Chacun de nous connait intuitivement la monnaie, on l’utilise partout dans notre vie quotidienne

# Une brève histoire de la monnaie

Source : <https://group.bnpparibas/actualite/breve-histoire-monnaie>

## Du troc à la monnaie

Pour les historiens, l’apparition de la monnaie découle de la répartition des tâches au sein d’une société. Bien sûr, la **première forme d’échange a été le troc** : l’éleveur échangeait une bête contre des outils fabriqués par le ferronnier…

Mais ce système pose des problèmes :

Il n’est **pas facile à mettre en œuvre**, quand par exemple un bœuf est difficile à « scinder » en morceaux pour des petits échanges !

Il n’est **pas toujours possible**, quand une personne n’est pas intéressée par les objets proposés en échange de sa propre production.

La **monnaie** résout ces deux problèmes :

**A chaque « objet »** à échanger, on fait correspondre une**certaine quantité de monnaie** ;

La monnaie **peut être scindée en fractions** (comme aujourd’hui les euros divisés en cents).

L’héritage du troc dans notre vocabulaire

La véritable richesse a longtemps été le bétail, qui servait de base aux échanges ou à l’évaluation d’un bien. Et cela se retrouve dans notre vocabulaire. **Pecus, troupeau en latin**, est à l’origine du mot « **pécuniaire** ». Les têtes de bétail servaient à évaluer une propriété (ou la dot d’une fille dans certains pays !), et**caput, tête en latin, a donné le mot « capital »**…

Des premières monnaies aux pièces métalliques

Des objets auquel on leur attribuait une valeur d’échange, et qui étaient faciles à stocker, ont parfois initialement servi de monnaie. Il s’agissait de biens directement utilisables comme **le sel**, qui a servi à payer les légionnaires romains… et a **donné le mot « salaire »**. Ou des objets symboliques comme **les coquillages** (les cauris dans certaines régions d’Afrique)…

Les pièces de monnaies, en métal, sont arrivées ensuite. D’abord en **Anatolie, vers 650 avant JC**. Puis en Grèce antique, chaque cité avait une monnaie frappée à son effigie. Les Romains étendront l’usage de la monnaie à tout leur empire.

**Au IIIème siècle avant JC est créé le premier atelier monétaire**, au Capitole : il était auprès du temple de Junon, **déesse « avertisseuse »** (ses oies ont prévenu d’une attaque des Gaulois), dit**« moneta » en latin**: c’est l’origine du mot monnaie !

## La monnaie, symbole de puissance

**Le denier** (denarius ou pièce de dix) est aussi une invention romaine : cette pièce, **première à porter une valeur inscrite** (un « X » pour 10 en écriture romaine), à la fin du IIIème siècle avant JC.   
Le système monétaire romain se dégrade avec la décadence. Alors Constantin Ier, au IVème siècle après JC, crée **une nouvelle pièce, en or : le solidus** (qui deviendra le « sol », puis le**« sou » en France**).  
Au fil des siècles, **chaque royaume ou empire, pour faciliter les échanges et unifier son territoire, crée sa monnaie** – frappée bien souvent du portrait ou de la devise de son roi ou empereur.   
La monnaie reflétait la **puissance économique et militaire d’une nation, d’où la répression inflexible de la contrefaçon monétaire.**

## La première monnaieinternationale

La première monnaie véritablement internationale n’apparaîtra qu’en 1750 : l’impératrice Marie Thérèse de Habsbourg crée le **thaler**à son effigie, **monnaie rapidement adoptée par les colonies espagnoles et anglaises d’Amérique…**  
Le nom **dollar**est une déformation phonétique de thaler !

## De la valeur à la confiance

Les monnaies métalliques étaient fabriquées en **métal précieux**, et avaient une valeur propre, liée à leur poids.   
En 1685, au Canada, les colons français, confrontés à une pénurie de monnaie, inventent la **monnaie fiduciaire**. Cette monnaie papier (créée sur une carte à jouer portant le sceau et la signature du Gouverneur) n’a pas de valeur intrinsèque : elle est fondée sur la **confiance des possesseurs.**

**En France**, la monnaie de papier apparait au **XVIIIème siècle**, avec des **billets de monnaie ou des assignats**.   
Après la révolution, des **banques d'émission** indépendantes de l'État sont créées. Mais en**1800, la Banque de France** est créée et reçoit en 1803 le **privilège exclusif d'émission de monnaie à Paris**. En **1848**, cette exclusivité est étendue à **l’ensemble du pays**.

# La Confiance: une épée a deux bords tranchants

the bankers created a powerful, new centralized system of trust. With the help of their specialized intermediating services, strangers that previously had no way of trusting each other enough to do business could now do so. In effect, the Medici created a high-powered system of money creation—money being not a physical currency but a system for organizing, expanding, and sharing society’s debts and payments. It made way for an explosion in mercantile trade, which in turn created the wealth and capital that would finance the projects from which great civilizations would grow and conquer the world.

