour retomber en dessous des 300 début avril 2018[109].

Coinbase/kraken : exchanges qui permettent d'échanger des crypto-monnaies entre elles, de les convertir en monnaie fiduciaire ou de les échanger contre une monnaie émise par une banque centrale.

Bitrex/Binance : permettent d'échanger des bitcoins contre n'importe quel altcoin[110].

2-2-Un comparatif des 06 plateformes de trading les plus actives

Tableau N°2 : Un Comparatif des 06 plateformes de trading les plus actives

plateforme	description	localisation	volume	Monnaie disponible	frais	Paiement & échange
Coinbase	Plateforme populaire et très simple d'utilisation. Echanges simplifiés. Vérifications rapides. Disponible en français. Application mobile.	USA	Elevé	Bitcoin, Litecoin, Ether	Elevé	Carte bancaire Virement Crypto-monnaies

[108] Coin Market Cap (http://coinmarketcap.com) est un site qui publie les cours de chaque monnaie, sa capitalisation boursière, la variation de son cours sur 24 heures, 7jours ou d'autres durées, les marchés sur lesquels elle est cotée, les données historiques de son cours, le site web de l'entité derrière la monnaie et aussi les coins qui ont été introduits récemment.

[109] Enée Bussac, Op.cit, P80.

[110]Altcoin est une crypto-monnaie alternative, un autre coin que le bitcoin, le terme est abrégé régulièrement en anglais en" Alts".

Binance	Plateforme réputée pour sa stabilité et sa rapidité. Monnaie de la plateforme.	Hong-Kong, Japon, Corée du sud	Très élevé	+ 200	Faible	Crypto-monnaies uniquement
Kraken	Une des plateformes les plus populaires en Europe. Les crypto-monnaies les plus connues sont présentes.	USA	Moyen	Bitcoin, Litecoin, +15	Moyen Faible	Virement Crypto-monnaies
Cex	Plateforme agréable. Plusieurs crypto-monnaies disponibles. Facile pour les débutants.	Royaume-Uni	Moyen	Bitcoin, Litecoin, +8	Moyen	Carte bancaire Virement Crypto-monnaies
GDAX	Plateforme proposant des fonctions avancées sur une interface ergonomique. Même société que Coinbase.	Royaume-Uni	Très élevé	Bitcoin, Litecoin, Ether	Moyen	Carte bancaire Virement Crypto-monnaies
Bittrex	Très grand choix de crypto-monnaies. Interface claire. Fonctionnalités avancées disponibles.	USA	Elevé	+ 200	Moyen	Crypto-monnaies uniquement

Source : www.cryptoencyclopedie.com

2-3-Les particularités du marché des crypto-monnaies[111]

Le marché des crypto-monnaies diffère de celui des actifs financiers classiques par les caractéristiques suivantes :

- La cotation a lieu 24h/24 et 7j/7 ;
- Il n'y a pas pour le moment aucune régulation globale, donc aucune sécurité pour les investisseurs autre que celle apportée par les exchanges ;
- Les frais et délais sont généralement très réduits (entre 0,1% et 1,5% du volume de la transaction suivant les exchanges) ;

[111] Enée Bussac, Op.cit, P81.

- Les variations de cours sont relativement grandes (+ou -5% en 24h) ;
- On peut acheter une fraction d'une monnaie : dans le cas du bitcoin, on peut théoriquement acheter un cent millionième de bitcoin (unité appelée Satoshi) ;
- La monnaie dominante sur ce marché est le bitcoin par sa capitalisation boursière (plus de 40% à elle seule) et le fait qu'elle peut être échangée contre toutes les autres crypto-monnaies et les monnaies fiduciaires majeures.

3-Les ICO (Initial Coin Offering)

Une ICO n'est jamais qu'un smart contract particulier[112]. C'est une levée de fonds en crypto-monnaies qui permet aux start-ups de la blockchain d'avoir accès à un financement très rapidement[113]. C'est une introduction en Bourse version crypto-monnaies[114]. Au lieu d'émettre des actions sur le marché primaire d'un pays donné (en Bourse) et de satisfaire les lourds coûts et exigences réglementaires d'une IPO (Initial Public Offering)[115], une entreprise émet une nouvelle crypto-monnaie généralement, qu'elle vend elle-même, avec le but d'être cotée sur des exchanges indépendants dans un futur proche.

L'idée est d'amasser des crypto-monnaies qui ont de la valeur, le Bitcoin et l'Ether, notamment pour financer la start-up derrière l'ICO en échange de la nouvelle monnaie qu'elle émet et propose dans ce cadre.

Dans le cas d'une ICO, il est rare que les sociétés qui lèvent des fonds aient une activité déjà établie. La plupart des ICO se déroulent selon le processus suivant :

- ✓ Un groupe de programmeur publie sur le Net un document de présentation de leur projet dit "livre blanc" (en anglais white paper) ;
- ✓ Si le livre blanc suscite de l'intérêt, il commence à faire l'objet de débats sur les forums s'intéressant aux crypto-monnaies ;
- ✓ Ensuite, les créateurs du projet commencent à diffuser les communiqués réguliers et à développer une communication publicitaire autour de leur opération ;
- ✓ Une prévente de" tokens"[116](jeton) de la monnaie virtuelle est réservée à des opérateurs professionnels ;

[112] Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P158.
[113] JDN en ligne consulté sur (journaldunet.com) le 23/10/2019.
[114] Enée Bussac, Op.cit, P118.
[115] Voir tableau de comparaison IPO/ICO.
[116] Dans l'univers des crypto-monnaies, un token désigne un actif numérique transférable entre deux parties sur internet sans avoir besoin, pour cela de l'autorisation d'un tiers. Il s'agit d'un instrument financier utilisé par les entreprises dans le cadre des ICO, pour lever des fonds.

- ✓ La vente de tokens démarre, les souscripteurs offrent des bitcoins, des ethers en échange de tokens qu'ils recevront à la fin de l'ICO ;
- ✓ A la conclusion de l'ICO, le token est officiellement émis et les souscripteurs reçoivent ce qui leur est dû ;
- ✓ Si le token a suffisamment de succès, il est alors côté sur les places de marché des crypto-monnaies.

Depuis janvier 2017, les ICO ont permis aux start-ups de faire rentrer près de 9 milliards de dollars dans leurs caisses. Et malgré la baisse du Bitcoin, la première moitié de 2018, 800 millions de dollars ont été levés[117].

❖ **Une comparaison IPO/ICO**

Tableau N°03 : Une Comparaison entre IPO/ICO

	IPO	ICO
Distribution	A travers un échange réglementé	A travers une plateforme décentralisée (Ethereum, Wave…)
Projet	Une compagnie privée qui devient publique	Ecosystème reposant sur un protocole sans cadre legal clairement définit
Titre	Actions et Obligations offrant des droits légaux (vote, action collective…) et financiers (dividendes, intérêts…)	Jetons qui offrent des droits et retour sur investissements différents pour chaque projet.
Objectifs	Lever des fonds pour investir	Lever des fonds pour investir, mais surtout de développer le nombre d'utilisateurs du protocole

Source : BEX, Blockchain exchange (www.bex.grou) plateforme d'échange de crypto-monnaies

[117] Enée Bussac, Op.cit. P159

CONCLUSION

Dans la taxonomie de la corolle des monnaies, les crypto-monnaies associent trois caractéristiques principales. D'abord, elles sont numériques, visent à constituer un moyen de paiement commode et s'appuient sur la cryptographie pour empêcher leur contrefaçon et les transactions frauduleuses. Ensuite, bien qu'elles soient créées de manière privée, elles ne sont le passif de personne en particulier : elles ne peuvent pas être remboursées et leur valeur tient uniquement au fait que l'utilisateur s'attend à ce que d'autres utilisateurs continueront de les accepter. Enfin elles permettent un échange numérique entre pair.

Les crypto-monnaies visent à constituer une nouvelle forme de monnaie et promettent de maintenir la confiance dans la stabilité de leur valeur au moyen d'une technologie décentralisée. Elles associent trois éléments, une série de règles (protocole), un registre comptabilisant l'historique des transactions (blockchain) et enfin, un réseau décentralisé de participants.

Les crypto-monnaies sont arrivées et, tout comme internet, le partage de fichiers et l'information libre. Elles ne peuvent être arrêtées. Le monde de la finance est sur le point de changer drastiquement.

Comme d'autres industries qui ont eu à faire face à des changements disruptifs, l'industrie de la finance (dont les banques, la gestion de fonds, les organismes de crédits, etc.) devra s'adapter. Ceux qui ne le feront pas vont vite se trouver remplacés par ceux qui l'auront fait.

ChapitreIII:

L'impact des crypto-monnaies, leurs Enjeux et Perspectives

CHAPITRE III : 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 renouvèle 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 211-2012, Tracfin[118] 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 danse tout en raison de leurs usages licites qu'illicites[119]. 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

[118] Tracfin (acronyme de Traitement du Renseignement et Action contre les Circuits Financiers Clandestins) est un organisme du ministère de l'économie et des finances de France, chargé de la lutte contre la fraude, le blanchiment d'argent et le financement du terrorisme, crée par la loi N°90-614 du 12/07/1990 à la suite du sommet de l'Arche du G7(juillet 1989).

[119] 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.

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 maitriser et orienter ces crypto-monnaies, et limiter leurs risques.

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 réserves 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'information[120].

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,

[120] Enée Bussac, Op.cit. P177-180.

