LA CRYPTOMONNAIE.

Tablesdes matières

[Introduction : 3](#_Toc9484804)

[Chapitre 1 : D’où vient le Bitcoin ? 8](#_Toc9484805)

[1.1 L’origine de bitcoin. 8](#_Toc9484806)

[1.2 La chaine des blocs ou « Blockchain » 9](#_Toc9484807)

[1.3 Le potentiel de la Blockchain 12](#_Toc9484808)

[1.4 Le minage et la preuve de travail "Proof of Work". 12](#_Toc9484809)

[1.5 Choisir le « mineur » 13](#_Toc9484810)

[Chapitre 2 : comparaison entre le système classique et le bitcoin. 15](#_Toc9484811)

[2.1La viabilité du bitcoin. 15](#_Toc9484812)

[2.1.1 Or & bitcoin. 15](#_Toc9484813)

[2.1.2 Dollar & Bitcoin. 16](#_Toc9484814)

[2.2. Avantages du bitcoin: 17](#_Toc9484815)

[2.2.1 Le cout de transaction très faible. 17](#_Toc9484816)

[2.2.2 Le bitcoin une alternative pour les populations ne pouvant pas accéder au servies bancaire. 19](#_Toc9484817)

[2.2.3 Problèmes du " Double Spending" et les problèmes des généraux byzantins. 20](#_Toc9484818)

[2.2.4le complet anonymat: une épée à double tranchant. 21](#_Toc9484819)

[2.3. Les inconvenants du bitcoin. 22](#_Toc9484820)

[2.3.1 Retour sur l'anonymat ("la face cachée de la lune"). 22](#_Toc9484821)

[2.3.2 Soucis de sécurité : La fragilité du réseau bitcoin: 22](#_Toc9484822)

[2.3.3 Volatilité du bitcoin. 24](#_Toc9484823)

[2.3.4 Minage trop coutant. 25](#_Toc9484824)

[Chapitre 3: Bitcoin autant qu’un actif financier. 27](#_Toc9484825)

[3.1 Pourquoi Bitcoin est considéré comme un actif financier. 27](#_Toc9484826)

[3.2 Le couple rendements risque de bitcoin. 27](#_Toc9484827)

[3.3 mesure de performance de bitcoin. 30](#_Toc9484828)

[3.3.1 La moyenne. 32](#_Toc9484829)

[3.3.2 La variance. 33](#_Toc9484830)

[3.3.3 L’écart-type. 35](#_Toc9484831)

[3.3.4 Le coefficient de variation. 35](#_Toc9484832)

[3.3.5 La covariance. 36](#_Toc9484833)

[3.3.6 Coefficient de corrélation. 36](#_Toc9484834)

[Chapitre 4: Bitcoin et réglementation. 38](#_Toc9484835)

[4.1- Exemple contemporain de faillite du système monétaire. 38](#_Toc9484836)

[4.1.1 La crise de l'argentine. 38](#_Toc9484837)

[4.1.2 La crise du Zimbabwe. 40](#_Toc9484838)

[4.1.3 Kenya et le Bitcoin. 40](#_Toc9484839)

[4.2 Bitcoin une solution à la crise mondiale économique ? 42](#_Toc9484840)

[4.3 La crise inflationniste et le bitcoin. 44](#_Toc9484841)

[4.3 Réglementation des pays envers le bitcoin. 45](#_Toc9484842)

[4.3.1 Droit de seigneuriage. 46](#_Toc9484843)

[4.3.2 Stabilisation macroéconomique et financière. 46](#_Toc9484844)

[4.4 Tentative de règlementation. 47](#_Toc9484845)

[4.4.1 La Chine interdit. 47](#_Toc9484846)

[4.4.2 La banque centrale allemande demande une réglementation mondiale. 48](#_Toc9484847)

[CONCLUSION. 49](#_Toc9484848)

[Épilogue. 50](#_Toc9484849)

# Introduction :

Pour qu'une monnaie soit viable; soit telle une crypto monnaie ou une monnaie traditionnelle (fiat) émise par les gouvernements ou les banques centrales, elle doit d'abord gagner la confiance de la communauté qui l'utilise. La confiance réside au centre de n'importe quel système monétaire.

* la monnaie "est" la confiance.

Dans son récent et provocateur livre " *La biographie non autorisée ",* Félix MARTIN stipule que: Si on se focalise uniquement sur l'approche matérielle de la monnaie, on oublie la force et le moteur essentiel du développement des civilisations. On traitant la monnaie comme une, ce qu'il appelle la" *Technologie sociale "* il déclare que la pièce métallique qui fait office de monnaie n'est pas en réalité LA monnaie.

Il explique que la monnaie est un système de compte à crédit qui représente la monnaie comme une nouvelle forme d'organisation sociale développé. elle a créé un système de valeur universelle, ce qui a permis un changement de forces dans les structures sociales des tribus qui était maintenus à l'ordre par la force physique, et qui maintenant grâce à cet nouvelle technologie sociale (la monnaie) a permis à tous les membres de la société non seulement les forts ou les dirigeants d'une telle tribus, de devenir puissants, ce qui a engendré une nouvelle notion qui est " *la richesse"* défini par l'accumulation de la monnaie, cette nouvelle notion abstraite deviendra par la suite de l'évolution historique une grande mesure du pouvoir. Cette nouvelle notion révolutionnera l'humanité.

Malgré le fait que ce changement qui est l'apparition de la monnaie est considéré comme une révolution, au pair avec l'invention de la roue ou la découverte du feu, il est difficile de concevoir la monnaie sur le plan individuel, car l’individu préfère les explications matérielles sur le comment de la monnaie. On peut remarquer facilement ce phénomène, sur les gens appartenant à l'ancienne génération, qui ont grandis avec les choses matérielles. Que peut signifier pour eux le mot " achat virtuel " ? Encore moins si il devrait payer ses même achats avec une "monnaie virtuelle" ! Ces gens ainsi que la plupart des gens d'ailleurs ne jure que par le Dollar et l'Euro ou encore le Dirham, ainsi une explication s'impose "Quesque c'est que la monnaie " ?

* la valeur de la monnaie.

Une pièce de monnaie constitue un prêt pour le système bancaire, qui établis les droits au futures porteurs de cette pièce de monnaie, la banque centrale ainsi que tout le circuit monétaire est obligé de reconnaitre la valeur de cette pièce, on peut facilement remarquer que pour que ce système marche il faut avoir des base de confiance dans le statut de la banque centrale, car si tous les citoyens décident du jour au lendemain et en commun accord que cette monnaie ne vaut plus rien, que peut la banque centrale faire? Hormis mettre en place des garanties pour retrouver la confiance de la société; cette approche qui stipule que la monnaie sans la confiance n'est **rien** est fondamentale.

On peut dire, "d'accord certes la monnaie ne vaut rien intrinsèquement mais l'or vaut forcement quelque chose non?"; bien que l'or est rare, très dur à détruire, facilement vérifiable, et modérément divisible, il ne reste en fin de compte qu'un simple métal, c'est l'humanité qui a choisi ce moyen comme symbole de richesse et de prestige, et sans confiance l'or ou d'ailleurs n'importe quel matériel physique soit il ou virtuel, ne vaut rien.

* les chartistes et les matérialistes.

Cette approche basée sur la confiance est le slogan de ce qu'on nomme les "*Chartiste"* du mot latin *charta*qui signifie tout simplement pièce. Contrairement au "*matérialiste "* qui stipulent que la monnaie est une simple commodité, une unité universellement reconnue pour éviter tout simplement les problèmes liés au "troc", cette philosophie dont le pionnier était Aristote, qui par la suite sera adopter par Adam Smith ce base sur le troc et les problèmes liés au troc, qui se résument sur ce qu'il appelle le *"la coïncidence des besoins "* qui veut dire en d'autre terme, qu'il n'existe aucune garantie que le berger en excès de chèvres cherche a échangé ses moutons contre le blés produits par un paysan; d'où la nécessité de créer un système de monnaie ou, la monnaie joue un simple rôle d'intermédiaire pour pallier à cette difficulté.

Pour les chartistes l'histoire est différente, premièrement ils ignorent l'histoire du troc et la traitent comme étant un simple mythe, ils se basent sur plusieurs anthropologistes du 20eme siècle, qui affirment qu'il n'existe aucune preuve que les gens du passé utilisait le troc, mais qu'il utilisait des codes et techniques pour traiter diverses obligations et créances.

En d’autres mots les créancessontapparues en premier lieu. L'anthropologiste David Graeber stipule que les premiers types de créance sont apparus sous la forme d'échange de cadeau qui agénéré un sens de "*créance morale*" (je vous dois moi et toute ma famille, une faveur). Ensuite les créances sont apparues sous la forme de pénalités (20 chèvres pour avoir tué le frère de quelqu'un ...). À partir de ce point les sociétés ont commencés à comprendre l'utilité de la monnaie pour le règlement des créances ....

* les rôles des banques centrales dans la monnaie.

Le système qu'on utilise maintenant, pour gérer les échanges de monnaie et les biens prend ses racines dans la famille de *Medici*, de la renaissance européenne, plus exactement la ville de **florentine**.

Ces gens était des penseurs révolutionnaires, qui ont découvert les besoins de la société et l'on remplit, ils ont réussi à trouver une façon de lier les préteurs de monnaie et les demandeurs, grâce à une relation d'intermédiation, en permettant d'accumuler l'excès de l'épargne et le rendre à disposions des entités en manque de liquidité, tout ça bien entendu en contrepartie d'une commission pour la banque.

Ce nouveau système **centralisé** basé sur les banques, était d'une efficacité fulgurante, il a réussi à propulser les économies des pays à des hauteurs extraordinaires.

Les banques ont en effet réussi à créer un système central basé sur la confiance ou les gens sans forcément ce connaitre peuvent effectuer des opérations financières.

La famille de *Medici* à créer en fin de compte à un système de création monétaire, l'argent n'étant pas une monnaie physique, mais néanmoins un système pour organiser, partager les créances et les paiements de la société. Cesystème est encore utiliséjusqu'àprésent.

* Le problème du système central.

Avec la création d'un système central, basé sur la confiance et en mettant les banques au centre de toutes les opérations financières.Les banques sont devenus trop puissantes, tellement puissantes en effet que *le monde*aussi complexe et interconnecté soit-il, est devenu à la merci de l'intermédiation des banques.

Cette dépendance a bel est bien des avantages, certain experts d'ailleurs considéraient cette dernière comme étant le prix à payer en contrepartie du progrès de la civilisation, certes cette dépendance commence à devenir de plus en plus gênante etpose pas mal de problèmes et de limitations dans le monde moderne, citons par exemple:

-La centralisation de l'information; c'est à dire que chaque personne désirant passer par l'intermédiaire d'une banque doit révéler toutes ses information personnelle, parfois beaucoup plus que nécessaire, ainsi les banques centrales qui sont généralement Contrôléespar les gouvernements peuvent utiliser les informations de la population à leur propres fins.

-2.5 milliard des gens sont isolés du marché financier (50% de la population mondiale active), ne possèdent tout simplement pas de compte bancaire, ils ne peuvent pas faire part au monde financier.

-Les taux des commissions exorbitantes, les commissions peuvent atteindre jusqu'à 10% de la valeur de la transaction, ainsi ce système bancaire n'est pas du tout optimisé pour les petites transactions, car des fois, ça ne vaut pas vraiment le cout de faire une transaction qui sera "taxé" par la banque à 50%.

-Le risque potentiel de vol, de fraude ou de perte d'information entrainant les pertes de fonds, ce risque est généralement accepté par les banques, malgré les techniques avancées en matière de cryptage et de sécurité dont font preuve ces dernières, elles ne sont et ne seront jamais immunisées contre ces risques.