But … by creating this centralized system of trust and then putting themselves in the middle of it, banks became extremely powerful—eventually, too much so. Since strangers could not do business with each other without the banks, the world’s increasingly complex and interconnected economies became utterly dependent on the bankers’ intermediation. The ledgers they kept inside their institutions became the vital means through which societies kept track of the debts and payments that arose among their citizens. Thus the banks created the ultimate rent-seeking business, positioning themselves as fee-charging gatekeepers, managers of the financial traffic that made economies tick. Anyone sitting at the sending or receiving end of that traffic had no choice but to deal with a bank—much as ParisaAhmadi did before the Film Annex changed its payment policy. As this new finance business grew and became more complex, other rent-seeking middlemen installed themselves as specialized providers of intermediated trust—from early bond and securities brokers, to insurance agents, to financial lawyers, to the payment processors and credit-card companies of our modern day. As it currently works, our high-charged global economic system would collapse if these middlemen stopped doing what they do. All of this has simply made the banks at the center of it all even more powerful, so much so that eventually a system that first empowered people has fostered a dangerous dependence upon them. This is what gave rise to the behemoths of Wall Street, which would ultimately take the world to the brink of disaster in 2008.

les banquiers ont créé un nouveau système de confiance centralisé puissant. Avec l’aide de leurs services d’intermédiation spécialisés, les étrangers qui n’avaient jusqu’à présent aucun moyen de se faire suffisamment confiance pour faire des affaires pouvaient désormais le faire. En effet, monnaie n’étant pas une monnaie physique, mais un système permettant d’organiser, d’étendre et de partager les dettes et effectuer des transactions au sein de la société, Qui créait à son tour la richesse et le capital qui financeraient les projets à partir desquels les grandes civilisations se développeraient et conquériraient le monde.

Mais… en créant ce système de confiance centralisé, les banques sont devenues extrêmement puissantes Etant donné que les étrangers ne pourraient pas commercer les uns avec les autres sans les banques, les économies de plus en plus complexes et interconnectées du monde sont devenues totalement dépendantes de l’intermédiation des banquiers. Les grands livres qu’ils gardaient à l’intérieur de leurs institutions devenaient le moyen essentiel par lequel les sociétés gardaient une trace des dettes et des paiements contractés chez leurs citoyens. Ainsi, les banques ont créé l’activité ultime de recherche de rente en se positionnant comme des gardiens payants, des gestionnaires du trafic financier qui a fait tic-tac les économies. Toute personne assise à l’extérieur ou à l’arrière de ce trafic n’avait d’autre choix que de traiter avec une banque, Au fur et à mesure que cette nouvelle activité financière grandissait et devenait de plus en plus complexe, d’autres intermédiaires en quête de rente se sont installés en tant que fournisseurs spécialisés de fiducies intermédiaires - courtiers en obligations, courtiers en valeurs mobilières, agents d’assurance, avocats en droit financier, processeurs de paiement et sociétés de cartes de crédit de notre temps moderne. En l'état actuel des choses, notre système économique mondial très chargé s'effondrerait si ces intermédiaires cessaient de faire ce qu'ils font. Tout cela a simplement rendu les banques au centre encore plus puissantes, à tel point que finalement, un système qui a d'abord responsabilisé les gens a créé une dangereuse dépendance à leur égard. C’est ce qui a donné naissance aux monstres de Wall Street, qui mèneraient finalement le monde au bord du désastre de 2008.

~~La confiance a cree un système de confiance centralise puissant, avec l’aide de leur service d’intermédiationspécialise, les étrangers qui on a l’époque pas une facon de faire confiance entre eux pour faire des affaires, sont maintenant capable de le faire, par conséquence, les banques ontcree un système de création de la monnaie, la monnaie étant pas monnaie physique, mais un system d’organisation, d’expansion et le partage des dettes et des paiement de la société, mais en créant ce système de confiance et être au centre de ce système les banque ont éventuellement devenu extrêment puissantes, que les ménages ne peuvent pas faires des affaires sans l’intervention des banques, la complexité et les économies interconnecte ont devenudépendant a l’intermédiation des banques, toutes les transactions se passent a travers la banques , de la gestions des portefeuilles, les assurances, au avocats financier, jusqu’à contrôleur des paiements, comme il fonctionne maintenant, le système des économies global va se détruire sans l’intermédiation de ces agents, cette dépendance est devenu dangereuse qui a causé la crise de 2008~~

# Pourquoi la Crypto monnaie ?

Ce qui rend la crypto monnaie très doué est l’élimination des parties intermédiaires et en maintenant une infrastructure qui permet des étrangers à s’engager entre eux sans l’intervention des banques centrales grâce a un réseau des ordinateurs autonomes, en créant un system décentralisé de confiance hors contrôle de n’importe quel institution, a son noyau la crypto monnaie est construit autour le principe d’un journal des transactions universel, difficile à frauder , public constamment vérifié par ces ordinateurs puissants, qui opèrent indépendamment l’un des autres, théoriquement ça 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 passe en toute securite. Le potentiel de la technologie en tant que force de transparence et de responsabilité va bien au-delà de l'argent et des paiements, car il permet d'éliminer de nombreuses autres formes d'échange humain les intermédiaires qui contrôlent l'information - lors d'élections, par exemple, où les enthousiastes des cryptomonnaies voient la capacité de mettre fin au vote - gréement. À la base, cette technologie est une forme d'organisation sociale qui promet de détourner le contrôle de l'argent et des informations des puissantes élites et de les transmettre aux personnes à qui elles appartiennent, en les remettant en charge de leurs actifs et de leurs talents. Lancé au plus fort de la crise financière de 2008, Bitcoin offrait une alternative à un système, le système financier existant, qui s'effondrait et menaçait d'entraîner quelques milliards de personnes. En quelques années, tout un mouvement de contre-culture s'est formé autour des crypto-monnaies et a continué de tourner autour d'elles. Sans cette crise qui expose douloureusement les failles du système financier mondial, il est difficile de dire où en seraient les bitcoins aujourd’hui. À mesure que la crise s’atténuera, l’impulsion pour adopter une monnaie electronique s’effacera-t-elle avec elle? Si les citoyens ne font pas confiance à un gouvernement pour défendre leurs intérêts, ils ne font pas confiance à sa monnaie - ou, mieux encore, ils ne font pas confiance au système monétaire autour duquel leur économie est organisée. Donc, quand on leur donne une chance, ils vendront cette monnaie et la fuiront pour quelque chose qu’ils considèrent comme plus fiable, qu’il s’agisse du dollar américain, de l’or ou de toute autre valeur refuge. Lorsque ce dysfonctionnement est enraciné, de telles croyances sont auto-réalisatrices. La perte de valeur de sa monnaie épuise les ressources financières du gouvernement, ce qui laisse l’impression de l’argent comme le seul moyen de payer ses dettes et d’assurer sa survie politique.