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 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, continuer 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 prés 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 tout un 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 efficients, 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 nos achat sur Amazon en « Amazoncoin »,

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 efficients, 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 une certaine public address à un certain moment équivaudra 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 règlementation. 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[121] 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.

[121] Enée Bussac, Op.cit. P219-222.

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 (Consensys[122] par exemple) 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 de lourdes conséquences financières. Si les conditions, les montants ou les échéances, par exemple, sont

[122] Consensys est une solution technologique de blockchain.

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 exchanges et des pourvoyeurs de public addresses, 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 reconnaitre les public addresses 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 addresses (adresses publiques)

Pour rappel, les public addresses permettent de recevoir des coins, un peu comme l'IBAN d'un compte en banque. Quand nous envoyons des coins à une public adress, nous ne pouvons pas y insérer de message comme dans un virement SEPA[123]. Pour pallier cela, c possible de générer *via* un wallet un nombre quasiment infini des public addresses dérivées d'une clé privée pour recevoir des coins, ce qui a pour conséquence qu'une société ou un exchange à qui l'envoie des coins est destiné va générer une public adress 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 addresses permettent donc d'identifier expéditeurs et destinataires de coins, pour vu que ceux-ci se soient fait connaitre (c'est-à-dire que l'utilisateur XYZ informe les personnes et sites pertinents que sa public address est xyzxyz).

3-2-la simplification et l'amélioration des paiements

Nous l'avons vu les crypto-monnaies donnent aux monnaies une quatrième fonction, 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[124].

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

[123] La zone SEPA couvre actuellement 27 états membres de l'UE ainsi que la Suisse, le Liechtenstein, Monaco, Norvège et l'Island. 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.

lui-même affecter ces revenus à trois recettes différentes : la TVA, l'accise[125] 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 dés 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 address par exemple. Sont affichées pour une transaction donnée les public addresses d'émission et de réception, les montants échangés, les frais induits, etc. si nous nous intéressons à un bloc, nous pourrons 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 address à telle public address à telle date et telle heure. Mais tout cela ne nous servira à rien si nous ne savons pas qui se cache derrière les public addresses. Pour que ces paiements soient traçables et donc intéressants

[125] Le droit d'accise est un impôt indirect perçu sur la consommation, parfois aussi le seul commerce de certains produits, en particulier le tabac, l'alcool et le pétrole et ses dérivés.

notamment pour l'administration fiscale mais aussi les banques ou entreprises, il faut pouvoir associer une public address 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'exchange ainsi que les public addresses 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 address 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 exchanges de cesser de proposer des monnaies anonymes, comme l'a fait récemment le Japon[126].

SECTION 2 : LES ENJEUX, RISQUES ET LIMITES DES CRYPTO-MONNAIES

La banque des règlements internationaux BRI, qui regroupe 60 Banques Centrales du monde entier, publie une étudie 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*."[127] Résume Hyun Song Schin, le responsable de la recherche à la BRI[128].

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

[126] Enée Bussac, Op.cit. P189.
[127] La tribune, publié sur (www.latribune.fr), le 18/06/2018, et consulté le 03/11/2019.
[128] BRI, La Banque des Règlements Internationaux (en anglais Bank Of International Settlements, BIS) est une organisation financière internationale créée en 1930 sous la forme juridique d'une société anonyme, dont les actionnaires sont des banques centrales. Située à Bâle en Suisse, elle se définit comme la" Banque des Banques centrales". Sa principale mission est la coopération entre Banques Centrales. Elle joue un rôle déterminant dans la gestion des réserves de devises de ces institutions. Elle héberge entre autres le comité de Bâle.

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'unité émise sans indexation de la valeur de celles-ci induit un risque de spéculation conduisant à une forte volatilité du cours[129].

1-2-Manque de transparence

A l'heure actuelle, l'ouverture d'un portefeuille[130] 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 œuvres, 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 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.

[129] 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.

[130] Le terme portefeuille de monnaie virtuelle est indifféremment utilisé avec celui de compte en monnaie virtuelle.

1-3-Extraterritorialité

L'utilisation des monnaies virtuelles permet, grâce aux facilités d'internet, de dématérialiser, d'anonymiser 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[131] 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[132] 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 ;

[131] Rapport annuel 2014 de Tracfin et un groupe de travail sur l'encadrement des monnaies virtuelles, Op.cit
[132] La validation d'une transaction en Bitcoin est de l'ordre d'une dizaine de minutes, sachant que ce temps se trouve fortement diminué dans le cas de nombreuses 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 inferieurs à ceux du réseau bancaire ou des sociétés de transfert international de fonds. Une étude de Goldman Sachs[133] 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[134]..

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 à ces monnaies : des CFD (Contract For Difference)[135] 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 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 ;

[133] 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..

[134] Goldman Sachs, "*tout sur Bitcoin*", Global macro research, top of mind, N°21, mars 2011.

[135] 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.

- ✓ 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 du 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 Tracfin 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 terrorisme[136].

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 plateforme mondiale d'échange de bitcoin, MtGox[137]), illustrent la vulnérabilité de l'écosystème des crypto-monnaies et le niveau élevé des risques associés, en l'absence de mécanismes de garantie[138].

[136] 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.
[137] 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.
[138] Rapport annuel 2014 de Tracfin et un groupe de travail sur l'encadrement des monnaies virtuelles, Op.cit.

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 an[139].

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

[139] Enée Bussac, Op.cit, P144.P145.

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 PIHR[140] 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[141].

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 et 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 millier 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 qui minent le bitcoin et d'autres représente un vrai problème qui prend des proportions

[140] 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.

[141] Enée Bussac, Op.cit, P146.

inquiétantes à mesure que le mining pools[142] investissent à coups de millions dans du matériel informatique et dans des fermes dans des régions froides. Tout ça pou faire tourner une fonction de hashage des milliards de fois par seconde pour obtenir une empreinte qui commence par le bon nombre de zéro[143].

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 1er 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 mondial[144].

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[145].

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**[146] 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 maitriser les risques identifiés ?

[142] 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.
[143] Enée Bussac, Op.cit, P151.
[144] WIKIPEDIA. Consulté sur (fr.wikipedia.org) le 15/11/2019.
[145] Banque de France, Focus, Op.cit.
[146] Proof Of Stacke (ou preuve d'enjeu en français) fait partie des mécanismes de consensus blockchain les plus courants. Le Pos ne nécessite aucune forme de minage et repose sur un mécanisme tout à fait différent. L'algorithme de preuve d'enjeu implique que différents utilisateurs du réseau mettent en dépôt de leurs possessions en crypto-monnaies pour devenir **minters** (on ne parlera donc pas de mineurs mais de "minters», forgeur), l'algorithme se base ensuite sur la tête de la blockchain (soit le dernier bloc de chaîne) pour sélectionner aléatoirement un minter et lui offrir le droit de créer le prochain bloc.

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 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 régulation[147] 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[148] :

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)[149] préconisent un élargissement de l'encadrement des prestations de services associés aux crypto-monnaies de manières 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

[147] Dans notre travail, nous nous appuyons sur les études, analyses et propositions faites, par les institutions et autorités de contrôle françaises, sur les crypto-monnaies.

[148] Il convient de signaler que ces recommandations sont fondées sur la base d'une analyse arrêtée au mois de juin 2014 par Tracfin et son groupe de travail constitué de : la direction générale du trésor (DGT), la direction générale des douanes et droits indirects (DGDDI), la direction générale des finances publiques (DGFiP), la direction générale de la concurrence, consommation et de la répression des fraudes (DGCCRF), la direction des affaires criminelles et des grâces (DACG), la direction centrale de la police judiciaire (DCPJ),la direction générale de la gendarmerie (DGGN), l'autorité des marchés financiers (AMF), et l'autorité de contrôle prudentiel et de résolution (ACPR).

[149] 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.

libellés dans une monnaie ayant cours légal, et pas de prestation associés 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 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)[150]. Cette directive prévoit, en effet, d'assujettir à cette réglementation les acteurs proposants 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[151].

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 compléter 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

[150] 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.
[151] Banque de France, Focus, Op.cit.

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 nouveau type d'offre. Ce travail sera mené en coordination avec les autres autorités publiques concernées[152].

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 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 national, 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.

[152] Banque de France, Focus, Op.cit.

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[153] ont été formulé 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 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[154] :

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

[153] Rapport annuel 2014 de Tracfin et un groupe de travail sur l'encadrement des monnaies virtuelles, Op.cit.
[154] Ibid.

Tableau N°04 : Une synthèse des trois piliers de la stratégie de lutte, proposée, contre les risques des crypto-monnaie

Volet Régulation & Coopération	Volet Encadrement de l'utilisation	Volet Connaissance & Investigation
• Règlementer les services offerts à l'interface entre la sphère réelle et les crypto-monnaies ; • Encadrer 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 régulation 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 coté 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.

ChapitreIV:

Bitcoin & Crypto-monnaie

CHAPITRE IV : BITCOIN & CRYPTO-MONNAIE

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[155]", 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 monnaie[156].

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 entrain 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.

[155] 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.

[156] Cyril fièvet," *Comprendre Bitcoin et les crypto-monnaies alternatives*." Edition Lbrinova, 2014, P3.

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.

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 envions 11 700 dollars[157]. Alors d'où vient cette monnaie ? Et comment fonctionne-t-elle ?

1-Qu'est ce que le 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

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

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[158].