On remarque que ce système présente plusieurs failles et limites auquel les économistes en longtemps critiqué, ainsi plusieurs méthodes alternative ont commencés à voir le jour, jusqu'à ce qu'un jour un certain *Satoshi NAKAMOTO* (dont on ne connait ni le visage ni l'identité autre que son pseudonyme)publie en 2009 une recherche sur un système qui marrie les procédés de cryptage et la monnaie, de la**crypto-monnaie**; le **Bitcoin**, bien que la crypto-monnaie existait déjà bien avant cette date (elle est apparu aussi tôt que les années 70) *Satoshi* a réussi à familiariser le Bitcoin avec le grand public et son système est devenu maintenant le système standard de référence de la crypto-monnaie, utilisé par des millions d'internaute partout dans le monde.

* L'ère du bitcoin et de la crypto-monnaie.

L’idée fondamentale de la crypto-monnaie est simple, tellement simple en vrai qu'on trouve ces traces tout au long de l'histoire humaine. L'idée ce base sur l’élimination des parties intermédiaires. Comment ?

Par la création d'une infrastructure qui permet aux étrangers de s’engager entre eux sans l’intervention des banques centrales, grâce à un réseau des ordinateurs autonomes, moyennant l'utilisation d'un système décentralisé de confiance qui ne serait Controller par aucune institution.

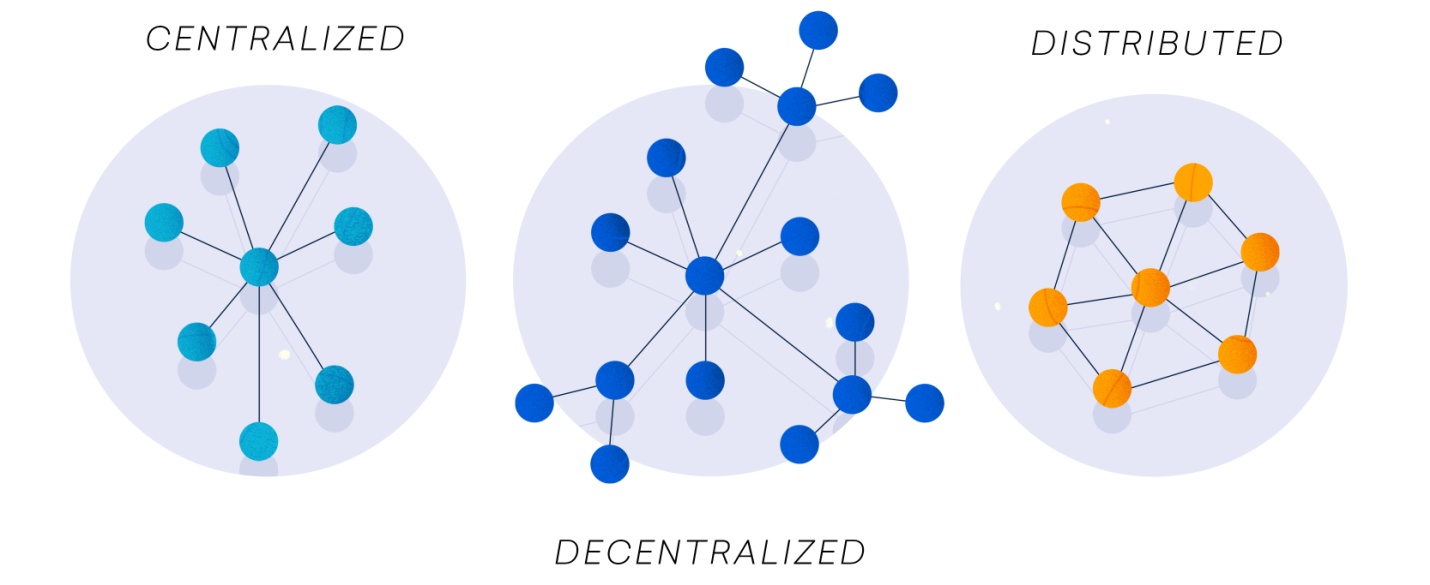


Figure 1: les systèmes centralisés, décentralisés, et distribués.

À son noyau la crypto- monnaie est construit autour d'un système élégant et fort ingénieux :

-le principe d’un grand livre des transactions universel, difficile à frauder , public et constamment vérifié par des ordinateurs puissants, qui opèrent indépendamment les uns des autres, théoriquement ca veut dire qu'on n'a pas besoins des banques ou des systèmes intermédiaires pour leur faire confiance, le réseau des journaux des transactions dans le cas de la crypto-monnaie s'appelle « Blockchain » joue le rôle d'intermédiaire qui assure que les transactions ce passent en toute sécurité.

Ce système lui aussi a était critiqué puisque il venait après une longue série de crypto-monnaiesimilaire, pourquoi le Bitcoin serait-il diffèrent? Mais certain enthousiastes pense réellement que ce moyen pourrais révolutionner l'économie tell que nous le connaissons...

# Chapitre 1 : D’où vient le Bitcoin ?

## 1.1 L’origine de bitcoin.

En 31 Octobre 2008, des centaines des membres d'une liste de mails appartenant à des experts et des enthousiastes en cryptographie, reçoivent un email de quelqu'un qui s’appelle "Satoshi NAKAMOTO", dans l'email il cite "Je suis en train de travailler sur un nouveau système de monnaie, pair à pair, sans tierce personne"

Sans autres commentaires, il leur envoya un article d'une longueur d'environ 9 pages où il explique[[1]](#footnote-2) , avec des illustrations, équations et code le système digital de monnaie.

NAKAMOTO avait déjà acquis un domaine sous 'bitcoin.org', mais il savait que pour propulser son système au niveau supérieur, ce systèmedevraitêtreutilisé par plusieursutilisateurs...

Le premier utilisateur du bitcoin fut Satoshi NAKAMOTO lui-même, ainsi qu'un volontaire qui faisait partie de liste de mail initiale, Hal FINNEY, àl'époque âgé de 53 ans, était un développeur clé dans la Ste PGP, une société crée par Phil ZIMMERMANN...

À partir du 10 janvier 2009, le duo commençaà travailler ensemble sur un projet intensif, d'une durée deux semaines, ils ont collaboré en partageant des notes à travers des emails, ce qui petit à petit a réussià rendre le bitcoin opérationnel.

Contrairement à la monnaie scripturale toute les transactions effectue par le Bitcoin sontenregistrées dans le grand livre que plusieurs, potentiellement tous les utilisateurs du système ont une copie dans leurs ordinateurs, ce grand livre est toujours disponible dans l’internet. Bitcoin est la première grande crypto-monnaie décentralisée. Il y a des centaines autres monnaiesalternatives comme Litecoin et Dogecoin, mais Bitcoin occupe plus de 90% de capitalisation de marché.

Bitcoin repose sur un système qui récompense l’énergieutilisé pour sa création, cette opération est appelé le « Mining », ou les utilisateurs offrent le pouvoir de leurs ordinateurs pour vérifier et enregistrer les transactions dans le grand livre public. Les individus ou les entreprises engagent dans le processus de minage en contre partie des couts de transactions et les Bitcoin secrètement crées, autre que le minage, les Bitcoins peuvent être obtenues en contre partie de la monnaie conventionnelle, biens ou services, les utilisateur peuvent envoyer et recevoir de Bitcoin pour un cout de transaction optionnel en utilisant un programme de portefeuille dans leur ordinateur personnel, Smartphone ou une application web.

Bitcoin est un réseau qui fonctionne sur un protocole appelé Blockchain. Et pendant un temps, Bitcoin et Blockchain étaient quasiment synonymes. La Blockchain a depuis été divorcée conceptuellement de sa première application et des milliers de Blockchain ont été créés à l'aide de techniques cryptographiques similaires. Cette histoire peut rendre la nomenclature déroutante. "Blockchain" fait parfois référence à l'original, bitcoin Blockchain; d'autres fois, il fait référence à la technologie de la Blockchain en général, ou à toute autre Blockchain spécifique, telle que celle qui alimente Ethereum.

## 1.2 La chaine des blocs ou « Blockchain »

La Blockchain est un grand livre comptable partagé et public sur lequel repose le réseau Bitcoin en entier. Toutes les transactions confirmées sont incluses dans la chaine des blocs. De cette façon, les portefeuilles Bitcoin peuvent calculer leurs soldes et il est possible de vérifier que les nouvelles transactions dépensent des Bitcoins appartenant effectivement à l'émetteur du paiement.

Par extension, une Blockchain constitue une base de données qui contient l’historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données étant sécurisée et distribuée: elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

La Blockchain cerésume ainsi:

1-Des blocks stockent l’information relativeaux transactions, par exemple la date, letemps, et le montant dépenser.

2-Les blocks enregistrent aussi les participants aux transactions. Utilisant une signature digitale pour marquer le passage des participants.

3-Les blocks ont des codes pour se distinguer des autres blocks, comme les gens ont des noms pour se distinguer entre eux, chaque block a un code unique appelé "hash" qui lui permet de se distinguer entre les autres blocks. Supposant par exemple un utilisateurvient d'acheter une pairede chaussure à partird'un site internet, supposant que directement aprèsle premier achat il a voulu acheter une autre paire, bien que le block serait similaire mais il aura un "hash" différent qui le rendra unique.[[2]](#footnote-3)

|  |
| --- |
| Le hash.  Le terme **hash** fait référence à un type de fichier utilisé dans le monde de l'informatique et celui de la cryptographie. Il est associé à la fonction de hashage, un algorithme mathématique qui consiste à convertir une chaîne de caractères en une valeur inférieure.  Un fichier **hash** permet de vérifier la taille et le caractère identique d'un fichier envoyé via un réseau informatique. En effet, lorsqu'un fichier transfère via un réseau, il est découpé en plusieurs morceaux, puis recollé une fois arrivé à destination. En définissant un nombre de hash correspondant à la taille des données, on connaît à l'avance la taille du fichier attendu à destination et on peut donc valider ou non le succès du transfert du fichier. Grâce à cette fonction, il devient très facile de comparer deux fichiers numériques très proches en apparence et vérifier que le fichier d'origine (l'entrée) n'ait pas fait l'objet d'une modification malveillante.[[3]](#footnote-4)  La fonction la plus utilisé par les systèmes de sécurité informatique est appelé SHA-256 qui signifie 256 bits, cette est d'une sécurité infaillible (elle n'a jamais réussi àse faire pénétrer depuis son instauration) et elle est utilisée partout dans le monde pour les dispositifs de sécurité. |

Concernant les adresses et les balances du bloc Genisis[[4]](#footnote-5), la chaine des blocs est vue comme étant la principale innovation technologique car elle se base sur un système « sans confiance » Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les nœuds du réseau appelés les “mineurs”, selon des techniques qui dépendent du type de Blockchain. Dans la Blockchain du bitcoin cette technique est appelée le “Proof-of-Work”, preuve de travail, et consiste en la résolution de problèmes algorithmiques.

Une fois le bloc 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.

Ce processus prend un certain temps selon la Blockchain, on parle environ une dizaine de minutes pour bitcoin,le créateur du bitcoin a jugé ce temps d'attente entre chaque block nécessaire pour éviter la surcharge du réseau bitcoin.

La chaine des blocs autant qu’architecture pour un nouveau système décentralisé est une innovation clé, permettant la désintermédiation et la décentralisation des toutes les transactions du system entier.



Figure 2: Le Fonctionnement du Blockchain

|  |
| --- |
| public Key et secret Key (clé publique et clé secrète).  La cryptographie peut généralement être divisé en deux grande catégorie larges, une clé secrète (symétrique) et une clé publique (asymétrique), dans la cryptographie à base de clés secrète, les utilisateurs utilisent la clé secrète pour encrypter et décrypter les messages. La difficulté principale relève de la difficulté de la distribution sécurisée des clés, surtout dans un réseau qui grandit de jour en jour.  Utilisant l'exemple suivant pour simplifier le concept: On peut dire que la clé publique est par exemple la clé de la résidence, chaque habitant de la résidence peut y accéder (en l'occurrence tousles utilisateurs du réseau bitcoin), la clé secrète en revanche est la clé de l'appartement ou le propriétaire seul et lui seul peut y accéder, (en l'occurrence le détenteur du compte bitcoin). On peut noter que malgré que les clés publiques soientdistribuées par le syndicat de la résidence, il n'existe en revanche aucun système centralisé pour les clés secrètes.  Toute perte de la clé secrète est irréversible et entrainera la perte des fonds dans le compte bitcoin de l'utilisateur. |

## 1.3 Le potentiel de la Blockchain

Le caractère décentralisé de la Blockchain, couplé avec sa sécurité et sa transparence, promet des applications bien plus larges que le domaine monétaire.