the technology’s potential as a force for transparency and accountability goes far beyond money and paymens, as it can strip out information-controlling middlemen from many other forms of human exchange—in elections, for example, where cryptocurrency enthusiasts see the capacity to end vote-rigging. At its core, this technology is a form of social organization that promises to shift the control of money and information away from the powerful elites and deliver it to the people to whom it belongs, putting them back in charge of their assets and talents.

launched in the throes of the 2008 financial crisis, bitcoin offered an alternative to a system—the existing financial system—that was blowing itself up and threatening to take a few billion people down with it. Within a few years, an entire counterculture movement formed around cryptocurrencies, and it has continued to revolve around them. Without that crisis painfully exposing the flaws of the world’s financial system, it’s hard to say where bitcoin would be today. As that crisis recedes, will the impetus to adopt a digital currency recede with it?

If citizens don’t trust a government to represent their interests, they won’t trust its currency—or better put, they won’t trust the monetary system around which their economy is organized. So when given a chance, they will sell that currency and flee it for something they regard as more trustworthy, whether it’s the U.S. dollar, gold, or some other safe haven. When this dysfunction is entrenched, such beliefs are self-fulfilling. The loss of value in its currency depletes the government’s financial resources, which leaves money-printing as the only means to pay its debts and ensure political survival.

# Chapitre 1: Le fonctionnement de Bitcoin

Source: <https://www.investopedia.com/news/how-bitcoin-works/>

Source:<https://bitcoin.org/fr/comment-ca-marche>

Source :<https://www.cryptocompare.com/mining/guides/what-is-proof-of-work/>

## 1.1 La philosophie des crypto-monnaies

Prenons un lecteur de DVD par exemple, vous n'avez pas besoin de connaître son fonctionnement interne pour le comprendre complètement ni de l'utiliser correctement. C’est le même cas de la crypto-monnaie son fonctionnement interne compliqué n'a pas empêché les gens de lui faire confiance.

Nous avons laissé entendre que l’un des grands avantages des crypto-monnaies est qu’elles sont décentralisées. Qu'est-ce que ça veut dire? Cela revient à utiliser un grand livre commun et entièrement public.

Jusqu'à présent, les systèmes monétaires reposaient sur la tenue centralisée des registres, que ce soit par les banques ou par des banques centrales exploitant des grands livres à l'échelle de la grande économie. Cela a apporté efficacité et sécurité aux communautés qui n’avaient aucun autre moyen de faire confiance aux comptes des autres pour savoir qui devait quoi à qui. Cependant, le problème a toujours été que ce modèle conférait trop de pouvoir et un profit excessif à ces archivistes centraux. Le défi consistait à trouver une solution de compromis: un système fiable et décentralisé permettant de garder l’ordre dans la société sans perdre l’efficacité et la sécurité offertes par la centralisation.

Pour créer un système moins centralisé, vous deviez trouver un moyen d'attribuer la tâche de conservation d'archives partagée à un groupe d'individus ou d'institutions connectés par un réseau, et de les inciter à s'acquitter de ces tâches. Vous devez également vous assurer que leur grand livre commun est géré de manière à ce que personne ne puisse l’archiver et le falsifier et y introduire des erreurs que les autres ne remarqueraient pas.

Bitcoin est vraiment juste une liste. La personne A a envoyé X bitcoin à la personne B, qui a envoyé Y bitcoin à la personne C, etc. En faisant le total de ces transactions, tout le monde sait où se trouvent les utilisateurs individuels. Un autre nom pour une blockchain est un "grand livre distribué", qui souligne la différence essentielle entre cette technologie et un document Word bien conservé. La blockchain de Bitcoin est publique. Tout le monde peut le télécharger dans son intégralité ou accéder à un nombre quelconque de sites qui l'analysent. Vous pouvez voir, par exemple, que 15N3yGu3UFHeyUNdzQ5sS3aRFRzu5Ae7EZ a envoyé 0.01718427 bitcoin à 1JHG2qjdk5Khiq7X5xQrr1wfigepJEK3t le 14 août 2017, entre 11h10 et 11h20, mais il en conserve de nouveau. longues chaînes de chiffres et de lettres.

## 1 .2 le Blockchain[[1]](#footnote-2)

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 blockchains 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.

Les bases de la technologie blockchain sont heureusement simples. Toute chaîne de blocs donnée consiste en une chaîne unique de blocs d’informations discrets, classés par ordre chronologique. En principe, ces informations peuvent être n'importe quelle chaîne de 1 et de 0 - courriels, contrats, titres de propriété, certificats de mariage, transactions obligataires - et cette polyvalence a attiré l'attention des gouvernements et des entreprises privées. Dans le cas de Bitcoin, cependant, les informations sont principalement des transactions.

A blockchain is quite literally like a giant spreadsheet for registering all assets, and an accounting system for transacting them on a global scale that can include all forms of assets held by all parties worldwide. Thus, the blockchain can be used for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property); and intangible assets (votes, ideas, reputation, intention, health data, etc.).