L'idée fut présentée pour la première fois en novembre 2008 par une personne, ou groupe de personnes, sous le pseudonyme de Satoshi Nakamoto[159]. Le code de l'implémentation de référence fut quant à lui publié en 2009[160].

Les symboles utiliser pour représenter Bitcoin sont : BTC, XBT, ₿ ou Ƀ[161] ou encore □[162].

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 nommé le Satoshi en hommage à son créateur et elle égale à 0,00000001BTC (1BTC=1/100000000satoshi)[163].

Le bitcoin peut également être subdivisé en millibitcoin (mXBT, 1mXBT=0,001XBT), microbitcoin (µXBT, parfois dénommé bit) ou nanobitcoin (nBXT)[164].

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 créer 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 certain il constitue un moyen de paiement et pour d'autres, un produit de spéculation[165].

---

[158] Adli Takkal Bataille, Jacque Favier,"*Bitcoin, la monnaie acéphale*", CNRS Editions, 2018, P94.
[159] 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.
[160] Prypto, "*Bitcoin pour les nuls*", Edition First, Paris, 2018, P11.
[161] Source (bitcoin.fr) consulté le 13/11/2019.
[162] Faisant suite à une proposition d'ajout, le consortium Unicode a accepté en novembre 2015 d'ajouter le bitcoin parmi ses caractères.
[163] Adli Takkal Bataille, Jacque Favier, Op.cit, P95.
[164] WIKIPEDIA sur (wikipédia.org) consulté le 12/11/2019.
[165] Le G20 considère que le Bitcoin est un "crypto-actif" qui ne remplit pas le rôle d'une monnaie, le terme actif fait alors référence à des "actifs virtuels" stockés sur un support électronique permettant à une communauté d'utilisateurs les acceptant en paiement de réaliser des transactions sans avoir à recourir à la monnaie légale.

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, 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 2010[166].

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[167].

Le 27 décembre 2012, la fondation Bitcoin est créée.

❖ **Tableau N°5 : 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 1er bloc de transaction de blockchain bitcoin.
12/01/2009	1ère 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.

[166] WIKIPEDIA, Op.cit.

[167] Clé d'alerte est une clé cryptographique privée unique permettant d'atténuer les effets d'une attaque potentielle sur le système Bitcoin, comme la découverte d'une faille cryptographique permettant de modifier *à posteriori* les transactions ou la prise de contrôle de plus de 51% des nœuds du réseau (connue sous le nom d'attaque 51%). Les opérations des nœuds du réseau peuvent lors d'une alerte, soit avertir leurs usagers, soit stopper tout enregistrement de transaction.

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.
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 1ère fois les 1000 dollars.
01/04/2017	Le Japon reconnait 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 (jounaldunet.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 payants[168].
- Le 14 février 2013, le site communautaire Reddit met en place un système permettant d'acheter des "Reddit Gold" avec des bitcoins.
- Le 16 février 2013, le site de stockage en ligne Mega[169], 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% depuis2016. Il y a 5 457 bitcoin ATMs dans le monde au 1er septembre 2019[170].

- 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 compagnes 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 progressivement au Bitcoin.

[168] WIKIPEDIA, Op.cit.
[169] 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.
[170] Statista, le nombre de bitcoin ATMs dans le monde, consulté en ligne sur (fr.statista.com) le 16/11/2019.

- En décembre 2017, le ministre français des Comptes publics, Gérald 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[171] Eugen Von Böhm-Bawerk[172], Ludwig Von Mises[173]et Friedrich A. Hayek[174], 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

[171] Source WIKIPEDIA, Op.cit.

[172] **Eugen Von Böhm-Bawerk** (1851-1914), est un économiste, professeur d'université, écrivain et homme politique, membre de l'académie autrichienne des sciences et l'académie royale des sciences de Suède, il contribue au développement de l'école autrichienne d'économie, occupe différents postes au ministre des finances à Vienne, conseiller 1889, ministre 1895 ensuite 1900-1904,…. Parmi ses contributions, nous trouvons sa critique de la théorie marxiste (les incohérences de Marx et le "le problème de la transformation", les difficultés abstraites et empiriques posées par la théorie de la valeur travail, l'investissement comme détour de production, etc.

[173] **Ludwig von mises** (1881-1973), est un économiste autrichien puis américain qui a eu une influence importante sur le mouvement libéral et libertarien moderne.il enseigne d'abord à Vienne puis à Genève jusqu'en 1940. Fils d'une famille juive de Galicie (Ukraine) et inscrit sur la liste noire des nazis, il fuit aux Etats-Unis de 1945 à 1969. Naturalisé américain en 1946, il meurt à New York en 1973.parmi ses œuvres : théorie de la monnaie et du crédit 1912, analyse économique et sociologique 1922, libéralisme 1927, les problèmes fondamentaux de l'économie politique 1933, la mentalité anti-capitaliste1956, le fondement ultime de la science économique 1962, etc.

[174] **Friedrich A. Hayek** (1899-1992) est un économiste et philosophe britannique originaire d'Autriche. Il partagea avec Gunnar Myrdal le Prix Nobel d'économie en 1974 pour "ses travaux pionniers dans la théorie de la monnaie et des fluctuations économiques et pour son analyse de l'interdépendance des phénomènes économiques, sociaux et institutionnels". Il est considéré comme un théoricien social ainsi qu'un penseur politique majeur du XX^{e}, et son compte rendu sur la manière dont le changement des pris communique des informations aux individus les aidant à coordonner leurs plans est largement considéré comme une réalisation importante en économie, conduisant à son Prix Nobel. Parmi ses grands travaux économiques la théorie autrichienne de la conjoncture en plus de ses critiques du keynésianisme.

déséquilibre généralisé ne peut plus perdure 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 – c'est-à-dire de la donnée- stockée dans un ordinateur ;

✓ Le système ne satisfait pas au « théorème de la régression[175] », ce qui explique que 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.

[175] 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 décrétées : l'euro vient du franc, de la lire, etc. qui eux-mêmes étaient grosso modo échangeables contre de l'or jusqu'en 1971.

- 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[176].

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 crées, 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[177].

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 2028[178].

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.

[176] Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P21, P22.
[177] Prypto, Op.cit.P51.
[178] Gilles Quoistiaux, Op.cit, P17.

Le prochain halving devrait avoir lieu aux alentour de Mai - Juin 2020, le récompense passera donc à 6,25 bitcoins par bloc[179].

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 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).

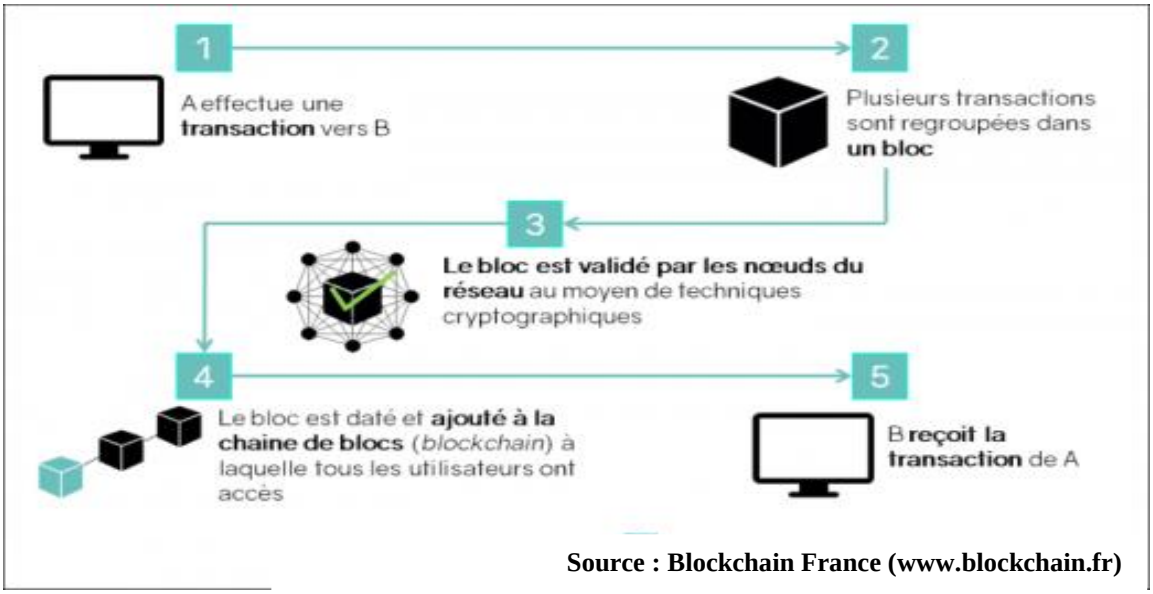
Cette blockchain, qui constitue une base de données contenant l'historique de tous les échanges effectués entre utilisateurs, est partagée pars ses différents utilisateurs, sans intermédiaire, et permet à chacun de vérifier la validité de la chaîne (appelé aussi logiciel de minage)[180].

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 N°04).

[179] Crypto-France publié le 16 novembre 2017, consulté en ligne sur (crypto-France.com) le 13/11/2019.
[180] Newsletter N°1 CONOBAFI (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.

Figure N° 04 : 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-Comment les bitcoins sont-ils crées ?

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[181].

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"[182].

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-Comment s'effectue une transaction bitcoin ?

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 porte feuille).