On peut classer l’utilisation de la Blockchain en trois catégories :

* Les applications pour le transfert d’actifs (utilisation monétaire, mais pas uniquement : titres, votes, actions, obligations…).
* Les applications de la Blockchain en tant que registre : elle assure ainsi une meilleure traçabilité des produits et des actifs.
* Les contrats-intelligents: il s’agit de programmes autonomes qui exécutent automatiquement les conditions et termes d’un contrat, sans nécessiter d’intervention humaine une fois démarrés.

Les champs d'exploitation sont immenses: banques, assurance, santé et industrie pharmaceutique, le supplychain de nombreux secteurs (agroalimentaire, luxe, commerce international, distribution, aéronautique, automobile...), industrie musicale, énergie, immobilier, vote...

La chaine des blocs est grand livre décentralisé avec l’historique complet des transaction dès la création du ce dernier, la base de donne est partage par toutes les nœuds du système, mis à jours par les mineurs, surveiller par tout le réseau, détenue par personne, c’est comme un journal interactifgéant ou tout le monde peut y accéder, et confirmer l’authenticité des transactions…

## 1.4 Le minage et la preuve de travail "Proof of Work".

Le minage du Bitcoin est le processus de créer, ou plutôt découvrir, de la monnaie Bitcoin, à l’ opposé des monnaie traditionnels scripturales qui peuvent être imprimé en cas de besoin, Bitcoin ne peut pas être créé aussi simplement que ça, il doit être "miné" à travers des procédés mathématiques. Bitcoin est un grand livre comptable publique qui contient les transactions passées, et le minage est le processus d'ajouter des nouvelles transactions dans le grand livre.

Le minage du bitcoin nécessite une mobilisation de ressources considérable, d'autant que le minage est crucial au développement une question c'est posé au fondateur de bitcoin comment inciter les utilisateurs pour dépenser leur énergie et leur temps pour le minage du bitcoin ?

SAKAMOTO avait trouver une réponse élégante a cette problématique, qui est tout simplement d'instaurer une récompense a qui ou a qu'elle réussira à résoudre le problèmes le premier, l'algorithme de récompense a fait office de catalyse qui a pousser les utilisateurs lambdaà miner du bitcoin en vue de faire profit, cette approche de SAKAMOTO a fait en sorte que maintenant les mineurs servent à maintenir le réseau Blockchain.

|  |
| --- |
| La réalité du minage.  Miner du bitcoin revient à résoudre des problèmes mathématiques, certes cette phrase est à la fois vrai mais à la fois trompeuse; la réalité est que le minage est le fait de résoudre des problèmes mathématiques **inutiles**. En vrai le minage est le fait de trouver le code SHA-256 (codeà 256 caractères composé de 0 et 1) correspondant à un algorithme qui le génère automatiquement chaque 10 dix minutes, le gagnant gagne le droit de mettre le prochain block ainsi qu'une récompense de 12.5BTC (6M25 MAD) plus les frais de transactions.  C'est exactement le même principe que jouer à la loterie, un nombre est générer automatiquement par une machine, le système récompense celui ou celle qui a trouvé le nombre gagnant.  Pour l'instant la récompense à la création du block est de 12.5 BTC, cette dernière sera divisée chaque 4 ans par deux, ainsi en 2020 elle sera de 6.25BTC et ainsi de suite jusqu'à ce que le dernier block sera crée en 2140 pour un total de 21Million de BTC. |

* Le minage en bref.

Imaginez dix personnes qui ne se connaissent pas dans une pièce : on en choisit une qui vérifie les transactions puis qui les écrit dans le registre. Une fois qu'elle a terminé, elle soumet son travail pour relecture aux neuf autres pour qu'ils approuvent.

Cette méthode totalement décentralisée pose immédiatement une question : qui va, et comment, choisir le membre (le nœud du réseau Blockchain) qui validera les transactions en cours et remplacer le tiers de confiance ?

## 1.5 Choisir le « mineur »

La plus célèbre et la plus répandue des « preuves » dans les Blockchains publiques est la « preuve de travail »

Elle consiste à vérifier qu’une transaction est valable (c'est à dire à vérifier que le débiteur possède bien les fonds en analysant les lignes précédentes du registre). Cette vérification fait partie du « consensus » mais elle ne demande que peu de ressources de calcul et peut être effectuée par n’importe quel ordinateur du marché.

**Consensus Bitcoin (validation) = vérification des transactions (simple) + PoW (compliqué)**

|  |
| --- |
| bitcoin et le dollar.  Pour que le bitcoin puisse se développer, il devait y exister une manière alternative pour l'obtenir autre que le minage, il devait y exister une manière d'acheter des BTC en échangeant du Dollar ou autres monnaies scripturales. Mais à quel prix ?  Ainsi en Octobre 2009, des gens de la communauté en instauré un système de change basé sur le dollar, en le postant sur un site s'appelant "New liberty standard.". ils s'étaient basés sur le cout en électricité pour produire 1 BTC, le premier cours de change fut instaurer a 1309BTC pour 1 Dollar, qui signifie simplement que chaque BTC avait une valeur de 0.08$.  Certain pensait que Liberty standard avait fait une fausse estimation et le cours réel devait être bien plus bas, néanmoins maintenant et pour la première fois, il existe un repère; un cours de change ou chacun peut échanger des BTCs contre n'importe qu'elle autre monnaie scripturale, ainsi fut la naissance de l'investissement dans le Bitcoin. |

# Chapitre 2 : comparaison entre le système classique et le bitcoin.

## 2.1La viabilité du bitcoin.

Avant de discuter des points faibles soit il ou fort du bitcoin et de la crypto monnaie, il parait pertinent de comparer entre les systèmes actuels ou pour ainsi dire les systèmes ayant déjà prouvé leur efficacité à travers l'histoire de l'humanité.

Pour ce faire on présentera tout d'abord le premier système qui a longtemps dominé le monde et qui fut la catalyse de l'apparition de la monnaie scripturale, on parle bien évidement de l'or. Puis par la suite en comparera avec la monnaie la plus dominante dans le monde qui est le dollar.

### 2.1.1 Or & bitcoin.

On présentera les donnée sous forme de tiré qui avec des perquisitions qui sera par la suite regrouper dans un tableau (Tableau1&2).

-**La rareté**: La quantité du bitcoin existant est limitée, tandis que l'or peut être miné dans la terre et possiblement dans des astéroïdes dans la future, Ainsi l'or est variable tandis qu'il ne peut pas exister plus de 21 million bitcoin.

-**La durabilité:** Grace au fait que le bitcoin est décentralisé et distribuer sur le grand journal publique, le bitcoin peut survivre une attaque nucléaire, tandis que l'or ne peut pas, puisque ça température d'évaporation est de 2856 °C, Or il existe l'éventualité que l'or des gouvernements serait dans des grottes bien en dessous de la terre pour assurer la protection de leurs réserve face à cette éventualité....

-**La portabilité**: Le bitcoin est très portable (une simple application dans votre Smartphone vous permet d'avoir tout l'argent dont vous avez besoin a une seule condition que vous possédiez une connexion internet...). Tandis que l'or présente l'inconvenant d'être lourd à transporter et d'attirer les regards indésirable, donc souci de portabilité et de sécurité.

-**La divisibilité**: L'or bien que divisible présente certain problèmes, ça divisibilité reste difficile et couteuse. Alors que le bitcoin, puisque qu'il est composé uniquement de bits il peut être divisible a jusqu'à 100 million de fois sans problèmes et sans aucun couts supplémentaires.

-**Le stockage**: L'or est très couteux pour son stockage car il a besoin d'être constamment protéger des malfaiteurs, aussià cause de sa grande taille il nécessite une infrastructure pour le déplacement. Or le Bitcoin est très simple à stocker (le cout d'un disque dur ...).

-La **Difficulté à falsifier**: L'or étant plus ou moins dur à falsifier, néanmoins il présente quelque challengestechniques comme par exemple l'or est considéré comme pur si sa densité présente 12% de son poids total, ( donc pour le falsifier on pourra par exemple jouer sur ce ratio ). Le bitcoin de l'autre côté et doté de mécanisme de la Blockchain et du proof of Work quirendent ce genre de manipulation très dures voire impossible.

Tableau 1: le système bitcoin et le système Or

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Rareté | Durabilité | Divisibilité | L'authenticité et la vérification | Stockage | L'égalité: | Difficulté à falsifier | Usage universelle | Portabilité |
| L’or | Oui | Oui | neutre | neutre | neutre | neutre | Neutre | Non | non |
| Bitcoin | oui | Oui | Oui | neutre | oui | oui | Oui | Non | oui |

### 2.1.2 Dollar & Bitcoin.

**-La rareté:** le bitcoin est plafonner à 21 millions de bitcoin actif dans le monde, le dollar en revanchene l'est pas, par exemple depuis 2008 la date de la crise l'émission du dollar a triplé.

-**La durabilité**: Les bitcoins peuvent se perdre ou être volé, mais ne peuvent en aucun cas être détruit, par contre la monnaie scripturale peut facilement être perdue, volé ou détruite malgré le fait qu'elle peut être remplacé facilement sans perte de valeur. Le bitcoin avec l'infrastructure adéquate peut durerà l'éternité.

-**La portabilité**: Bitcoin étant de nature digitale, ce qui implique que n'importe quel montant peut êtretransporté à n'importe quel distance facilement et gratuitement moyennant une connexion internet, la monnaie scripturale est plus ou moins aussi facile à transporter mais elle devient un inconvenant lorsque la quantité devient significative, dans ce cas elle nécessite une infrastructure et de la sécurité.

-**La divisibilité:** Chaque bitcoin peut être divisé jusqu'à 100 million de fois, alors que le dollar ne peut être divisé que 100 fois (le centime).

-**L'authenticité et la vérification**: Bitcoin étant un moyen digital, il doit être identifiéà l'aide d'une clé publique dans le grand livre, le dollar lui aussi est facilement vérifiable à l'œil nu par les experts.

-**Le stockage:** les clés privées qui contrôle l'accès des bitcoins peuvent être stockées dans du papier, dans le cerveau, ou dans une cléUSB, par contre le stockage de la monnaie scripturale nécessite une infrastructure lorsque la quantité devient significative.

-**L'égalité:** Tout les bitcoins sont traiter de la même façon sans discrimination, alors que dans le monde des monnaies scripturales, il existe des taux de change qui détermine la préférence d'une monnaie au profit d'une autre monnaie.

- La **Difficulté à falsifier**: Il est mathématiquement impossible de falsifier un bitcoin. Or les monnaies scripturales ont était falsifier depuis la nuit des temps.

Tableau 2: le bitcoin et la monnaie scripturale

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Rareté | Durabilité | Divisibilité | L'authenticité et la vérification | Stockage | L'égalité: | Difficulté à falsifier | Usage universelle | Portabilité |
| Fiat | Neutre | neutre | oui | oui | neutre | oui | Neutre | oui | oui |
| Bitcoin | Oui | Oui | oui | neutre | oui | oui | Oui | non | oui |

Maintenant et après comparaison du bitcoin avec les deux systèmes classique à savoir l'or et la monnaie scripturale, ceci nous a permet de démontrer la compétitivité et la viabilité de ce nouveau système cryptographique, maintenant nous nous intéresserons au avantages et aux inconvenant de ce système.

## 2.2. Avantages du bitcoin:

Ce système étant d'une efficacité très impressionnante permet de contourner divers failles du système classique.