#### But what is hash function?

Let’s go little bit into theory. Hash function is a any function, which **arbitrary size data** input, and it is taking output a **data with a fixed size**. The returned value usually called **hash code**, **hash value** or just simply **hashes**. By saying hash should have fixed size, we mean that no matter what the input data will be, after processing the data with hash function, we will always receive data with same fixed size. You may think that you can hash numbers just making the reminder of dividing to 9, or you can hash strings just by taking their first symbol? Let’s go over properties a **hash function** can have.

Depending on which hash algorithm is being used, the process produces a hash of a fixed length. In bitcoin’s case the algorithm is called SHA-256, which delivers a hash of sixty-four characters in length taken from the full range of numbers (0–9) and letters (a–z). To see what one looks like, you can visit any hash generator Web site and write something into the text field. Here’s what [quickhash.com](http://quickhash.com) came back with when we wrote, “The only thing we have to fear is fear itself”:

f72​680​b97​551​fc5​eda​1b3​a33​dda​557​96b​a96​19b​371​fdd​03f​664​09f​2c4​958​c2cb

what is fonctionsfx

* Un petit historique du Bitcoin.

31,Octobre 2008,14:10, temps de new York, les centaines de membres d'une liste de mail appartenant a des experts et des enthousiastes en cryptographie , reçoivent un email de quelqu'un qui ce nomme "Satoshi NAKAMOTO", dans l'email il cite "Je suis entrain de travailler sur un nouveau système de monnaie,pair à pair , sans tierce personne"

Sans d'autres commentaires, il leur envoyé un article d'une longueur d'environ 9 pages ou il explique , avec des illustration, équations, code le système digital de monnaie.

NAKAMOTO avait deja auparavant aquis un domaine qui l'a nomme 'bitcoin.org', mais il savait que pour propulser son systeme au niveau superieur, ce systeme devra utilser par plusieur utilisateur...

Le premier utilisateur du bitcoin fut Satoshi NAKAMOTO lui même, ainsi qu'un volontaire qui faisait partie de liste de mail initiale, Hal FINNEY, a cette epoqueagé de 53 ans ,etait un develpeurcle dans la ste PGP[[2]](#footnote-3), une sociétecreer par Phil ZIMMERMANN[[3]](#footnote-4)...

A partir du 10 janvier 2009, le duo a commencer a travailler ensemble sur un projet intesive, qui a durer deux semaine, ils ont collaborer en partageant des notes à travers des emails, et qui ont petit a petit reussi a rendre le bitcoin operationel.

H

* le grand livre (ledger)

Jusqu'à présent, les systèmes monétaires reposaient sur la tenue centralisée des registres, que ce soit par les banques ou par des banques centrales exploitant des grands livres à l'échelle de la grande économie. Cela a apporté efficacité et sécurité aux communautés qui n’avaient aucun autre moyen de faire confiance aux comptes des autres pour savoir qui devait quoi à qui. Cependant, le problème a toujours été que ce modèle conférait trop de pouvoir et un profit excessif à ces archivistes centraux. Le défi consistait à trouver une solution de compromis: un système fiable et décentralisé permettant de garder l’ordre dans la société sans perdre l’efficacité et la sécurité offertes par la centralisation.

Le mode opératoire du grand livre: Imaginons 4 personnes qui sont tout les quatre des étudiants qui étudient dans la même classe; ces 4 personnes font des transaction entre eux de façon fréquentes et périodiques, un jour un des membres a eu l'idée d'au lieu chaque fois qu'une transaction entre les membres s'engendre pas la peine de la payer directement avec de la monnaie mais on petit utiliser un petit tableau, auquel on écrira tout les transaction qui ce sont écoulé par exemple au cours du mois.

A paye 100 dh B

B paye 50 dh C

C paye 150 dh D

D paye 100dh A

Supposons que a la fin de chaque mois les membre de ce petit groupes , vont chacun payer les sommes qui leur sont respectivement due, imaginons maintenant qui les membres de ce groupe n'échange pas avec le monde extérieur mais effectue des transaction uniquement avec ce groupe, on voit bien si cette hypothèse est vérifier en peut carrément ce passer de la monnaie, on peut juste ce contenter d'écrire les transaction dans ce tableau ...

Mais il existe 2 problèmes lier a l'utilisation du grand livre qui sont:

-on a dit 'A paye 100 dh B ' mais comment peut on vérifier que la transaction a elle réellement était effectuer, donc il faut que la personne B "signe" que effectivement elle a reçus le montant du, on verra par la suite comment les signatures électroniques peuvent elle exister.

- le deuxième problème, et supposant qu'on utilise uniquement le système du grand livre et non la monnaie, par exemple C pourra s'endetter de 1000 dh et juste quitter s'en aller sans jamais payer les gens a qu'il leur doit de l'argent, ce problème trouve solution en l'instauration de limites, qui sont assez simples; tu ne peut dépenser que ce que tu possède déjà en argent, ce système est le même utiliser par les cartes bancaires par exemple....

-3-il existe un problème courant qui est le "double spending" qui signifie payer deux fois ou même plus, c'est a dire payer un ordinateur moyennant 10 bitcoin et ensuite payer un téléphone portable moyennant les "mêmes" bitcoin, il existe une solution a ce problème qui chaque bitcoin a un numéro de série propre a lui, le système fait en sorte que la première opération faite avec les numéros de séries qui corresponde aux bitcoins est valable, tout autre opération moyenne les même bitcoin étant impossible.