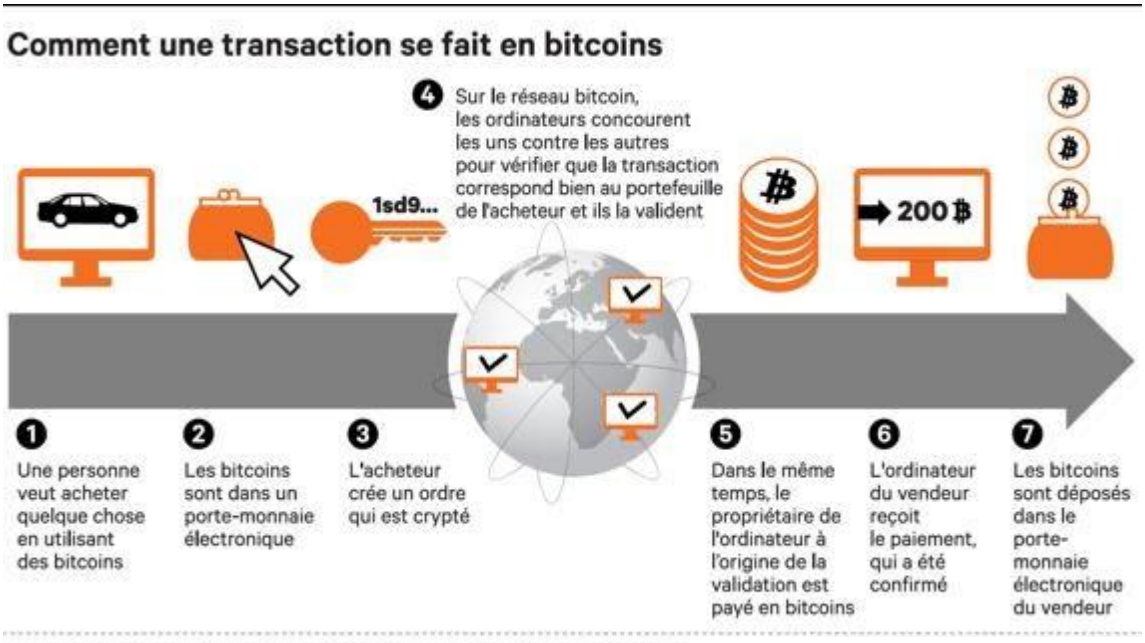
[181] Coin List,"*Bitcoin : la première crypto-monnaie*" consulté en ligne sur (coinlist.me/fr/altcoins/bitcoin) le 15/11/2019.
[182] Crypto-monnaie.Pro,"minage de crypto-monnaies" consulté en ligne (crypto-monnaie.pro) le 15/11/2019.

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 N°05).

Figure N° 05 : Comment s'effectue une transaction bitcoin ?



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[183].

SECTION 2 : ÉVOLUTION DU 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, malgré 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

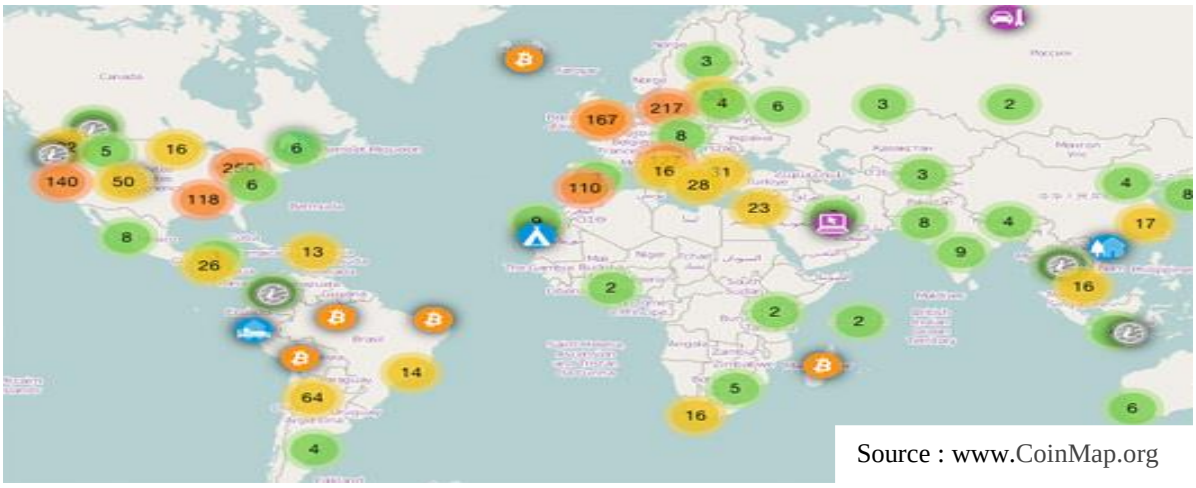
1-1-Le Bitcoin, une monnaie qui s'inscrit dans un processus de mondialisation

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

[183] Gilles Quoistiaux, Op.cit, P37.

niveau des pays développés notamment la Triade[184] tandis que l'Afrique réalise très peu de transaction (voir figure N°06). 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 N° 06 : 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 ventes sur internet (Bitfinex pour le dollar, Okcoin pour le yen…)[185]. 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.

[184] La triade désigne l'ensemble des trois groupes de pays les plus puissants de la planète : Amérique du Nord (Etats-Unis et Canada), Europe occidentale (Union européenne, Norvège, Suisse) et Asie pacifique (Japon, Corée du Sud, Taïwan, Singapour).

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

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 $[186].

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.

A partir de 2012, le cours commence à s'accroître 0,562 $ pour un bitcoin au 1er janvier 2012, 400 $ pour un bitcoin, au 1er janvier 2014, 1028 $ pour un bitcoin au 1er 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)[187].

Graphique N°01 : Evolution Du Cours De Bitcoin (2009-2019)

Source : www.blockchain.info

❖ Au lancement du bitcoin, en 2009, il n'y avait presque pas de mineurs sur le réseau. La difficulté du minage s'adapte aux 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 entraine la première bulle spéculative, et le prix du bitcoin prend réellement son envole entraînant un accroissement de la compétition entre mineurs.

[186] Source Lockchain-expert consulté en ligne sur (lockchain-expert.com) le 14/11/2019.
[187] Source Blockchain.com consulté en ligne sur (blockchain.com) le 13/11/2019.

❖ 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'au 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 enrailler la tendance baissière.

❖ 2019. Il est clair que le prix du bitcoin a connu une forte chute en 2018, entrainant avec la majorité des autres altcoins. Le prix des crypto-monnaies est en effet corrélé à celui du bitcoin

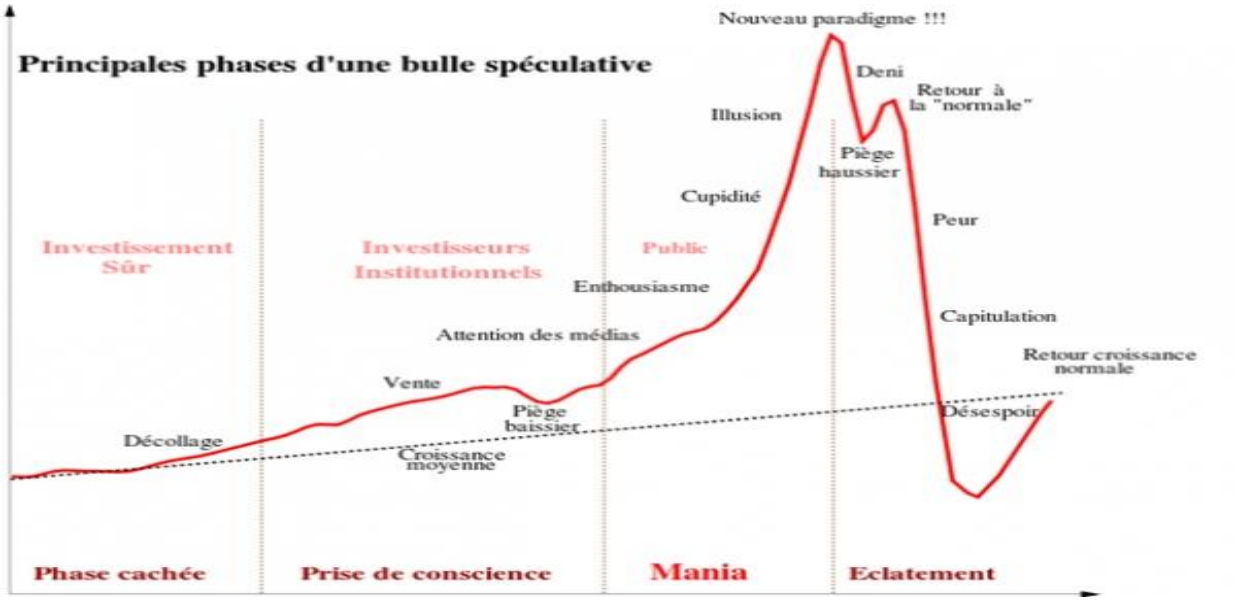
Jusqu'où les prix vont descendre, c'est difficile à dire. La courbe de la bulle peut prendre plusieurs formes.

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.

Graphique N°02 : 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 parcourt que celui des actions Apple et Amazon[188].