### 2.2.1 Le cout de transaction très faible.

Le premier avantage du bitcoin réside dans son anatomie, c'est à dire le fait qu'il soit un réseau décentralisé, n'ayant guère besoin d'une entité régulatrice qui veille à son bon fonctionnement, n'ayant aussi pas besoin d'une personne tierce pour servir de "bridge"[[5]](#footnote-6) entre l'acheteur et le vendeur.

Le bitcoin fonctionne avec le modèle pair à pair, qui dit pair à pair dit; contact direct, anonyme et sécurisé entre les deux parties prenantes de la transaction, cette option constitue un avantage concurrentiel très conséquent et qui bien sur joue en la faveur du bitcoin.

Le système classique présente un inconvenant majeur pour l'utilisateur lambda, qui est tout simplement les couts de transaction très hauts, ce cout est en effet le cout de l'intermédiation de la banque, cette marge va directement à la banque et lui sert de rentabiliser son intervention.

Les banques contemporaine étant trop puissante de nos jours, peuvent se permettre d'imposer des grandes marges sans qu'aucune perte de clients ne soit enregistrer, pourquoi; parce que tout simplement il n'existe aucun moyen de contourné les banques ( hormis bien sur la crypto monnaie qui est actuellement dans son phase "Fœtus" ), soit vous faite partie du système bancaire et vous payez les frais exorbitant ou vous vous trouver propulser soudainement au moyen âge sans aucun accès aux services indispensables des banques...

Le cout des transactions étant variable de banque en banque mais elles sont généralement élever surtout dans les régions à faible concurrences, en l'occurrence les banques qui se trouve en situation de monopole. Ainsi les gens vivant en Afrique et qui utilise des plateformes d'échanges tel que Money gram ou encore Western Union ce voient "taxé" de 8 à 12 % par transaction, ce qui représente un cout conséquent, considérant le fait que les africains comptes parmi les gens les plus pauvres de la planète.

En 2009 la banque mondiale a lancé une opération dite: "objectif 5x5"[[6]](#footnote-7). Qui avait pour but de réduire les couts des envois de fonds partout dans le monde a 5% maximum, un calcul a était effectuer pour supporter cette thèse et qui stipule qu'au cas de l'application de cette opération, ceci permettra aux migrants africains d'économiser 4 milliard de dollars par ans, ce qui est en effet un chiffre très conséquent!

D'autre part le bitcoin présente des avantages non négligeable en la matière, les transactions sont instantanées avec cout d'intermédiation très faible qui oscillent entre 1% et 3%, ce qui séduira forcement les utilisateurs aux quarts coins du globe.



Figure 3: les couts de transaction de Bitcoin

### 2.2.2 Le bitcoin une alternative pour les populations ne pouvant pas accéder au servies bancaire.

Un autre point pesant dans la balance; est l'accessibilité et la facilité de l'accès aux services ...

Essayant de voir la grande image, il n'existe pas que les gens habitant dans les zones fortement urbaniser ou l'accès à une banque est aussi simple que de dire bonjour, bien au contraire il existe des gens vivant dans des régions reculer ou ce type de service est en effet très rare, et ne pas les inclure dans le réseau financier relève de la discrimination, puisque ne pas être y inclut signifie l'isolation.

La banque mondiale avait publié un article qui stipule que 2.5 Milliard de personnes ne sont pas incluses dans le système financier pour plusieurs raisons:

- La non existence d'une infrastructure dans la zone d'habitat de ces gens par exemple pour les pays pauvres où dans les régions éloigner...

- La discrimination envers la femme dans certains pays, ou ces femmes-là, ne peuvent pas créer un compte bancaire a titre personnelle, et peuvent uniquement créer un compte si un homme de la famille ( père, frère, fils...) donne son accord; une petite anecdote est celle d'une jeune fille pakistanaise nommé Parisa Ahmadi, qui malgré le fait qu'elle soit une élève brillante, elle fut empêchée de continuer ses études à cause de contrainte familiales ( la perception de la femme dans son pays natal, et la difficulté d'accéder aux services financier), et qui grâce à une entreprise étrangère ou Parisatravailla qui payait ses employer en Bitcoin[[7]](#footnote-8), put finalement financer ses études sans l'aide de sa famille et continuer son rêve[[8]](#footnote-9)...

Ainsi toutes ces tranches de gens qui ne peuvent pas participer au monde financier, peuvent être incluse grâce à l'implémentation du bitcoin; bien sur l'accès à ce service nécessite un accès internet, un ordinateur ou à défaut un Smartphone, mais avec le développement technologique ces composante qui permettent l'accès au bitcoin sont de plus en plus accessible au large publique.

Il faut tout de même rester réaliste et garder les pieds sur terre, le bitcoin n'est pas un remède miracle contre toutes les maladies financière mondiale, ce qui est sur ce qu'il offrira d'avantage d'opportunité pour les gens "délaissé" par le système classique, ceci se répercutera sur le niveau de vie de ces gens.

### 2.2.3 Problèmes du " Double Spending" et les problèmes des généraux byzantins.

Même sans considérer les multiples utilisations possible du bitcoin et de la Blockchain, bitcoin en lui-même est une révolution extraordinaire dans le monde de l'informatique, qui n'est pas apparu du jour au lendemain mais qui a suit une évolution de plus de 20 ans dans la monnaie cryptée et plus de 40 dans le domaine de la cryptographie.

Bitcoin est la solution a un problème qui a longtemps toucher le secteur de la monnaie digitale est qui a savoir le problème de la double dépense "Double Spending"; car avant l'apparition de la monnaie régie par la Blockchain, la monnaie virtuelle était comme n'importe quel n'importe quelle donnée virtuelle infiniment copiable (comme la capacité de cloner n'importe fichier à l'infini), et il n'existait aucun moyen de vérifier que la monnaie envoyer est la véritable monnaie existante qui n'a pas était virtuellement cloner sans passer par un intermédiaire qui est en effet la banque (ou une autre entité telle que Paypal par exemple), que ce chargera de vérifier l'authenticité de la monnaie.

Un autre problème tout aussi crucial que le bitcoin a réussi à résoudre; est le célèbre connu : "problème des généraux byzantins"[[9]](#footnote-10), l'énoncer est le suivant: plusieurs généraux byzantins sont entrain de assiéger une ville ennemie, pour ce faire il doivent élaborer un plan en commun pour passer à l'offensive, le succès ou la faillite de l'invasion dépendra de la collaboration des généraux, mais il existe deux problèmes; le premier est que les généraux n'ont aucun moyen de ce contacter directement mais doivent le faire par l'intermédiaire de messager, ainsi le message est à la merci de la façon dont le messager l'exprimera, le deuxième problème est que parmi les généraux il puisse exister des traitresqui essaierons de faire échouer l'invasion.

Le bitcoin résout le problème du "double Spending" en combinant la fonctionnalité du pair à pair avec le système de clé privé et publique pour créer une nouvelle forme de monnaie digitale. L’appartenance de chaque bitcoin est enregistrer dans le grand livre publique et approuver par les protocoles de la Blockchain et des mineurs.

Pour le second problème cité, la réponse se trouve sous forme d'un algorithme mathématique qui prend en compte à la fois les différentes informations nécessaire, le transport d'un point à l'autre, mais également les potentiels problèmes de défaillances du système, qu’elles soient d'origine matérielle, accidentelles, ou encore malveillantes.

Ce système révolutionnaire bitcoin est le premier à avoir trouvé la solution au du problème du transfert de la propriété digitale, dans le monde d'internet, à un interlocuteur qui peut être inconnu tout en garantissant la sécurité de ce transfert, c'est à dire ce transfert aura lieu et que le contenu ne sera pas volé ou victime d'une attaque, et que la personne ne peux pas revenir dessus ("Backtrack")

### 2.2.4le complet anonymat: une épée à double tranchant.

Le bitcoin opérant par le système de la clés publique et la clés secrète, enregistre toutes les opération dans un grand livre accessible à tous, néanmoins bien que toutes les opération sont inscrites, personne ne connait à qui appartient cette transaction, a l'exception du détenteur de la clé secrète, ainsi les deux partis de la transaction sont les seules à savoir de quoi il s'agit (supposant une transaction entre A et B; seul A et B savent de quoi qu'il s'agit; et A et ne connait pas l'identité de B et inversement...).

Donc ce système promet l'anonymat le plus complet pour une transparence complète, surtout dans l'ère ou les lobbies tels que Facebook et autre société sont soupçonné de la vente d'information de ses utilisateurs.

Ce même système est d'ailleurs utiliser par les banques classique, cette dernière pour jouer son rôle d'intermédiaire, demande des information complètes et détailler de la situation complète de chaque contribuant , ces informations peuvent d'ailleurs être non justifiée, l'argument principal des banques centrales; est que cette dernière fait office de gendarme qui garantis la sécurité et la traçabilité de chaque contribuant, ainsi en cas de problème, de vol ou de soupçons elle peut remonter jusqu'à la source du problème.

Par contre pour le bitcoin l'histoire est différente, les utilisateurs peuvent s'inscrire avec des emails qui sont affilier uniquement à des pseudonymes, ainsi aucune information en dehors du réseau n'est nécessaire (telle que le nom, l'adresse ...). Cette approche à double tranchant garantis aux utilisateurs de bitcoin d'être àl’abri des yeux et des oreilles des gouvernements.

Ce point est très important, et pour être réaliste, cette option ne présente pas toujours un avantage, on dire qu'il s'agit d'une épée à double tranchant pourquoi?

D'une part il a les utilisateurs honnêtes qui ne veulent pas que les banques sachent qu'ils viennent d'acheter un nouveau téléphone, voulant préserver leur vie privée, leur argument est simple: "j'ai un rideau dans ma chambre par principe non pas parce que je fais quelque chose de mal...", bien entendu il n'existe pas que les utilisateurs honnêtes il existe aussi les malfrats qui profitant de l'anonymat de bitcoin, l'utilise pour tout sorte d'opérations illicite que nous verrons dans le prochain chapitre.

## 2.3. Les inconvenants du bitcoin.

### 2.3.1 Retour sur l'anonymat ("la face cachée de la lune").

L'anonymat dans le bitcoin relève d'un sujet sensible qui a fait pas mal de polémique et débats, certain refuse de voir le bitcoin être implémenter à grande échelle, par peur de la non réglementation et surtout que depuis 2013 l'affaire de "Silk Road" un site de vente de drogue et qui utilise Bitcoin fut un buzz énorme au grand public.

Depuis l'affaire "Silk Road" un site du Dark web américain qui suite aux investigation de l'FBI a était clôturer en octobre de 2013, ce site était tellement vaste que d'après le FBI il représentait plus de 70% du trafic de drogue du marché mondial, il permettait aussi de se fournir en armes et autres services tel que le piratage de compte Facebook et autre comptes bancaires, le flux de ce site était tellement grand que l'FBI estime que plus de 9 million de bitcoin ont circuler à travers ce site, pour un total équivalent de 1.2 milliard de dollars.

Une des plus grandes barrières qui freine le développement du bitcoin est sa mauvaise perception par le grand publique, comme étant un catalyseur pour le blanchiment d'argent sur le "Dark web", l'achat et la vente d'arme et de drogue et tout autre activité prohiber par le gouvernement.

Bitcoin et la Blockchain étant eux même neutres, et comme n'importe quel technologie peuvent être utiliser pour de bonnes comme pour de mauvaise fins, bien que qu'il existe une possibilité que le bitcoin peut être utilisé par des malfrat pour les mauvaises raisons, il présente néanmoins plus d'avantage que d'inconvenant et son potentiel ne devrait pas être gâcher à cause de ces derniers.

### 2.3.2 Soucis de sécurité : La fragilité du réseau bitcoin:

Une autre barrière significative qui freine l'adoption du Bitcoin est la fragilité des utilisateurs envers les tentatives de vols, les arnaques dans l'industrie.

La faillite de la société japonaise (Tokyo) MtGox le plus grand réseau d'échange de Bitcoin de son temps, en 2014 a fait couler pas de mal d'encre est ainsi devenu une preuve irréfutable de la fragilité du réseau bitcoin.[[10]](#footnote-11)

Une explication s'impose; comment diable expliquer que des "coins" peuvent disparaitre pendant des mois, dans le journal le publique le plus transparent qui soit ?