Or c'est exactement comme ca que fonctionne le bitcoin. 3 choses essentielle a savoir

-1:tout les ordinateurs sont connecter dans un réseau décentralisé et chaque ordinateur ou utilisateur a ca propre version de son grand livre

2- pour garantir l'authenticité des information dans le grand journal, chaque transaction commence par un identifiant de 64 caractère la date et une signature électronique, code sur une fonction de cryptage connu sous le nom de "hash", qu'on verra par la suite.

3- Le grand livre est un livre publique, ou chaque internaute puisse y accéder sans restriction, toutes les transaction effectuer depuis la création du bitcoin y sont garder.

SOURCES FOR CHAPTER 2 :

Source : <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>

Source: <https://www.lemagit.fr/conseil/Blockchain-bien-comprendre-le-fonctionnement-de-la-Preuve-de-Travail>

Source: <https://www.finyear.com/attachment/648901/>

Source: <https://bitcoin.fr/wp-content/uploads/2016/04/Est-il-juste-de-penser-que-le-Bitcoin-favorise-les-actes-frauduleux-M%C3%A9moire-de-C%C3%A9cile-LAURENT.pdf>

Chapitre 2 : D’où vient le Bitcoin ?

## 2.1 L’origine de bitcoin

En 31 Octobre 2008, des centaines des membres d'une liste de mail appartenant a 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 entrain de travailler sur un nouveau système de monnaie, pair à pair, sans tierce personne"

Sans d'autres commentaires, il leur envoyé un article d'une longueur d'environ 9 pages où il explique[[4]](#footnote-5) , 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 système devrait être utilisé par plusieurs utilisateurs...

Le premier utilisateur du bitcoin fut Satoshi NAKAMOTO lui-même, ainsi qu'un volontaire qui faisait partie de liste de mail initiale, Hal FINNEY, à l'époque âgé de 53 ans, était un développeur clé dans la Ste PGP[[5]](#footnote-6), une société crée par Phil ZIMMERMANN[[6]](#footnote-7)...

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

Contrairement à la monnaie scripturale toute les transactions effectue par le Bitcoin sont enregistrées 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 décentralisé. Il y a des centaines autres monnaie alternative comme Litecoin et Dogecoin, mais Bitcoin occupe plus de 90% de capitalisation de marche.

Bitcoin repose sur un système qui récompense l’énergie utilisé pour sa création, cette opération est appelé le « Mining », ou les utilisateurs offrent le pouvoir de leur ordinateur 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 méninge, 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 Blockchains 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.

## 2.2 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 de 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. *Grosso modo* la Blockchain ce résume ainsi :

1-Des blocks stockent les information relatifs au transactions, par exemple la date, le temps, et le montant dépenser.

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

3-Les blocks ont des codes pour ce distinguer des autres blocks, comme les gens ont des noms pour ce distinguer entre eux, chaque blocks a un code unique appelé "hash" qui lui permet de ce distinguer entre les autres blocks. Supposant par exemple un utilisateur vient d'acheter une pair de chaussure à partir d'un site internet, supposant que directement après le premier achat il a voulut acheter une autre pair, bien que le block serait similaire mais il aura un "hash" différent qui le rendra unique.[[7]](#footnote-8)

|  |
| --- |
| ---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.[[8]](#footnote-9)  La fonction la plus utilisé par les systèmes de sécurité informatique est appelé SHA-256 qui signifie 256 bits, cette est d'une sécurité infaible ( elle n'a jamais réussi a ce faire pénétrer depuis son instauration) et elle est utiliser partout dans le monde pour les dispositifs de sécurité. |

Concernant les adresses et les balances du bloc Genisis[[9]](#footnote-10), 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 dont on parle environ une dizaine de minutes pour bitcoin, la 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 X Le blockchain[[10]](#footnote-11)

|  |
| --- |
| -----public key et secret key (clé publique et clé secrète ).  La cryptographie peut généralement être diviser en deux grande catégorie larges, une clé secrète (symétrique) et une clé publique (asymétrique), dans la cryptographie a base de clés secrète, les utilisateurs utilisent la clé secrète pour encrypter et décrypter les messages. La difficulté principales relève de la difficulté de la distribution sécuriser 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 tout les utilisateur 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 sont distribuer par le syndicat de la résidence, il n'existe en revanche aucun système centralisé pour les clé secrète.  Toute perte de la clés secrète est irréversible et entrainera la perte des fonds dans le compte bitcoin de l'utilisateur. |

## 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](https://blockchainfrance.net/2016/01/28/applications-smart-contracts/) 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](https://blockchainfrance.net/2016/08/17/quels-impacts-de-la-blockchain-sur-les-banques/), [assurance](https://blockchainfrance.net/2016/02/17/assurances-et-blockchain/), [santé et industrie pharmaceutique](https://blockchainfrance.net/2016/03/02/la-blockchain-et-la-sante/), [supplychain](https://blockchainfrance.net/2017/08/23/blockchain-logistique-et-supply-chain-panorama-des-possibilites/) de nombreux secteurs (agroalimentaire, luxe, commerce international, distribution, aéronautique, automobile…), [industrie musicale](https://blockchainfrance.net/2016/12/09/la-blockchain-sauvera-t-elle-lindustrie-musicale/), [énergie](https://blockchainfrance.net/2016/07/07/la-blockchain-pour-lenergie/), [immobilier](https://blockchainfrance.net/2017/02/28/blockchain-quel-avenir-pour-limmobilier/), [vote](https://blockchainfrance.net/2016/02/12/democratie-et-blockchain-le-cas-du-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 interactif géant ou tout le monde peut y accéder, et confirmer l’authenticité des transactions…