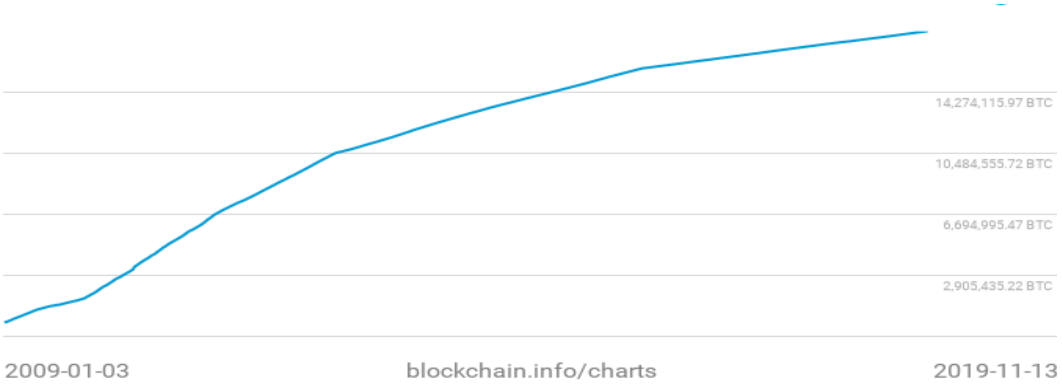
1-3-Evolution des transactions en bitcoins

Bien qu'essentiellement acquis à des fins spéculatives, le Bitcoin peut-être également utilisé pour les transferts internationaux entre particuliers et comme monnaie de paiement pour les commerces.

Dans de nombreux pays émergant 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 utilisé comme valeur refuge par certaines personnes pour éviter la fluctuation de leur propre monnaie.

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

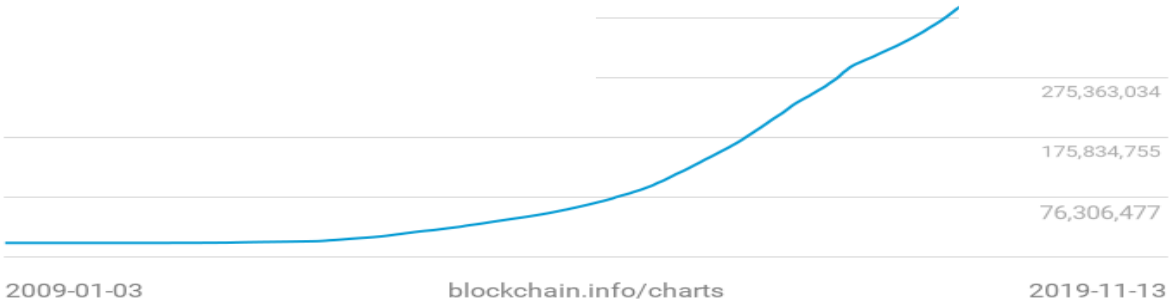
Graphique N°03 : Evolution Du Nombre De Bitcoin En Circulation (2009-2019)



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 21millions.

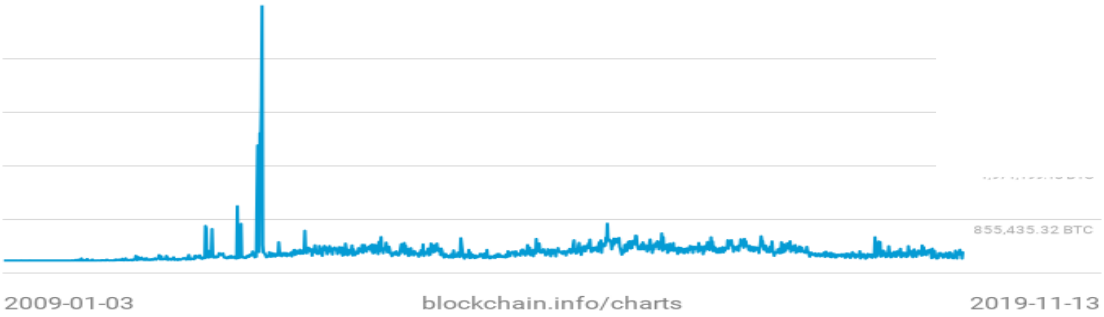
Graphique N°04 : Evolution Du Nombre De Transactions En Bitcoin (2009-2019)



Source : https://www.blockchain.info

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

Graphique N°05 : La Valeur Des Transactions En Bitcoin (2009-2019)



Source : https://www.blockchain.info

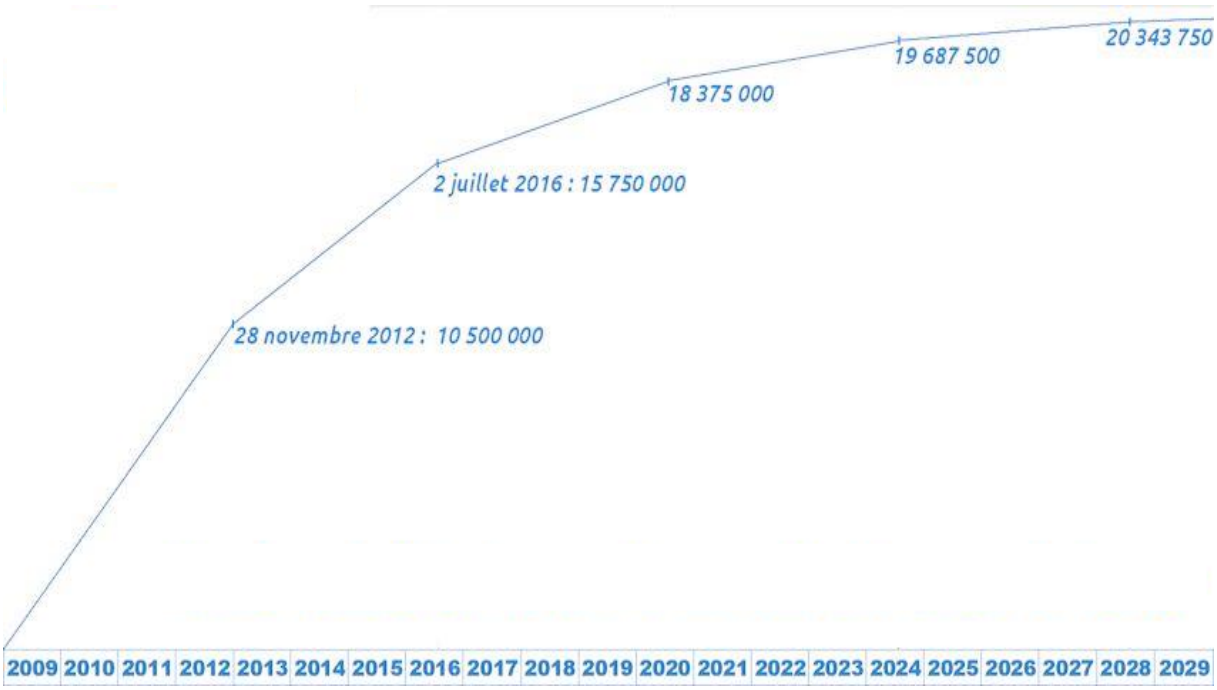
Graphique N°06: Evolution De la capitalisation boursière du Bitcoin (2009-2019)

Source : https://www.blockchain.info

Quant à la capitalisation boursière de Bitcoin, elle estéstimée 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.

Graphique N°07: Evolution Du Nombre De Bitcoins Crées 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 2019[189], 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 (voir figure N°07)

[189] Block Blog, distribution des nœuds bitcoins dans le monde, consulté en ligne sur (blockblog.fr) consulté le 16/11/2019.

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 significative.

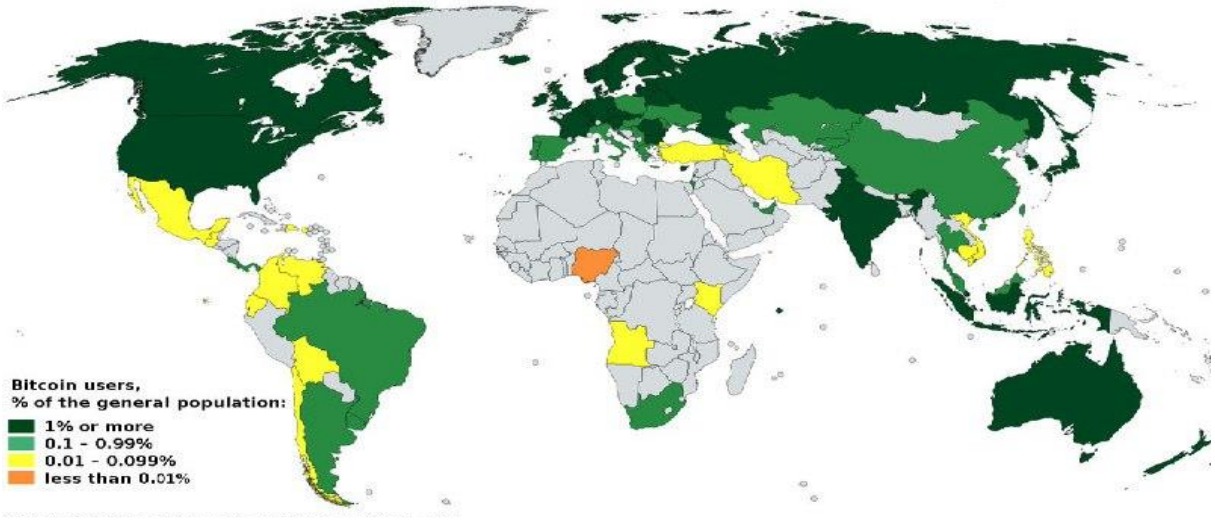
Afrique

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**[190], 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)[191].