La réponse officielle de MtGox est que son système était infiltrer par des arnaqueurs qui ont réussi à exploiter un bug courant qui s'appelle le "Transaction malleability bug", ce bug permettait les arnaqueurs de dépenser doublement "Double Spend" leur argent tout en faisant croire que a la société MtGox qu'elle reçoit réellement les fonds, cette dernière qui étant une plateforme d'échange entre divers détenteur de fonds bitcoin, suite à cette crise cette dernier a simplement "disparu" avec plus de 750 000 bitcoin, laissant les utilisateurs avec des pertes plus ou moins importantes.

Les analystes externes reste perplexes; ils ne savent pas avec certitude si cette dernière a était réellement pénétrer de l'extérieur ou simplement il s'agit d'une manigance pour cacher les fraudes que la société a commis en interne...

Le problème est que quel que soit la cause soit elle interne ou externe ce genre de manipulation continue à persister, avec le CEO d'une société appeler "MOOLAH" qui disparait avec l'équivalent de 1.4 de dollar en bitcoin en octobre de 2014, ainsi que de 2million en Vericoin qui fut volée en juillet de 2014, et 620.000 de dollar pirater dans une opération de Minining en juin de 2014.

En outre les vols, il existe aussi des risques intrinsèque du système par exemple la perte de sa clés secrète, entrainement la perte des bitcoins pour son utilisateur mais aussi pour tout le réseau économique, il est en de même pour la suppression non intentionné de ses propre bitcoin ou aucun retour en arrière n'est possible, les transaction non réversible et le dénis de service reste toutefois des problèmes très récurant et très graves, qui laisse à penser que le Bitcoin a encore besoin de modification et de raffinement pour enfin atteindre ca phase "adulte".

Les modèles de l'industrie Blockchain en encore besoin de ce solidifier et murir, pour offrir plus de garantie de sécurité en place, pour stabiliser l'industrie et ainsi garantir les intervenant intérieur ou extérieur de distinguer entre les bon et les mauvais "joueurs".

### 2.3.3 Volatilité du bitcoin.

Lors de ca création le bitcoin ne valait pas plus que rien, mais au cours de son évolution il s'est avérer qu'il est doté d'une volatilité extraordinaire; une volatilité si haute en effets qu'elle n'a jamais était enregistrer dans l'histoire des actifsréels.Des pourcentages de hausse qui défient les lois de l'entendement. Les acheteurs de bitcoin de la première heure ont profité de cette envolée, [parfois pour devenir milliardaires](https://bfmbusiness.bfmtv.com/entreprise/humilies-par-mark-zuckerberg-ces-deux-freres-deviennent-les-premiers-milliardaires-en-bitcoins-1319147.html). Mais paradoxalement, elle décrédibilise le bitcoin en tant que monnaie.

La volatilité est un risque, bien que certaines choses risquées sont bonnes; comme les actifs boursier par exemple, mais le problèmese pose lorsqu'il y a trop de volatilité qui présente une réelle entrave pour l'utilisation courante; "trop de risque tue le risque", le but principale du Bitcoin étant de remplacer la monnaie scripturale et ainsi devenir une monnaie courante, mais à cause de cette volatilité insoutenable, le cours du Bitcoin peut faire des sauts gigantesque en quelques secondes.

Un rapide exemple permet de comprendre pourquoi les variations extrêmes du bitcoin le rendent parfois inutilisable. Pour cela, il suffit d’imaginer l’achat d’un [iPhone X](https://www.01net.com/tests/test-iphone-x-un-apercu-du-futur-bien-ancre-dans-le-present-5849.html) valant 0,1 bitcoin - environ 13000 dirhams à l’heure actuelle. En raison des limites techniques liées à une utilisation massive, les délais avant que la transaction soit effective peuvent atteindre plusieurs heures. Au moment du transfert, le débit pourrait finalement correspondre à 12000 dirham - l’utilisateur serait ravi - ou à 14000 dirham - Apple serait ravi.

Pour les vendeurs comme pour les acheteurs, il s’agit donc de spéculer à chaque transaction, qu’il s’agisse d’un iPhone, d’une voiture ou d’un café. Une prise de risque impensable pour des entreprises dont la rentabilité dépend de marges de l’ordre de quelques pourcents.[[11]](#footnote-12)

Le Bitcoin étant risqué de ca nature les utilisateurs le considère comme une source d'investissement (ce point sera traiter dans le chapitre suivant) et non pas un moyen de transaction,«La volatilité des actifs cryptographiques est une sorte de problème de la poule et de l’œuf», déclare auteur de Blockchain et consultant Omid Malekan. «L'une des raisons de la volatilité du Bitcoin est que ses marchés sont très peu liquides et que le meilleur moyen de rendre les marchés plus liquides est de rendre le Bitcoin moins volatil.» En effet, il faut plus de personnes pour intégrer un marché risqué. Réduire le risque est une énigme.[[12]](#footnote-13)



Figure 4: Cours du Bitcoin depuis sa création

### 2.3.4 Minage trop coutant.

Le minage du bitcoin une pratique qui nécessitait à l'aube du bitcoin qu'un simple ordinateur et une modeste consommation d'énergie pour résoudre les problème mathématique et ainsi générer des bitcoins, cette ère est malheureusement bel et bien révolue, car maintenant des sociétés voient le jours avec l'unique but le minage intensif du bitcoin en vue de générer des profits, et qui par conséquent consacrent des moyens énormes pour réaliser cette objectif, surtout que le minage deviendra de plus en plus difficile au cours du temps.

En d'autre mots; la production annuelle du bitcoin consomme plus de 29 TWh( térawatt heurs, l'équivalent de 1 million de mégawatt heurs) cette consommation est dédié au fonctionnement des ordinateurs qui sont derrière cette opération de minage, ce chiffre est énorme car cette consommationconsiste en 0.13% de la consommation globale de l'électricité au monde entier, et d'aprèsDigiconomist[[13]](#footnote-14), ceci classera le bitcoin au 61 rang comme s'il était un pays à part entière.

En effet le minage de bitcoin utilise plus d'électricité que 156 pays individuels, même plus que notre pays le Maroc, ainsi que la majorité des autres pays.



Figure 5: Indexe de consommation du Bitcoin

# Chapitre 3: Bitcoinautant qu’un actif financier.

## 3.1 Pourquoi Bitcoin est considéré comme un actif financier.

La majeure partie des transactions du bitcoin impliquent des transferts entre des spéculateurs. Les achats de biens et services représentent 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, mais avant d’investir il faut prendre en considérations plusieurs facteurs.

-Le premier facteur est que la plus part des économistes ne considèrent pas le bitcoin comme un actif financier.

-Deuxièmement le bitcoin est un investissement complexe car il a des caractéristiques uniques, et avec des caractéristiques uniques, vient un risque unique.

- Finalement le bitcoin est une monnaie sans régularisationmonétaire, et générée par le Minage qui résulte un taux de croissance prédictible. L’adoption du bitcoin dans un portefeuille peut êtreintéressante d’un point de vu d’investissement.

La raison est le bitcoin n’a aucune relation avec la macroéconomie, et le développement financier, par contre le bitcoin est seulement sensitive à la loi de l’offre et la demande, et autre facteurs qui sont spécifique à la crypto-monnaie, comme l’attraction du bitcoin, la forte **volatilité** du prix des crypto-monnaies entraine parfois de fortes fluctuations. Si cela peut amener à de gros **gains**, cela peut aussi amener à de lourdes **pertes**. Il est donc recommandé d’investir seulement une petite partie de son capital.

## 3.2 Le couple rendements risque de bitcoin.

Selon la théorie moderne de portefeuille développée par Markowitz, les agents ont pour but ultime de combiner un ensemble d’actifs ayant une rentabilité maximale avec un niveau de risque donné ou ce qui revient au même un risque minimal pour un niveau donné de rentabilité. C’est le portefeuille efficient, En ce qui concerne le choix de la mesure de risque, plusieurs alternatives se présentent.

Par exemple, dans le modèle de gestion de portefeuille de Markowitz, le risque du portefeuille est déterminé par sa variance. Ainsi, tous les écarts, négatifs ou positifs, par rapport à la rentabilité espérée sont pris en compte. Le résultat principal de ce modèle stipule qu’à l’optimum, le portefeuille détenu par l’investisseur doit être parfaitement diversifié. Dominant depuis plus un demi-siècle, le modèle de Markowitz reste l’un des plus utilisés par les praticiens. Il s’appuie sur l’hypothèse forte que les agents possèdent une fonction d’utilité quadratique et utilise (l’écart-type (ou la variance)) des rendements des titres pour mesurer le risque d’un portefeuille. Le modèle de Markowitz ne définit pas un unique portefeuille optimal mais génère une frontière efficiente comprenant l’ensemble des portefeuilles optimaux.



Figure 6: la frontière efficiente

C’est à l’investisseur de choisir son portefeuille optimal en fonction de son degré d’aversion au risque, L’important est qu’il existe deux principaux facteurs de risque qui préoccupent les investisseurs.

C’est le risque de marché et le risque spécifique à l’entreprise. Le risque spécifique à l'entreprise est également appelé risque non systématique, risque unique ou risque diversifiable. Le risque unique est déterminé par des facteurs micro-économiques. Chaque facteur microéconomique n'influence que l'entreprise en question. Fama et French (1993) sont des exemples bien connus de risques spécifiques à des entreprises: *Small moins Big et High moins High.*

La diversification peut éliminer le risque spécifique à l’entreprise. Ce qui est visible à la figure si dissous, où spécifique à l'entreprise correspond à la ligne convexe montrant que plus le nombre d'actifs est élevé, plus le risque spécifique à l'entreprise est faible (Bodie, Kane et Markus, 2014).



Figure 7: le Risque systématique et le risque spécifique

Cependant, ce n'est pas tout à fait vrai. Cela sera expliqué après le risque de marché. Le risque de marché est également appelé risque systématique ou risque non diversifiable. Le risque de marché se caractérise par le fait qu’il est inhérent à l’investissement sur le marché. En aucun cas, cette forme de risque ne peut être réduite de quelque montant que ce soit. Le risque de marché est exposé à des facteurs macroéconomiques tels que les cycles de conjoncture et les taux d’intérêt. Chaque facteur influence le marché dans son ensemble (Bodie, Kane et Markus, 2014). Dans la figure, le risque de marché est indiqué par la ligne droite horizontale. Peu importe le nombre d'actifs, le risque de marché sera toujours le même. En d'autres termes, la diversification ne peut pas éliminer tous les risques.

Mais dans le cas de bitcoin Il existe deux principaux composants de risque qui nécessitent une élaboration plus poussée, car la plupart des actifs ne sont pas exposés à ces risques. Tout d'abord, le prix des bitcoins est extrêmement volatil. La volatilité extrêmeest une dimension supplémentaire lorsqu’on envisage d’investir dans le bitcoin. Du point de vue du risque, cela n'a pas d'importance, mais considérons que plus un actif est risque plus qu’il est rentable. Un actif avec une plus grande volatilité générera moins d’utilité, ce qui, dans la pratique, constituerait une considération importante pour les investisseurs.

Un autre problème est que les bitcoins, contrairement aux monnaies traditionnelles, sont sensibles aux pirates. Au moyen d'attaques de logiciels malveillants ou de cyber-attaques comme cite précédemment dans le chapitre 3, il est possible de voler des bitcoins et de déstabiliser le système, ce qui peut générer une volatilité des prix encore plus grande. Selon Moore et Christin, qui ont examiné 40 échanges Bitcoin, 18 des 40 échanges ont-ils été fermés en raison d'attaques informatiques? En 2014, même le plus grand échange de bitcoins s'est effondré à la suite d'une cyberattaque. Puisque le bitcoin est et sera une monnaie numérique, ce sera une menace permanente et parfois une réalité.