## 2. 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, a l'opposé des monnaie traditionnels scripturales qui peuvent être imprimer en cas de besoin, Bitcoin ne peut pas être créer aussi simplement que ca, il doit être "miner" a travers des procéder mathématiques. Bitcoin est un grand livre comptable publique qui contient les transactions passées, et le minage est le processus d'ajouter des nouvelles transaction 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 poser au fondateur de bitcoin comment inciter les utilisateur 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 a résoudre le problèmes le premier, l'algorithme de récompense a fait office de catalyse qui a pousser les utilisateurs lambdas a miner du bitcoin en vue de faire profit, cette approche de SAKAMOTO a fait en sorte que maintenant les mineurs servent a maintenir le réseau Blockchain.

|  |
| --- |
| ------La realiter du minage.  Miner du bitcoin revient a résoudre des problèmes mathématiques, certes cette phrase est a la fois vrai mais a 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 ( code a 256 caractères composé de 0 et 1 ) correspondant a 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 a la loterie, un nombre est générer automatiquement par une machine, le système récompense celui et celle qui a trouver le nombre gagnant.  Pour l'instant la récompense a la création du block est de 12.5 BTC, cette derniere diminuera chaque 4 ans par deux, ainsi en 2020 elle sera de 6.25BTC et ainsi de suite jusqu'a ce que le dernier block sera créer 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 ?

**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 ce 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 des autre money scripturales. Mais a quel prix ?  Ainsi en Octobre 2009, des gens de la communauté en instaurer 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 3 : comparaison entre le système classique et le bit coin.

3.1La viabilité du bitcoin.

Avant de discuter les points faible soit il ou fort du bitcoin et de la crypto monnaie, il partait pertinent de comparer entre les systèmes actuel ou les système ayant déjà prouver leur efficacité a travers l'histoire de l'humanité..

Ainsi pour ce faire on présentera tout d'abord le premier système qui a longtemps dominé le monde et qui fut le 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.

A\*L'or et le bitcoin

on présentera les donnée sous forme de tiré qui avec des perquisition qui sera par la suite regrouper dans un tableau ( figure X )

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

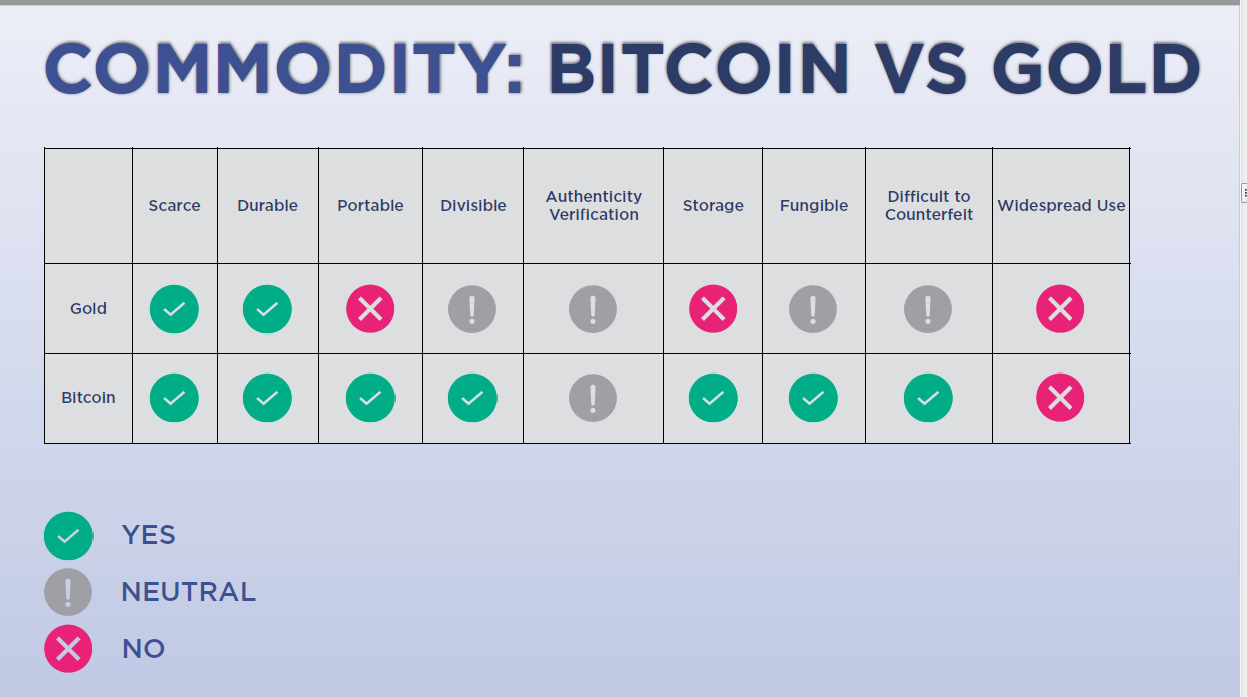
-**La durabilité:** Grace au fait que le bitcoin est décentralisé et distribuer sur le grand journal publique, le bitcoin peut survivre une attaque nucléaire, tandis que l'or ne peut pas, puisque ca température d'évaporation est de 2856 °C, Or il existe l'éventualité que l'or des gouvernement serait dans des grottes bien en dessous de la terre pour assurer la protection contre 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 posséder une connexion internet... ). Tandis que l'or présente l'inconvenant d'être lourd et d'attirer les regards indésirable, donc souci de portabilité et de sécurité. ( un point de pour le bitcoin).

-**La divisibilité**: L'or bien que divisible présente certain problèmes, ca divisibilité reste difficile et couteuse. Alors que le bitcoin, puisque qu'il est composé uniquement de bits il peut être divisible a jusqu'a 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 malfaiteur ainsi a cause de ca grande taille qui nécessite une infrastructure pour le déplacement. Or le bitcoin est très simple a stocker ( le cout d'un disque dur ... ).