Figure N° 07 : La Carte Géographique De La Concentration De Nœuds Bitcoin Accessibles Dans Des Pays Du Monde Entier

Les données de la carte géographique sont basées sur la distribution des nœuds jusqu'au 27/01/2019



Source: Block Blog (www.blockblog.fr)

La distribution globale de nœuds bitcoin joignables à compter du samedi 16 novembre 2019 à 08h18:01 GMT + 0100 (heure normale de l'Europe centrale) est 9 448 nœuds.

Tableau N°6 : Les 10 principaux pays par rapport au nombre de nœuds accessibles (arrêté au 16/11/2019)[192].

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

[190] Site internet pour les estimations de la distribution des nœuds de Bitcoin dans le monde
[191] Actuellement l'Afrique de sud est au 35e rang à l'échelle mondiale au 16/11/2019.
[192] Bitnodes (bitnodes.fr) consulté le 16/11/2019.

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.

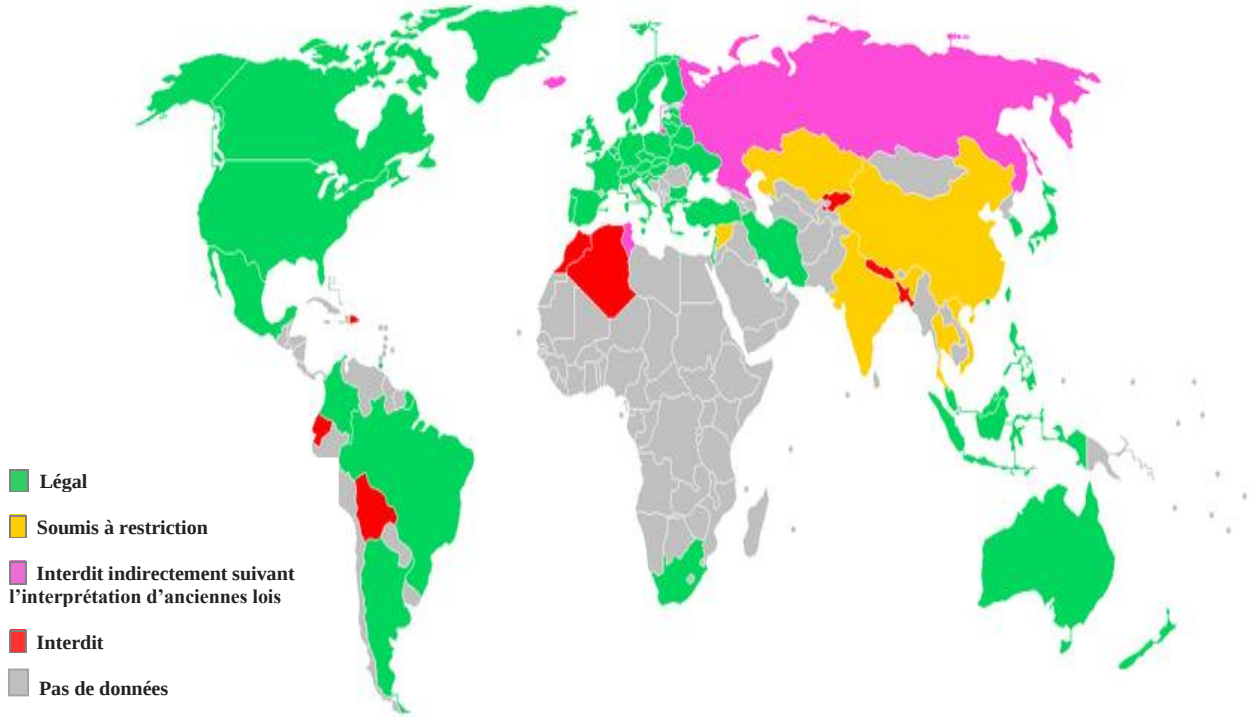
2- Cadre juridique du Bitcoin

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 du droit.

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.

Figure N° 08 : Statut juridique du Bitcoin (la crypto-monnaie) dans le monde



Source : www.marketcap.org

2-1-Union européenne

L'autorité bancaire européenne a mis en garde les consommateurs contre les risques liés au bitcoin (13 décembre 2013)[193], considérant les crypto-monnaies comme des "représentations virtuelles" de monnaie**.** Elle a également recommandé le 04 juillet 2014 aux institutions bancaires et financières de ne pas utiliser le bitcoin ni de proposer des services autour de ce dernier.

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.

2-2-Etats-Unis

Le rapport parlementaire du sénateur Tom Carper (03 février 2014) dresse un premier panorama des enjeux juridiques du bitcoin.

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 compagne et des finances politiques, il s'agit d'une "monnaie sans statut légal défini". Pour la direction générale des finances publiques, le

[193] WIKIPEDIA, Op.cit.

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[194], le ministre de l'économie, Bruno le Mair, 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.

[194] WIKIPEDIA, Op.cit.

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 est 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[195].

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.

[195] WIKIPEDIA, Op.cit.

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 vigueur[196].

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 constant 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*»[197].

Un bitcoin égale à 970 928,23 DA[198].

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.

[196] El watan "*Les crypto-monnaies indésirables en Algérie* " publié en ligne le 12/02/2018 consulté sur (https://www.elwatan.com) le 18/11/2019.
[197] 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.
[198] Données fournies par Morningstar pour la devise et Coinbase pour la crypto-monnaie la journée du 19/11/2019.

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 parait 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.

SECTION 3 : DÉBAT AU TOUR DU 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 vu 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[199]

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);

[199] WIKIPEDIA, Op.cit.

- 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 bouses d'échange), 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

- **Faible sensibilisation et compréhension du protocole,** la compréhension du fonctionnement du protocole Bitcoin est nécessaire pour bien l'utiliser.
- **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[200]. 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 tulipomanie[201].
- 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.

[200] WIKIPEDIA, Op.cit.

[201] Tulipomanie, (tulipe mania en anglais) est le nom donné au soudain engouement pour les tulipes dans le nord des Provinces-Unies au milieu du XVII[e] 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).

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-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*"[202] : 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 seigneuriage 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'expliciter.

2-1-1-Moyen d'échange

Pour l'instant, l'utilisation du bitcoin dans le commerce quotidien est plutôt restreinte[203]. 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. Etant donnée sa faible utilité en tant que moyen de paiement dans les transactions commerciales, le bitcoin n'a pas de valeur intrinsèque significative.

[202].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.

[203] 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.

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 jour avoisine 304 671 au 18/11/2019[204]. 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[205]. 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

[204] Source Blockchain.com, Op.cit.
[205] Bulletin de l'Observatoire des Politiques économiques en Europe, Op.cit, P9.

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.

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 sites web 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[206]. 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'or[207]. 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 seigneuriage

Le droit de seigneuriage 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

[206] De nombreux incidents ont été signalés tel que l'effondrement de MtGox dû au détournement de 744 408 bitcoins en 2014 suite à un piratage informatique, ou encore celui de James Howells, un Gallois qui a déclaré avoir jeté un disque dur contenant 7 500 bitcoins en 2013.

[207] Bulletin de l'Observatoire des Politiques économiques en Europe, Op.cit, P10.

des Etats-Unis. En Europe, les profits nets de la BCE varient entre 10 et 30 milliards d'euros sur la période 2002-2015[208].

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

Dans le système financier actuel, les banques commerciales privées réalisent aussi des revenus de seigneuriage 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[209]. Toutefois, il y a un certain équilibre dans le partage des revenus de seigneuriage 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 seigneuriage 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 seigneuriage.

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

[208] Bulletin de l'Observatoire des Politiques économiques en Europe, Op.cit.
[209] Ibid.

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[210].

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 Reserve Fédérale des Etats-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.

[210] Bulletin de l'Observatoire des Politiques économiques en Europe, Op.cit.P11.

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[211].

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 contient 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'usager 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.

[211] Crypto-France publié le 11/02/2018 sur (cryptofrance.com) consulté le 17/11/2019.

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 coté 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,…)[212] 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.

[212] Crypto-France. Op.cit.

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 vu 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 nécessaire 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 crées 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 donnée 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 considérer 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"[213]. 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".

[213] Charlotte de Montpellier," *Le Bitcoin est-il vraiment une monnaie ?"*, publié le 28/05/2019 consulté en ligne sur (www.ing.be) le 25/11/2019.

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*"[214]. 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.

Malgré 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

[214] En ligne sur (www.usbeketrica.com) oublié le 07/01/2019 consulté le 25/11/2019.

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 certains 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 connaitre au mieux la crypto-monnaie.

Références Bibliographiques

RÉFÉRENCES BIBLIOGRAPHIQUES

1 - Ouvrages

- 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, anticiper et investir."*, Dunod.
- CHAUM D. (1983): ″Blind signatures for Untraceable payements″.
- 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.
- OTTAVJ C. (2014) :"*Monnaie et financement de l'économie*", Edition Hachette, Paris Cedex.
- 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.

2 - 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.
- DELAHAY.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) 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 (ww.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 de blanchiment", Juin 2014, consulté sur (www.economie.gouv.fr) le 05/11/2019.