Bitcoin est unique en raison de plusieurs caractéristiques. Même si certaines de ces caractéristiques donnent un grand avantage à bitcoin certains posent également des problèmes. Deux problèmes principaux qui entravent le fonctionnement de Bitcoin seront abordés sous peu. La volatilité est beaucoup plus élevée par rapport aux devises largement utilisées, ce qui crée un risque important à court terme pour les utilisateurs effrayés.

Bitcoin ne fonctionne donc pas bien comme moyen d'échange. Les prix en Bitcoin des biens de consommation exigent des nombres très impairs avec des zéros non significatifs, ce qui est inquiétant pour les acteurs du marché de détail, rendant Bitcoin ne fonctionnant pas bien comme unité de compte. Baur et al. (2015) confirment que le bitcoin est davantage un actif d'investissement qu'une devise, Afin de déterminer la fiabilité et l’attractivité du bitcoin, nous avant choisi le dollar comme repère pendent les années 2015, 2016,2017 pour faire notre analyse vue que ce dernier représente le volume de transaction le plus élevé dans le marché financier.

## 3.3 mesure de performance de bitcoin.

Figure 8: cours de clôture BITCOIN/USD (2015-2016-2017)

Figure 9: Volume des transactions Bitcoin/USD (2015, 2016, 2017)

En analysant les graphiques des cours du bitcoin pendant les années étudies en constate que l’investissement en bitcoins présente une très grande volatilité mais également des rendements très élevés. Pour étudier la volatilité et le rendement on va procèdera par la Méthode de calcul suivante :

### 3.3.1 La moyenne.

La moyenne ou valeur moyenne, est la mesure de tendance centrale la plus importante pour une variable. En mathématiques, **la moyenne** est un outil de calcul permettant de résumer une liste de valeurs numériques en un seul nombre réel, indépendamment de l'ordre dans lequel la liste est donnée.

La moyenne des cours de clôture du Bitcoin/USD pour les années étudié :

|  |  |  |
| --- | --- | --- |
| La moyenne 2015 | La moyenne 2016 | La moyenne 2017 |
| 272.0233971 | 566.9958193 | 3981.071526 |
| Taux de variation | 108.43% | 602,13% |

En comparent les moyennes, on constate une l’évolution spectaculaire de 108.43% entre 2015 et 2016 et de 602,13% entre 2016 et 2017 choses qui indique une très grande rentabilité.

### 3.3.2 La variance.

La variance est une mesure de dispersion qui utilise toutes les Observations. Elle est basée sur la déférence entre la valeur de chaque Observation (x) et la moyenne des observations pour un échantillon La déférence entre chaque observation xi et la moyenne est appelée

Écart par rapport à la moyenne.

La variance des cours de clôture du Bitcoin/USD pour les années étudié :

|  |  |  |
| --- | --- | --- |
| La variance 2015 | La variance 2016 | La variance 2017 |
| 3471.870196 | 19140.06389 | 15897566.81 |

La variance de l’année 2016 et surtout 2017 qui représente une valeur très élever indique des écarts importent expliquer par la forte volatilité du cours du bitcoin/USD.

### 3.3.3 L’écart-type.

L’écart-type est une mesure de la dispersion des cours par rapport à la moyenne, indiqué pour chaque dimension évaluée entre parenthèses après la moyenne. La formule de calcul exacte est la racine carrée de la variance, cette dernière étant la moyenne au carré des écarts avec la moyenne. Plus simplement, ce nombre indique dans quelle mesure la moyenne est une valeur représentative et fiable pour interpréter le résultat.

L’écart-type des cours de clôture du Bitcoin/USD pour les années étudié :

|  |  |  |
| --- | --- | --- |
| L’écart-type 2015 | L’écart-type 2016 | L’écart-type 2017 |
| 58.922 | 138.347 | 3987.175 |

*Grosso modo* :**plus l’écart-type Est important, plus la dispersion des cours de clôture du bitcoin de chaque jour est important, ce qui signifie que la moyenne est peu représentative est que cette monnaie est peu fiable en ce qui concerne conservation de valeur et se caractérise par une grande volatilité.**

### 3.3.4 Le coefficient de variation.

Le coefficient de variation est une mesure de dispersion relative, il mesure l'écart type relatif à la moyenne.

Il est généralement exprimé en pourcentage. (L’écart-type/ La moyenne) \*100

|  |  |  |
| --- | --- | --- |
| Coefficient de variation 2015 | Coefficient de variation 2016 | Coefficient de variation 2017 |
| 21.66% | 409.83% | 99.84% |

Généralement pour un investissement l’actif le plus intéressent est celui avec un coefficient de variation moins élevé.

### 3.3.5La covariance.

En [statistique](https://fr.wikipedia.org/wiki/Statistique), la covariance entre deux [variables aléatoires](https://fr.wikipedia.org/wiki/Variable_al%C3%A9atoire_r%C3%A9elle) est un nombre permettant de quantifier leurs écarts conjoints par rapport à leurs [espérances](https://fr.wikipedia.org/wiki/Esp%C3%A9rance_math%C3%A9matique) respectives. Elle s’utilise également pour deux séries de données numériques (écarts par rapport aux [moyennes](https://fr.wikipedia.org/wiki/Moyenne)).

Dans le cadre de notre analyse, l’étude de la covariance va nous permettre de déterminer le lien entre le cours et le volume du bitcoin vs USD.

|  |  |  |
| --- | --- | --- |
| Covariance 2015 | Covariance 2016 | Covariance 2017 |
| 688871862.7 | 798055434.9 | 2.61022E+12 |

Étant donné que la covariance est positive, lorsque la valeur du cours du bitcoin augmente celle du volume augmente aussi, c'est une relation linéaire positive.

### 3.3.6Coefficient de corrélation.

|  |  |  |
| --- | --- | --- |
| Covariance 2015 | Covariance 2016 | Covariance 2017 |
| 4.54168E-10 | 6.90046E-11 | 2.92132E-13 |

Le coefficient de corrélation varie entre -1 et +1. Des valeurs proches de -1 ou de +1 révèlent une forte relation linéaire. Plus le coefficient est proche de 0, plus la relation est faible.

Nous concluons que les rendements des cryptomonnaies sont peu exposés aux classes d’actifs traditionnelles - actions, devises. Nos résultats jettent un doute sur les explications populaires selon lesquelles le comportement des cryptomonnaies est guidé par ses fonctions en tant que participation à l’avenir de la technologie Blockchain similaire aux actions, en tant qu’unité de compte similaire aux monnaies, ou en tant que réserve de valeur similaire aux produits en métaux précieux. Dans le même temps, les rendements de la crypto-monnaie peuvent être prédits par deux facteurs spécifiques à ses marchés - la dynamique et les investisseurs.

Nos résultats remettent en cause les explications populaires selon lesquelles des facteurs tels que les coûts de minage les cours moyens ou la volatilité réalisée sont utiles pour prédire le comportement de la crypto-monnaie.

Enfin, nous documentons que la technologie de Blockchain incorporée dans les cryptomonnaies est un potentiel pour un gain significatif mais aussi à des pertes monumentales, certes les gens qui ont bénéficié le plus sont ceux qui était présent lors de la naissance de ce dernier, un exemple célèbre est les 2 des pizzas acheter à 10.000 bitcoin en 2010, leur capitalisation a était faite en 2014 pour un total astronomique de 5million de dollar), lui donnant le titre de la pizza la plus chère au monde![[14]](#footnote-15)

Petite anecdote personnelle à ce sujet: nous avons commencé l'écriture de ce projet de fin d'étude en début de mois d'avril à cette date le bitcoin valait un peu moins de 40.000 DH le BTC en 15 Mai le prix du BTC a doublé de ca valeur atteignant presque 80.000DH.

En outre et malgré que cette ère et belle et bien révolue le bitcoin reste encore une source d'investissement avec un potentiel énormegrâceà son volatilité impressionnante. Bien sûr il ne faut pas se laisser aveugler par les gains énormes car qui dit gain énorme dit aussi perte énorme comme le célèbre dicton le résume "le malheur des uns fait le bonheur des autres" ainsi il est conseillé d’agir avec prudence en utilisant les règles d'investissement de prudence déjà établie pour les actifs réels.

# Chapitre 4: Bitcoin et réglementation.

Nous nous étions intéresse durant les chapitres précédent à la puissance et aux défauts d'un système basé sur le Bitcoin comme monnaie principale, il est temps de voir maintenant la grande échelle, comment le monde réagira si un jour le Bitcoin ou autre monnaie à base de Blockchain deviendra monnaie souveraine principale.

## 4.1- Exemple contemporain de faillite du système monétaire.

Pour qu'une monnaie fonctionne, la confiance entre le gouvernement et les citoyen est essentielle pour garantir le bon fonctionnement du système, Or ce fil fragile a était rompus plusieurs fois au cours de l'histoire humaine. Citons quelques exemples contemporains.

### 4.1.1 La crise de l'argentine.

Tout a commencé en 2002 en argentine lorsque le gouvernement commença à imposer des restriction sur les sortis de devise à cause d'un manque cuisant dans les réserve de devise du pays, devenant de plus en plus sévère en 2013 et engendrant une inflation de 20%.

Les citoyen argentins ayant perdu confiance en leur gouvernement et dans les banques; gardaient des réserve de devises (le dollar principalement ) ou en Or, ce manque de confiance envers le gouvernement et les banques "officielle" donna naissance à des institutions non réglementaire qui jouaient le même rôle des banques mais sans les restrictions que le gouvernement leur imposait, ainsi l'économie est passer d'une économie à grande échelle ou les banques servent de relais, à une économie à très petite échelle ou chaque individus pour effectuer une transaction doit connaitre l'autre partis personnellement.

Ainsi les argentins cherchant une solution en commençait à s'orienter vers les monnaies virtuelle, à savoir principalement le bitcoin ainsi en juin de la même année les applications de transaction à base de bitcoin ont vu leur nombre de téléchargement doubler en argentine, qui en résulta d'une utilisation massive du bitcoin causant une hausse locale de 38% de son cours en argentine.



Figure11: popularité du bitcoin à travers le monde

### 4.1.2 La crise du Zimbabwe.

Zimbabwe est un autre exemple, Zimbabwe étant un pays généralement pauvre ce situant à la frontière de l'Afrique du sud, une large partie de son PIB provient du secteur primaire à savoir l'agriculture.

En 1999 Robert Mugabe président du Zimbabwe à l'époque commença la privatisation des terres servant à l'agriculture, causant une forte basse au PIB du pays, en 2000 le Zimbabwe entre en guerre avec le Congo, le Zimbabwe pour financer cette guerre commença à produire en masse de la monnaie ( le dollar zimbabwéen Z$) dépensant jusqu'à 22 million de dollar par mois, en 2008 l'inflation grimpe a des hauteurs astronomiques atténuant un nombre absurde de (6.500.000.000.000.000.000% qui ce lis 6.5 sextillion pour cent ), ainsi en 2009 le Zimbabwe abandonne le dollars Zimbabwéen, et ne le remplace par aucune monnaie scripturale.

Bitcoin étant un système décentralisé adhérant un nombre strict de règles, ce dernier a besoin d'une influence mondiale pour le dérailler de son bon fonctionnement, cette qualité rend ce système plus stable et immune à ce genre de manipulation et de mauvais management.



Figure12: Taux d'inflation au Zimbabwe

### 4.1.3 Kenya et le Bitcoin.

Kenya est un exemple de pays utilisant des monnaie virtuelle et ayant réussi à trouver à succès, grâce à une société du nom de M-PESA cette dernière étant une société mobile centralisé qui facilité les transferts de monnaie, elle est utilisée par 35 million de personnes se situant en Kenya, Tanzanie, Afrique du sud, Afghanistan, et l'inde.

Le fonctionnement de M-PESA est le suivant: les utilisateurs peuvent acheter et vendre des " Pass" pré payer grâce à leur téléphone, ces "Pass" peuvent être utilisé pour payer leur facture, ou pour payer directement leur achats, les frais d'intermédiation sont inversement proportionnelle à la taille de la transaction ce qui signifie plus la transaction est petite plus les frais sont grands (de 1% à 15%).En 2011, 10.000.000.000 de dollar ce qui l'équivalent de 30% du PIB de Kenya avait était transférer à travers le service M-PESA.