-La **Difficulté à falsifier**: l'or étant plus ou moins dur a falsifier mais présente quelque chalenge technique comme par exemple l'or est considéra comme pur si ca densité présente 12% de son poids total, ( donc le falsifier pourra par exemple jouer sur ce ratio ). Le bitcoin de l'autre coté et doté de mécanisme de la Blockchain et du proof of Work qui rendre ce genre de manipulation très très dures voir impossible.



(figure X : le système bitcoin et le système Or )

B\* l'or et le dollar ( la monnaie scriptural ):

**-La rareté:** le bitcoin est plafonner a 21 millions de bitcoin actif dans le monde, le dollar non ( depuis 2008 la date de la crise ) l'émission du dollar a triplé.

-**La durabilité**: Les bitcoins peuvent ce 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 faite qu'elle peut être remplacer facilement sans perte de valeur. Le bitcoin avec l'infrastructure adéquate peut duré a l'éternité.

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

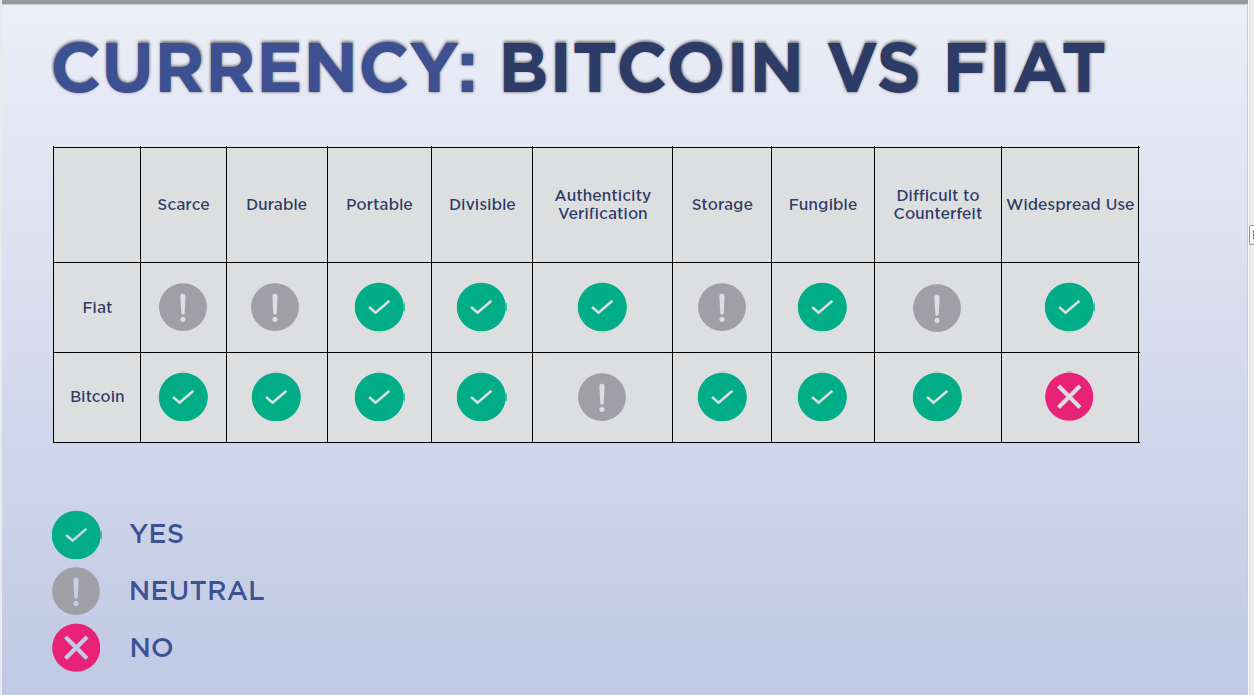
-**La divisibilité:** Chaque bitcoin peut être divisé jusqu'a 100 million de fois, alors que le dollar ne peut être divisé que 100 fois ( le centime).

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

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

-**L'égalité:** Tout les bitcoins sont traiter de la même façons sans discrimination, alors que dans le monde des monnaie scripturale 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 monnaie scripturale ont était falsifier depuis la nuit des temps.



(Figure X : le bitcoin et la monnaie scripturale)

Maintenant et après comparaison du bitcoin avec les deux système classique a 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 parce que qu'il présente toute fois des défauts .

3.2. Avantages du bitcoin:

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

A- Le cout de transaction très faible.

Le premier avantage du bitcoin réside dans son anatomie, c'est a dire le fait qu'il soit un réseau décentralisé, n'ayant guère besoin d'une entité régulatrice qui veille a son bon fonctionnement, n'ayant aussi pas besoin d'une personne tierce pour servir de "bridge"[[11]](#footnote-12) 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 partie prenante de la transaction, cette option constitue un avantage concurrentielle 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 le cout de transaction très hauts, ce cout est en effet le cout de l'intermédiation de la banque, cette marge va directement a la banque et lui sert de rentabiliser son intervention.

Les banques contemporaine étant trop puissante de nos jours, peuvent ce 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 "Fetus" ), 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 au services très pratique des banques...

Le cout des transaction étant variable de banque en banque mais elle sont généralement élever surtout dans les régions a faible concurrences, surtout les banques qui ce 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 a 12 % par transaction, ce qui représente un cout conséquent, considérant le fait que les africains comptes parmi les gens les plus pauvres de la planètes.