3 - 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, Maitrise en droit des technologies de l'information, 2015

4 - Sites internet

- http://nassimbelouar.com. Blog de BELOUAR Nassim (Entrepreneur, formateur et consultant Blockchain). Consulté le 15/09/2019.
- http://www.ses-nouilles.fr. Blog De Cours En Economie consulté le 06/10/2019.
- http://www.triste.over-blog.com. Blog De Cours En Economie consulté le 06/10/2019.
- http://www.alainbeitone.blogspot.com. Blog d'Alain Beitone consulté le 17/11/2019.
- http://www.wikipedia.org. Consulté le 30/07/2019.
- http://www.cryptoactu.com. Consulté le 15/09/2019.

- http://www.Yaka Saider.fr. Consulté le 09/10/2019.
- http : //www.fr.m.wikipedia.org. Consulté le 11/10/2019.
- http://www.e-gold.com. Consulté le 20/10/2019.
- http://www.bitcoin.org. Consulté le 22/09/2019.
- http://www.cryptoencyclopedie.com. Consulté le 23/10/2019.
- http://www.coinmarketcap.com. Consulté le 31/10/2019.
- https://www.fr.slideshare.net. Consulté le 28/10/2019.
- http://www.lesechos.fr. Blog les Echos consulté le 28/10/2019.
- http://www.journaldunet.com. Consulté le 23/10/2019
- http://www.latribune.fr. Consulté le 03/11/2019.
- http://www.economie.gouv.fr. Consulté le 05/11/2019.
- http://www.alti-trading.fr. Consulté le 10/11/2019.
- http://www.bitcoin.fr. Consulté le 13/11/2019.
- http://www.conseilcrypto.com. Consulté le 16/11/2019.
- http://www.crypto-France.com. Consulté le 13/11/2019.
- http://www.fr.statista.com. Consulté le 16/11/2019.
- http://www.blockchain.fr. Consulté le 12/11/2019.
- http://www.coinlist.me/fr/altcoins/bitcoin. Consulté le 15/11/2019.
- http://www.crypto-monnaie.pro. Consulté le 15/11/2019.
- http://www.lockchain-expert.com. Consulté le 14/11/2019.
- http://www.blockchain.com. Consulté le 13/11/2019.
- http://www.blockchain-expert.com. Consulté le 16/11/2019.
- http://www.cryptonaute.fr. Consulté le 16/11/2019.
- http://www.blockblog.fr. Consulté le 16/11/2019.
- http://www.bitnodes.fr. Consulté le 16/11/2019.
- https://www.commons.wikimedia.org. Consulté le 16/11/2019.
- http://www.bloomerg.com. Consulté le 17/11/2019.
- http://www.cryptofrance.com. Consulté le 17/11/2019.
- http://www.cryptoast.fr. Consulté le 19/11/2019.
- http://www.usbeketrica.com. Consulté le 25/11/2019.
- http://www.coin.org. Consulté le 22/11/2019.
- http://www.coicoin.com. Consulté le 10/11/2019.
- http://www.diskcoin.org. Consulté le 11/11/2019.

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 personne 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.

Hashage: (dans les crypto-monnaies) Le hashage 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 compagne 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.

Par exemple, la fonction SHA-256 appliquée au mot CHAT renverrait le hash suivant :

d8f65e96e482a37e047634e3a087f6fd6 a88a636587d7d3b622bb2e123b546fb

Rappelons que les lettres A à F et les chiffres 0 à 9 sont une représentation alpha-numérique d'une suite de 0 et 1.

En fait, la séquence ci-dessus correspond à cette suite de 0 et 1 :

01100100 00111000 01100110 00110110 00110101 01100101 00111001

00110110 01100101 00110100 00111000 00110010 01100001 00110011

00110111 01100101 00110000 00110100 00110111 00110110 00110011

00110100 01100101 00110011 01100001 00110000 00111000 00110111

01100110 00110110 01100110 01100100 00110110 01100001 00111000

00111000 01100001 00110110 00110011 00110110 00110101 00111000

00110111 01100100 00110111 01100100 00110011 01100010 00110110

00110010 00110010 01100010 01100010 00110010 01100101 00110001

00110010 00110011 01100010 00110101 00110100 00110110 01100110

01100010

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 futur 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.

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

Annexes

LES ANNEXES

Liste des annexes

Annexe N°01 : Les Principaux Acteurs De La Communauté "***Cypherpunk".***

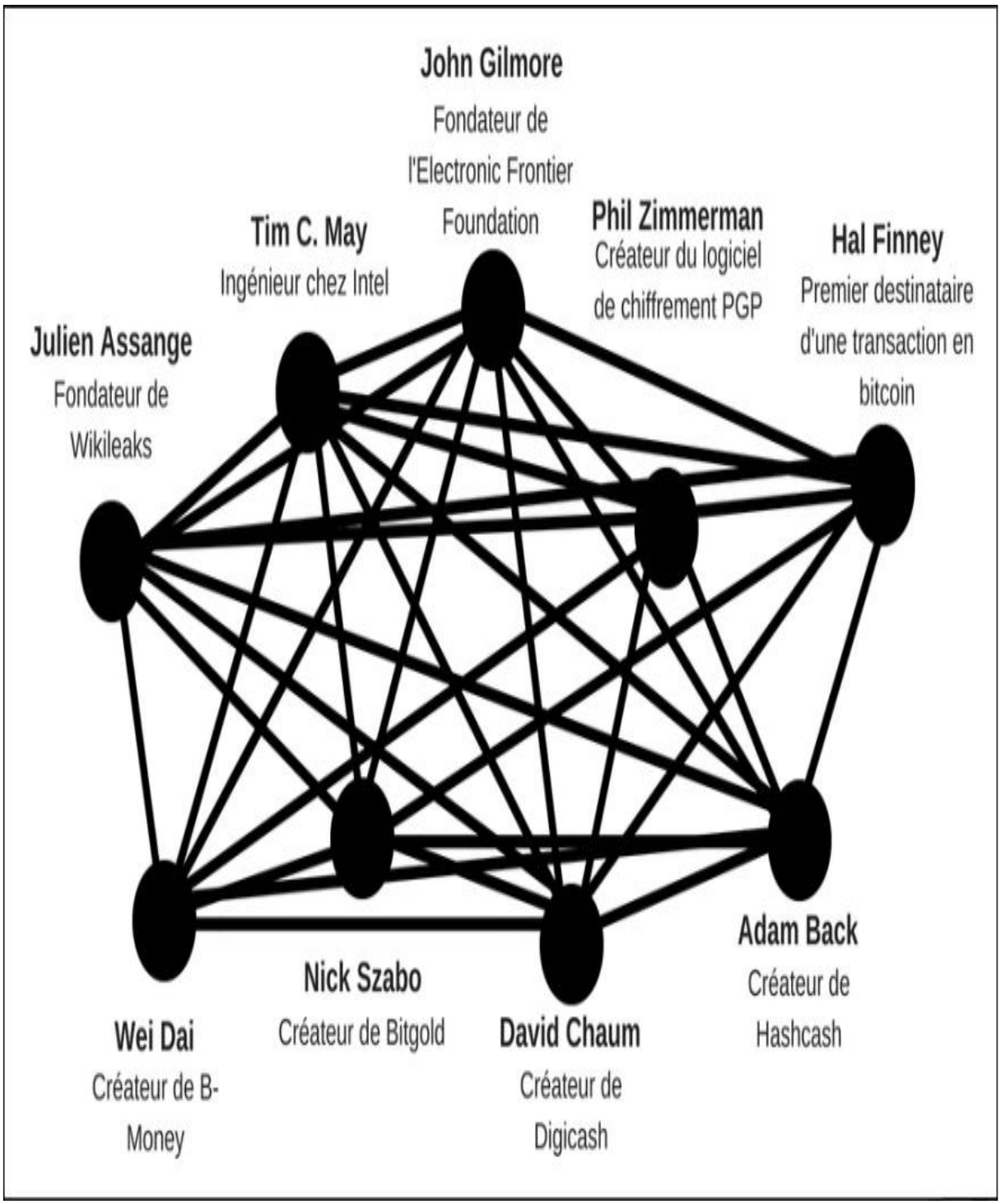
Annexe N°02 : La Distribution Globale De Nœuds dans le Monde entier.

Annexe N°03 : Le Classement Des Principaux Pays En Fonction Des Montants Levés Par ICO.