Malgré le fait que M-PESA n'est pas un système similaire du bitcoin et que la Blockchain représente encore plus d'avantage en matière de sécurité et de frais de transfert, il en résulte néanmoins n que cette expérience de M-PESEA reste un succès, une preuve que des systèmes virtuelle telsque le Bitcoin peuvent réellement marcher en pratique.

## 4.2 Bitcoin une solution à la crise mondiale économique ?

L'or est considérer comme la source ultime de valeur pour une caractéristique spéciale, la rareté aucune personne ou groupe ne peux créer a volonté de l'or "ex nihilo"; son émission reste soumise à la loi de la nature. Plusieurs études économiques et statistiques on était fait en la matière et en prouver que le taux d'inflation de l'or reste stable et restera toujours stable.

* *Bitcoin ou l'or virtuel.*

SAKOCHI NAKAMOTO le créateur du bitcoin s'est inspiré du modèle de l'or pour créer un système équivalent virtuel basée sur la rareté, avec une tendance déflationniste plutôt qu'inflationniste (qui est la norme pour la monnaie scripturale "fiat").

Il existe un nombre prédéterminé et fixé par le créateur à savoir 21 millions de bitcoin (en théorie certes mais en en pratique ce nombre devra être légèrement inférieur à cause des pertes irréversible de bit sous forme de perte de clé secrète...),ce dernier constitue un plafond auquel aucun bitcoin ne pourra être miné de plus, pour l'instant plus de 80% du total de ce plafond a était déjà générer. Ce plafond consiste un mur de brick qui signifiera que plus on s'approche de ce "mur" plus l'inflation diminuera et la valeur du bitcoin individuel augmentera.

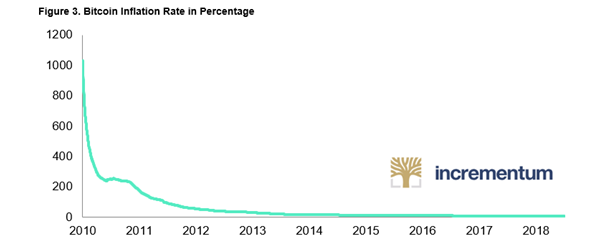


Figure14: Tendance déflationniste du bitcoin

Cette tendancedéflationniste est une caractéristique voulue, créer délibérément par le créateurSatoshi Nakamoto qui explique dans son article.   
«Pour compenser l'augmentation de la vitesse matérielle et l'intérêt variable d'exécuter des nœuds au fil du temps, la difficulté de la preuve de travail est déterminée par une moyenne mobile ciblant un nombre moyen de blocs par heure», a expliqué ce dernier. «Si elles sont générées trop rapidement, la difficulté augmente».[[15]](#footnote-16)

En Mai 2018, le taux d'inflation de Bitcoin est de 3.82%[[16]](#footnote-17). En raison de la difficulté de réajustement, il est impossible de simplement extraire davantage de Bitcoins en allouant davantage de ressources informatiques au réseau. Alors que de plus en plus de gens essaient d’exploiter Bitcoin, le Protocol augmente automatiquement la difficulté d’exploiter avec succès un Bitcoin et vice-versa. Une fois le taux d'inflation aura atteint zéro, les mineurs ne seront plus en mesure de gagner de l'argent à partir du minage des bitcoins nouvellement créés. Au lieu de cela, les frais de transaction devront augmenter ou le nombre de transactions augmenter.

## 4.3 La crise inflationniste et le bitcoin.

La monnaie scripturale "Fiat" compte parmi ses adeptes les personnes âgées qui ont du mal à accepter le changement. Selon les recherches d’Alice Leng[[17]](#footnote-18), les transactions sur devises réagissent moins aux chocs de marché et, si une réaction se produit, elle ne dure pas longtemps. C’est pourquoi le dollar américain semble être moins volatil que les crypto-monnaies. Mais la monnaie fiduciaire n’est pas aussi stable qu’elle ne le semble.

Comme le souligne VitalikButerin[[18]](#footnote-19), sur Twitter, le dollar américain est une monnaie extrêmement volatile qui a chuté de 96% depuis 1913. Pour savoir quelle monnaie est la véritable "bulle", considérons la histoire de la monnaie fiduciaire et en apprendre davantage sur sa volatilité.

Le prix du dollar américain a augmenté de 2 900,45% depuis 1900. Le taux d’inflation moyen est de 2,92% par an. En d’autres termes, 100 US $ en 1900 équivalaient à environ 3 000 US $ en dollars d’aujourd’hui. De plus, son prix a été multiplié par 30 en 118 ans. Le taux d’inflation en 1900 était de 1,20% et se situe maintenant à 2,18%. 100 $ aujourd'hui équivaudra à 102,18 $ en 2019.



Figure15: Le taux d'inflation historique en U.S

Les experts affirment que la première raison pour appeler le dollar américain une «bulle» plus grande que la crypto-monnaie provient de l’immunité de Bitcoin à l’inflation. La principale raison en est son offre limitée. C’est pourquoi Bitcoin est protégé de l’inflation qui menace toutes les monnaies nationales, dont le taux d’inflation dépend de la quantité croissante de monnaie imprimée émise par le Trésor.

Ces derniers affirment aussi que le dollar américain est plus une bulle que Bitcoin car personne ne sait combien de dollars américains ont été émis. Un BTC vaut toujours un BTC. Et le montant en dollars américains qu’un BTC vaut dépend de l’inflation de la monnaie fiduciaire. Qui dit bulle dit fragilité ce qui signifie que peut être le bitcoin peut être une solution à la crise financière et aux bulles spéculatives tant redoutées par les économies modernes.

## 4.3 Réglementation des pays envers le bitcoin.

La monnaie est synonyme de pouvoir, pour l'instant la monnaie est détenue par les élites du mondes, les banques centrales, les banques commerciale qui monopolise l'accès aux ressources monétaires, bitcoin bien au contraire promet la "démocratisation" des ressources monétaires en la plaçant dans la main de la peuple. Cette nouvelle approche promet un changement drastique de la balance politiques, mais ce changement ne pourra pas être fait non sans combat contre l’autoritéà savoir les l'état et les lobbys.

### **4.3.1 Droit de seigneuriage**.

Le droit de seigneuriage représente une source de revenu importante pour le budget de l’État. Par exemple, en 2016, la Fed a versé 92 milliards de ses profits nets au gouvernement fédéral des États-Unis.  En Europe, les profits nets de la BCE varient entre 10 et 30 milliards d’euros sur la période 2002-2015.

Les crypto-monnaies telles que le bitcoin privatisent les revenus de 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. 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-monnaies 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 États vont prendre, d’une manière ou d’une autre, le contrôle de la création des crypto-monnaies pour récupérer ces revenus de seigneuriage.

Toutefois, pour éviter les conséquences néfastes et les désordres financiers engendrés par une nationalisation des crypto-monnaies dans l’avenir, certains pays préfèrent interdire leur utilisation dès maintenant. La Banque centrale de Chine a même commencé à créer sa propre crypto-monnaie basé sur le Blockchain. Par contre, d’autres pays tels que les États-Unis, l’Allemagne, le Japon et la France, sans encourager l’utilisation des crypto-monnaies par le grand public, ont actuellement adopté une approche plutôt bienveillante en acceptant leur utilisation dans le commerce et leur échange sur les marchés financiers via des cotations des fonds investis en bitcoin.

### 4.3.2 Stabilisation macroéconomique et financière.

Le bitcoin remplit mal les fonctions de moyen d’échange, d’unité de compte 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. Bien que la déflation ait pu se développer dans une économie se servant uniquement d’une monnaie fiduciaire, comme c’est le cas au Japon, il est possible d’y remédier en pratiquant une politique monétaire suffisamment accommodante. La pratique des taux d’intérêt nominaux négatifs par des banques centrales européennes et japonaises ces dernières années s’inscrivent dans cette logique.

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

### 4.4Tentative de règlementation.

### 4.4.1 La Chine interdit.

Premier "producteur" de bitcoin au monde du fait de ses gigantesques fermes de serveurs informatiques utilisées pour le "minage" de la Crypto monnaie, la Chine envisage d'interdire cette activité jugée trop polluante. La principale autorité de planification économique chinoise, la Commission nationale du développement et de la réforme (CNDR), a publié une liste d'activités industrielles que le gouvernement souhaite restreindre ou bannir[[19]](#footnote-20).

Le projet inclut le minage de Crypto monnaies, dont le bitcoin, parmi les 450 activités que la Chine juge incompatibles avec les lois et réglementations en vigueur ou insuffisamment sûres ou trop polluantes et gaspillant des ressources.

La part de la Chine dans le minage du bitcoin est estimée entre 70% et 80% au niveau mondial. Le pays est aussi le premier producteur de matériel de minage (puces, ordinateurs, baies de serveur, etc.).

Cette étape, met en avant la volonté de la chine à s'approprier le monopole du bitcoin et du monde de l'argent virtuel en général, pour ainsi en avoir le contrôle complet, a l'instar de la censure qu'elle a imposée au site internet et au web visible en général.

### 4.4.2 La banque centrale allemande demande une réglementation mondiale.

L'approche de l'Allemagne est différente cherchant des solutions réalistes à ce problème moderne, la banque centrale allemande stipule que tout projet visant à réglementer les crypto-monnaies comme le bitcoin doit se faire à l'échelle mondiale, car des règles nationales ou régionales seraient difficiles à appliquer dans un environnement virtuel sans frontières.

Les autorités nationales à travers le monde, et en particulier en Asie, ont tenté de freiner l'essor du bitcoin et d'autres monnaies virtuelles, devises sous forme numérique créées et gérées par leurs utilisateurs et qui n'ont le soutien d'aucun gouvernement. Detelles règles à caractère local ne pourront pas à eux seuls contenir ce phénomène mondial.

Une régulation efficace des monnaies virtuelles ne serait donc possible que grâce à la plus grande coopération internationale possible, car le pouvoir réglementaire des Etats-nations est évidemment limité. L'année dernière, les autorités chinoises de régulation ont interdit de lever des fonds par émissions de Bitcoin, fermé des plates-formes locales d'échanges de Cryptomonnaies et limité le minage du bitcoin (procédé de création par lequel les transactions sont sécurisées). Cela n'a pas empêché l'activité de poursuivre son développement sur des canaux alternatifs en Chine.[[20]](#footnote-21)

# CONCLUSION.

Pour toute ca gloire, Bitcoin acompte jusqu'à présent pas plus que 12 million de portefeuille "Wallet" aux quatre coin du globe, avec 1 million de marchand acceptant bitcoin pour un total équivalent à 500 million de dollar investis dans des projets de cryptographique , ces nombres pale en comparaison avec 6 milliards de personne au monde, utilisant le système conventionnel "fiat", malgré le faible nombre de recherche effectuer d'étude à ce sujet, néanmoins des rapports anecdotique estime a seulement 1% d'homme d'affaire acceptant le Bitcoin.

C'est nombres mettent en valeur la perception du bitcoin parmi la populace générale; pour que le bitcoin soit une révolution, il devrait y avoir un changement global de force permettant à plusieurs facteur d'évolution de ce mettre en place:

* La première étant la perception du public; Bitcoin est toujours entacher par le mémoire de Silk Road et de MTGOX, la majorité des personne pense que toute cette histoire de Bitcoin n'est juste qu'une plaisanterie ou une arnaque, une étude a était faite à ce sujet en U.S (2014) et qui a conclu que seulement la moitié des américain connaissent l'existence de bitcoin, encore moins qui l'utilise (3%) avec 65% admettant ne jamais vouloir l'utilisé.
* Le second problème stipule que si bitcoin deviendra un jour une monnaie dominante dans le monde, ces propriétés exotiques créeront une nouvelle économie auquel les gens du 21 siècle ne sont pas encore prêts à affronter, car Bitcoin avec son plafond de 21 million est une monnaie déflationniste. L'économie actuelle ce base sur le modèle inflationniste, les économistes critique le système classique car il enduit une perte de valeur (10 Dollar maintenant ne vaudra que 5 dollar dans 20 ans par exemple), néanmoins en temps de crise cette réserve illimité de monnaie permet aux banques centrales de diffuser les crises économiques, en imprimant de la monnaie en masses, pour ainsi libérer le crédit et créer des nouvelles opportunités de travail.

Or le système Bitcoin étant un système qui ne nécessite pas l'intervention des banques centrales, les économistes prévoient que le système bitcoin réagira mal en situation de crise, les utilisateurs préférant garder leur BTC de peur qu'il gagne en valeur, ainsi le système sera en manque de liquidité à cause de la thésaurisation excessive, ce qui rétractera d'avantage le cours de la monnaie et qui aura pour effet d'accélérer encore d'avantage la crise économique telle qu'une boule de neige. Sans banque centrales pour jouer le rôle de préteur de dernier recours, le cours de la monnaie gèlera et personne n'utilisera le BTC d'avantage ce qui sera une crise économique au part avec la grande dépression de 1929.

* Un troisième point est la compétition; et s’il existait un système qui offrait tous les avantages de la monnaie digitale, sans les dangers réel ou fictif du système bitcoin? Et si ce système existait déjà sous la tutelle d'une société que tout le monde déjà fait confiance? Il s'agit en effet de la société Apple, car cette dernière avait déjà révéler son ambition de créer un système de monnaie digitale, ce basant sur les principes conventionnels, grâce à sa renommer mondiale a son large accès au grand public la "Pomme" trouvera plus de facilité d'instaurer son système que le Bitcoin. Le problème de la compétition reste très dur à résoudre , non pas car les crypto monnaie sont inférieurs, bien au contraire les services offerts par Apple ou autres tel que Visa ou Paypal reste des services soumis au système conventionnel avec tous les défauts qu'on vient de citer au cours de cette étude, alors que le Bitcoin offre des avantages indéniables en la matière, mais la question la plus importante qui se pose est "Pour quel système optera le monde ".

### Épilogue.

Le bitcoin n'est pas encore un produit fini il est encore dans ca phase "fœtus" ou il a encore besoin de pas mal de modification pour qu'il soit viable à très grandes échelle, avec ses soucis de sécurité ( MT GOX et autre ), son anonymat complet a ca forte traçabilité qui le rend séduisant pour les gens mal intentionné ( l'affaire de SILK ROAD), ça tendance déflationniste qui le rend plutôt comme une réserve de valeur et non une monnaie d'échange, l'absence de réglementation et loi concernant le bitcoin est aussi un point dans la balance.

Grosso modo il existe un ultime facteur qui déterminera le future de la crypto monnaie : Si face à la compétition, est ce que les gens ayant foi en ses bienfaits et n'ayant pas peur de ses point faibles opterons pour la crypto monnaie, tout en abandonnant le système des monnaies scriptural auquel il ont été habitué, ce n'est guère une tâche facile et personne ne peut dire avec certitude si le bitcoin verra le jour un jour ou il resterais un produit utiliser par une minorité, néanmoins tout compte fait , il reste une révolution et une innovation extraordinaire à ne pas négliger.

*L’histoire du bitcoin s'écrie maintenant on ne sait pas si la réponse sera positive ou négative en tout cas l'avenir lui seul nous le diras...*

#### Table des figures :

[Figure 1: Le Fonctionnement du Blockchain 11](#_Toc9382433)

[Figure 2: les couts de transaction de Bitcoin 19](#_Toc9382434)

[Figure 3: Cours du Bitcoin depuis sa création 25](#_Toc9382435)

[Figure 4: Indexe de consommation du Bitcoin 26](#_Toc9382436)

[Figure 5: la frontière efficiente 28](#_Toc9382437)

[Figure 6: le Risque systématique et le risque spécifique 29](#_Toc9382438)

[Figure 7: : cours de clôture BITCOIN/USD (2015-2016-2017) 30](#_Toc9382439)

[Figure 8: Volume des transactions Bitcoin/USD (2015, 2016, 2017) 31](#_Toc9382440)

[Figure 11: popularité du bitcoin au monde 41](#_Toc9382441)

[Figure 12: Taux d'inflation au Zimbabwe 42](#_Toc9382442)

[Figure 13: le flux monétaire après introduction de M-PESA 43](#_Toc9382443)

[Figure 14: Tendance déflationniste du bitcoin 44](#_Toc9382444)

[Figure 15: Le taux d'inflation historique en U.S 46](#_Toc9382445)

ANNEXE 1: Un point sur le

minage.

Pour assurer l'authenticité et la véracité des blocks créer , les utilisateurs du réseau bitcoin doivent consacrer une partie de la puissance de calcul dont ils disposent à la validation les transactions et à leur enregistrement. Il faut que de nombreux utilisateur fassent ce travail, sinon le système tombe a l'eau. le système élégant de Satoshi NAKAMOTO promets donc une récompense de 12.5 Bitcoin pour chaque block créer, cette promesse de récompense fait office de catalyseur pour les utilisateurs qui en effets seront tenter de consacrer leur ressources pour le minage.

**Le travail du mineur.**

Les règles du jeu sont les suivantes :

- les utilisateurs consacrent leur puissance de calcul (moyennant des ordinateur ) pour mener des opérations, Plus de puissance de calcul signifie plus de chance de gagner les 10 minutes écouler.

- le but est de calculer des valeurs *f*(*x*) un très grand nombre de fois, où *f* est une fonction bien définie et fixée une fois pour toutes ( il s'agit de la fonction hachage SHA256).

- Le nombre moyen de fois qu'il faut effectuer un calcul du type *f*(*x*) pour gagner est régulièrement et automatiquement ajusté pour que gagner exige environ 10 minutes à l'ensemble des mineurs.

La conséquence de ce système est qu'aujourd'hui dans le monde une somme considérable de moyens est consacrée à calculer des *f*(*x*) qui ne servent à rien. La somme dépensée, D à ces calculs est en gros équivalente à celle à gagner, G. En effet, quand D < G de nouveaux mineurs arrivent, car il y a de l'argent facile à gagner, et quand D > G il n'est plus rentable de miner et donc certains mineurs renoncent. On dépense donc plus d'un million de Dollar en moyenne par jour pour calculer des *f*(*x*) qui sont ne servent à rien. Aujourd'hui, on évalue la fonction *f*=SHA256 plus de 240 millions de milliards de fois par seconde.

Bien que les monnaies traditionnelles on aussi des cout de fonctionnement importants: coffres, conception et impression des billets, transports, etc. Il n'en reste pas moins que les centaines de millions qui ont été dépensés pour calculer des *f*(*x*) n'ont pas servi directement à la gestion de la monnaie *Bitcoin*, mais seulement à la désignation des gagnants toutes les 10 minutes parmi ceux qui participent à la gestion de la monnaie. Ce n'est pas pareil, et cela conduit à se poser la question :

- N'y aurait-il pas un système de désignation des gagnants qui n'entraînent pas cette absurde course aux calculs des *f*(*x*) ?

Plusieurs solutions pour remédier à l'absurdité gravissime du minage des *Bitcoins* ont été envisagées et certaines ont été mises en place. Mentionnons trois idées.

**A Mener des calculs utiles**

Plutôt que de multiplier le calcul de *f*(*x*) (pour la fonction SHA256) ce qui ne sert à rien, ne peut-on pas envisager un autre calcul qui serait utile ?

C'est l'idée à la base des [*Primecoin*](http://primecoin.io/). Le calcul de *f* est remplacé par des calculs qui permettent de trouver des chaînes de nombres premiers qui intéressent certains mathématiciens.

Le défaut de cette méthode est que ces chaînes de nombres premiers ne sont pas très utiles, et que les mathématiciens intéressés sont un nombre infime. Grâce à ce minage particulier, la découverte de nouvelles chaînes s'est produite ce qui est un succès de *Primecoin*. Malheureusement, l'impact mathématique de ces découvertes est très faible.

l'idée de base de [*Curecoin*](http://curecoin.net/index.php/fr/) est similaire au *Primecoin*, de façon a diriger la puissance computationnelle des mineurs vers quelque chose d'utile, en effet cette énergie est utilisé pour la résolution de problème biologiques couteux en calcul comme l'alignement des séquences génétiques ou le repliement des protéines. les calculs des mineurs peuvent être derrière la création d'un remède miracle ou une découverte importante dans le domaine de biologie et la médecine.

**B Plutôt que d'engager du calcul, engager de la mémoire.**

l'idée des *Permacoins* est de prendre comme référence non pas la puissance de calcule utiliser pour générer les *f*(*x*), mais de ce référer a la mémoire consacrer par chaque utilisateur a ce but, ce qui signifie que plus un utilisateur consacre de la mémoire plus il gagnera plus. cette mémoire sera utile a tous car il peut être utiliser a plusieurs fins comme par exemple faire de archives, ou des copies de sécurité, maintenir des serveurs...)

**C Limiter l'absurdité du minage.**

 Le protocole du minage exige la désignation d'un mineur gagnant une fois les 10 minutes écoulés, plutôt que de mener la compétition pendant 10 minutes, on peut concevoir un autre protocole qui organise la compétition chaque 10 seconde avec un temps de mort de 9 minute 50 seconde ou rien ne ce passera et le protocole attendra juste le fin du temps "timer" pour démarrer une nouvelle compétition, le fonctionnement interne du minage restera invariable mais ce nouveau protocole permettra d'économiser massivement l'utilisation de l'électricité. Si le nouveau protocole s'avère utile on pourra juste changer 10 seconde par 1 seconde ou encore moins pour encore plus d'économie.

1. Une fiche qui décrit le fonctionnement de Bitcoin. [↑](#footnote-ref-2)
2. <https://www.investopedia.com/terms/b/blockchain.asp> [↑](#footnote-ref-3)
3. <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203455-hash-definition-traduction/> [↑](#footnote-ref-4)
4. Le premier block de bitcoin qui’ a été créé par Nakamoto en 2009 [↑](#footnote-ref-5)
5. C'est dire un pont de confiance entre l'acheteur et le vendeur. [↑](#footnote-ref-6)
6. <http://blogs.worldbank.org/voices/fr/objectif-smart-agir-intelligemment-pour-reduire-le-cout-des-envois-de-fonds> [↑](#footnote-ref-7)
7. Bitcoin la monnaie à ne pas confondre avec Bitcoin le système (la Blockchain). [↑](#footnote-ref-8)
8. Source: The age of Cryptocurrency. [↑](#footnote-ref-9)
9. De l'ouvrage: The age of Cryptocurrency. [↑](#footnote-ref-10)
10. Source: Blockchain blueprint for a new economy (par Melanie Swan) [↑](#footnote-ref-11)
11. <https://www.01net.com/actualites/cinq-raisons-de-vous-eloigner-du-bitcoin-1322611.html> [↑](#footnote-ref-12)
12. <https://fr.coinnewstelegraph.com/bitcoins-volatility-is-still-an-issue/> [↑](#footnote-ref-13)
13. Site internet qui parle des économies dans le monde digital [↑](#footnote-ref-14)
14. Source: The age of Cryptocurrency. [↑](#footnote-ref-15)
15. bitcoin.org [↑](#footnote-ref-16)
16. <https://charts.bitcoin.com/bch/chart/inflation> [↑](#footnote-ref-17)
17. Bank of America Corp. [↑](#footnote-ref-18)
18. Co fondateur du réseau Ethereum. [↑](#footnote-ref-19)
19. [Selon le South China Morning Post](https://www.scmp.com/tech/policy/article/3005334/china-home-worlds-biggest-cryptocurrency-mining-farms-now-wants-ban). [↑](#footnote-ref-20)
20. <https://www.capital.fr/entreprises-marches/la-bundesbank-plaide-pour-une-reglementation-mondiale-du-bitcoin-1265638> [↑](#footnote-ref-21)