Annexe N°04 : La Liste Des Incidents Intervenus Sur Les Plateformes D'échange Au 13/06/2018

Annexe N°05 : Présentation Des Incidents Intervenus Sur Les Plateformes D'échange Au 13/06/2018

Annexe N°01 : Les Principaux Acteurs De La Communauté "*Cypherpunk*"



Source : https://www.bitcoin.org

Annexe N° 02 : La Distribution Globale De Nœuds dans le Monde entier

9 448 nœuds à compter du samedi 16 novembre 2019 à 08:18:01 GMT + 0100 (heure normale d'Europe centrale)

1. Etats-Unis (2465)
2. Allemagne (1896)
3. France (605)
4. Pays-Bas (502)
5. Singapour (365)
6. Canada (334)
7. Royaume-Uni (328)
8. Chine (306)
9. Fédération de Russie (240)
10. Japon (196)
11. Hong Kong (158)
12. n / a (152)
13. Finlande (151)
14. Australie (146)
15. Suisse (136)
16. République de Corée (120)
17. Ukraine (96)
18. Suède (88)
19. Irlande (82)
20. République tchèque (75)
21. Lituanie (67)
22. Italie (67)
23. Espagne (60)
24. Bulgarie (59)
25. Inde (55)
26. Pologne (54)
27. Autriche (50)
28. Roumanie (43)
29. Norvège (42)
30. Belgique (40)
31. Malaisie (35)
32. Hongrie (32)
33. Brésil (31)
34. Slovénie (23)
35. Afrique du Sud (22)
36. Danemark (22)
37. Grèce (20)
38. Slovaquie (19)
39. Argentine (19)
40. Biélorussie (17)
41. Portugal (17)
42. Taïwan (17)
43. Nouvelle Zélande (13)
44. Thaïlande (13)
45. République de Moldova (12)
46. Mexique (11)
47. Turquie (10)
48. Israël (10)
49. Estonie (9)
50. Lettonie (9)
51. Luxembourg (9)
52. Kazakhstan (7)
53. Islande (6)
54. Colombie (5)
55. Emirats Arabes Unis (5)
56. Bosnie-Herzégovine (4)
57. Serbie (4)
58. Croatie (4)
59. Chili (4)
60. Chypre (4)
61. Seychelles (4)
62. Iran (4)
63. Philippines (3)
64. Cambodge (3)
65. Venezuela (3)
66. Îles Vierges américaines (3)
67. Bahreïn (2)
68. Géorgie (2)
69. Costa Rica (2)
70. Kirghizistan (2)
71. Kenya (2)
72. Arabie saoudite (2)
73. Vietnam (2)
74. Qatar (2)
75. Bangladesh (1)
76. Bermudes (1)
77. Bolivie (1)
78. Jersey (1)
79. Belize (1)
80. Réunion (1)
81. Guatemala (1)
82. Gibraltar (1)
83. Andorre (1)
84. Panama (1)
85. Îles Caïmans (1)
86. Monténégro (1)
87. Monaco (1)
88. Îles Féroé (1)
89. Curaçao (1)
90. Suriname (1)
91. Koweït (1)
92. République dominicaine (1)
93. Trinité-et-Tobago (1)
94. Arménie (1)
95. île de Man (1)

Annexe N° 03 : Le Classement Des Principaux Pays En Fonction Des Montants Levés Par ICO

Pays	Montants levés (en M USD)	Part des montants totaux levés
Etats-Unis	1 031	31.1 %
Russie	310	9.3 %
Singapour	260	7.8 %
RPC	256	7.7 %
Hong Kong	196	5.9 %
Allemagne	187	5.6 %
Canada	175	5.3 %
Royaume-Uni	145	4.4 %
Suisse	79	2.4 %
Estonie	63	1.9 %
Argentine	62	1.9 %
Lituanie	51	1.5 %
Thaïlande	47	1.4 %
Australie	34	1.0 %
Ukraine	32	1.0 %
Espagne	25	0.8 %
Costa Rica	23	0.7 %
Liechtenstein	23	0.7 %
Slovénie	20	0.6 %
Corée du sud	18	0.5 %
Bulgarie	12	0.4 %
France	12	0.4 %
Autres	65	2.0 %
Total	3126	100 %

Source : Rapport de Jean-Pierre Landau, Alban Genais,"*Les crypto-monnaies*", ministère de l'Economie et des Finances, du 04/07/2018

Annexe N°04 : La Liste Des Incidents Intervenus Sur Les Plateformes D'échange Au 13/06/2018

Nom de la plateforme	Date	Montants perdus (en million de $)
Mt Gox	2011 puis 2014	487
Bitcoinica	Mars 2012 Mai 2012	6 2.4
Bitfloor	Septembre 2012	0.25
Poloniex	4 Mars 2014	12.3% des réserves en bitcoin de la plateforme
Bitstamp	4 Janvier 2015	4.3
Bitfinex	Août 2016	72
The DAO	Juin 2016	53
Steemit.com	Juillet 2016	0.085
Parity	Juillet 2017	32
Bithumb	Juillet 2017	1
Veritaseum	Juillet 2017	8.5
Tether	Novembre 2017	30.9
Youbit	Décembre 2017	2.125
Coinchek	Janvier 2018	530
Bitgrail	Février 2018	170
Coinrail	Juin 2018	Entre 0.530 et 0.795
Bithumb	Juin 2018	30

Source : Rapport de Jean-Pierre Landau, Alban Genais,"*Les crypto-monnaies*", ministère de L'Economie et des Finances, du 04/07/2018

Annexe N°05 : Présentation Des Incidents Intervenus Sur Les Plateformes D'échange Au 13/06/2018

Plateforme concernée	Nature de l'incident
Mt Gox	**Montant perdu :** 750 000 BTC. **Cause du piratage :** faille de sécurité des *hots wallets*.
Bitcoinica	**Montant perdu :** 46 703 BTC lors du 1er piratage ; 18 000 BTC lors du 2em piratage. **Cause du piratage :** faille de sécurité du serveur Linode et du serveur Rackspace permettant le vol des clés privées des utilisateurs.
Bitfloor	**Montant perdu en bitcoin :** 24 000 BTC. **Cause du piratage :** faille de sécurité de l'encryptage des données et des *hots wallets*
Poloniex	**Montant perdu en bitcoin :** 12.3 % de ses réserves en bitcoins. **Cause du piratage :** mutabilité des signatures ou malléabilité des transactions.
Bitstamp	**Montant perdu en bitcoin :** 18 866 BTC. **Cause du piratage :** hameçonnage de six salariés de la plateforme.
Bitfinex	**Montant perdu en bitcoin :** 119 756 BTC. **Cause du piratage :** faille de sécurité dans le portefeuille multi-signatures de Bitfinex et de Bitgo.
The DAO	**Montant perdu en bitcoin :** 3.5 millions d'Ethers. **Cause du piratage :** faille de sécurité dans la programmation des *smart contracts.*
Steemit.com	**Montant perdu en bitcoin :** 85 000 $. **Cause du piratage :** indéterminé, mais plaintes des utilisateurs relatives à la fiabilité des systèmes d'authentification.
Parity	**Montant perdu en bitcoin :** 150 000 Ethers. **Cause du piratage :** faille de sécurité dans les portefeuilles numériques ; faille de sécurité des *hots wallets*.
Bithumb	**Montant perdu en bitcoin :** 1 million de dollars. **Cause du piratage :** hameçonnage d'un employé de la plateforme
Veritaseum	**Montant perdu en bitcoin :** 153 037 Ethers.

	Cause du piratage : indéterminé.
Tether	**Montant perdu en bitcoin :** 30.9 millions de dollars. **Cause du piratage :** faille de sécurité du logiciel Omni Core, utilisé par Tether pour prendre en charge les transactions.
Youbit	**Montant perdu en bitcoin :** 2.125 millions de dollars. **Cause du piratage :** faille de sécurité permettant aux pirates d'infiltrer le système de retrait de la plateforme ; Hameçonnage donnant accès aux clés privées.
Coinchek	**Montant perdu en bitcoin :** 530 millions de dollars. **Cause du piratage :** faille de sécurité des *hots wallets***.** Dispositif de sécurité multi-signatures insuffisamment robuste**.**
Bitgrail	**Montant perdu en bitcoin :** 17 millions de Nano-XRB. **Cause du piratage :** indéterminé
Coinrail	**Montant perdu en bitcoin :** entre 530 000 et 795 000 $ **Cause du piratage :** faille de sécurité des *hots wallets***.**
Bithumb	**Montant perdu en bitcoin :** équivalent de 30 millions de dollars. **Cause du piratage :** faille de sécurité des *hots wallets***.**

Source : Rapport de Jean-Pierre Landau, Alban Genais,"*Les crypto-monnaies*", ministère de L'Economie et des Finances, du 04/07/2018

LISTE DES FIGURES

LISTE DES GRAPHIQUES

LISTE DES TABLEAUX

TABLE DES MATIERES

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.

Mots clés

Monnaie, Bitcoin, crypto-monnaie, Cryptographique, Monnaie numérique, Monnaie virtuelle, Monnaie digitale, système de paiement, Banque, Confiance, unité de compte, réserve de valeur, moyen de paiement, système décentralisé, anonymat, pair à pair.

ABSTRACT

In last recent years, we have been witnessing the emergence of new types of currencies, based on cryptographic processes, managed in pairs according to a distributed consensus: these are crypto currencies, the most representative of which would be the one launched after the 2008 financial crisis; "the bitcoin". The crypto currency system appears as an alternative to contemporary capitalism, whose dynamics are driven by a cooperation between banks and governments. It makes also a part of a protest movement against the political and banking powers, judged incapable of offering a "quality currency". Crypto-currencies then come into conflict with the traditional conception of the unitary, sovereign, territorial and centralized currency, but also constitute a means of "democratizing finance" within alternative (transnational) spaces and restoring to individuals that common good that is the currency. Therefore, we propose in this memoir to analyze the nature of crypto currency. Once having explained the various definitions related to this currency and the way it works, we are going to examine and study the nature of this newborn (digital currency) while presenting its advantages, the risks to which it exposes its users, as well as the legal scope of it. However, we are going to see how its technology's disruptive nature, as well as its innovation potential, make crypto currency a stimulating object for fundamentally new studies and debates in the history of monetary ideas. Crypto currencies, if we admit that it is a phenomenon, is far from having reached maturity in all its aspects; the vast majority of people being still in a phase of ignorance, learning and discovery.

Keywords

Currency, Bitcoin, crypto-currency, cryptographic, digital currency, virtual currency, digital currency, payment system, bank, trust, unit of account, store of value, means of payment, decentralized system, anonymity, peer-to-peer.