En 2009 la banque mondiale a lancé une opération dite: "objectif 5x5"[[12]](#footnote-13). 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'on cas d'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 transaction sont instantanées avec cout d'intermédiation très faible qui oscillent entre 1% et 3%, ce qui séduira forcement les utilisateur aux quartes coin du globe.



(figure X: le cout de transaction de bitcoin [[13]](#footnote-14))

B- Le bitcoin une alternative pour les population 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 a 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 finance relève de la discrimination, puisque ne pas être y inclut signifie l'isolation.

La banque mondial avait publier un article qui stipule que 2.5 Milliard de personnes ne sont pas incluse dans le système financier pour plusieurs raison:

- La non existence d'une infrastructure dans la zone d'habitat des ces gens par exemple pour les pays pauvres ou dans les région éloigner...

- La discrimination envers la femme dans certain pays, ou ces femmes la, 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 une jeune fille pakistanaise nommé Parisa Ahmadi, qui fut une élève brillante et fut empêcher de continuer ses études a 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 Parisa travailla qui payait ses employer en Bitcoin[[14]](#footnote-15), put finalement financer ses études sans l'aide de sa famille et continuer son rêve[[15]](#footnote-16)...

Ainsi tout ces tranche de gens qui ne peuvent pas participer au monde financier, peuvent être inclus grâce a l'implémentation du bitcoin; bien sur l'accès a ce service nécessite un accès a internet, un ordinateur ou a défaut d'un Smartphone, mais avec le développement technologique ces deux composante qui permet 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 ce répercutera sur le niveau de vie de ces gens.

C- problèmes du " Double Spending" et le problèmes des généraux byzantins.

Même sans considérer les multiples utilisation 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 apparus 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 a 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 a résoudre; est le célébrèment connu : "problème des généraux byzantins"[[16]](#footnote-17), 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 a l'offensive, le succès ou la faillite de l'invasion dépendra de la collaboration des généraux, mais deux problème ce présente 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 a la merci de la façon dont le messager l'exprimera et le deuxième problème est que parmi les généraux il puisse exister des traitre donc il n'e ce font pas entièrement confiance.

Le bitcoin résoud le problème du "double Spending" en combinant la fonctionnalité du pair a 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 protocole de la Blockchain et des mineurs.

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

Ce système révolutionnaire bitcoin est le premier a avoir trouvé la solution au du problème du transfert de la propriété digitale, dans le monde d'internet, a un interlocuteur qui peut être inconnu tout en garantissant la sécurité de ce transfert, c'est a 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")

D- le complet anonymat: une épée a 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 a 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 a 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 lobby telle que Facebook et autre société sont soupçonné de la vente d'information de ses utilisateur.

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'a 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 a des pseudonymes, ainsi aucune information en dehors du réseau n'est nécessaire ( telle que le nom , l'adresse ... ). Cette approche a double tranchant garantis au utilisateurs de bitcoin d'être a l'abris 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 a 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 fait 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.

3.3.Inconvenant du bitcoin.

A-retour sur l'anonymat ( "la face cacher 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 a 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 marcher 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 a 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 ca 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 utiliser par des malfrat pour les mauvaises raisons, il présente néanmoins plus d'avantage que d'inconvenant et son potentiel ne devrait pas être gâcher a cause des malfrats.

B- Soucis de sécurité : La fragilité des utilisateur de le réseau bitcoin:

Une autre barrière significative qui freine l'adoption du Bitcoin est la fragilité des utilisateur envers les tentative 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.[[17]](#footnote-18)

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 arnaqueur qui ont réussi a 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, a suite a cette crise simplement "disparu" avec plus de 750 000 bitcoin, laissant les utilisateurs avec des pertes plus ou moins importantes.

Les analyste 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 commit en interne...

Le problème et que quelque soit la cause soit elle interne ou externe ce genre de manipulation continue a 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 toute fois des problèmes très récurant et très grave, 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".

C-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 actifs réels. 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 certaine choses risquée sont bonnes; comme les actifs boursier par exemple, mais le problème ce 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 a 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 dirham 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.[[18]](#footnote-19)

Le Bitcoin étant risqué de ca nature les utilisateur 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 illiquides 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. [[19]](#footnote-20)



(figure X: Cour du Bitcoin depuis ca creation [[20]](#footnote-21))

D- Minage trop coutant.

Le minage du bitcoin une pratique qui nécessitait a 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 vu 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 consommation consiste 0.13% de la consommation globale de l'électricité au monde entier, et d'après Digiconomist[[21]](#footnote-22), ceci classera le bitcoin au 61 rang comme s'il était un pays a part entière.

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

 figure X: indexe de consommation du bitcoin [[22]](#footnote-23)

1. Blockchain: un **grand livre comptable partagé et public** sur lequel repose le réseau Bitcoin en entier. Toutes les transactions confirmées sont incluses dans la chaine de 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. L'intégrité et l'ordre chronologique de la chaine de blocs sont assurés par des moyens [cryptographiques](https://bitcoin.org/fr/vocabulaire#cryptographie) [↑](#footnote-ref-2)
2. [↑](#footnote-ref-3)
3. [↑](#footnote-ref-4)
4. Une fiche qui decris le fonctionnement de Bitcoin. [↑](#footnote-ref-5)
5. [↑](#footnote-ref-6)
6. [↑](#footnote-ref-7)
7. <https://www.investopedia.com/terms/b/blockchain.asp> [↑](#footnote-ref-8)
8. <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203455-hash-definition-traduction/> [↑](#footnote-ref-9)
9. Le premier block de bitcoin qui’ a été créé par Nakamoto en 2009 [↑](#footnote-ref-10)
10. http://blockchain.open.ac.uk/ [↑](#footnote-ref-11)
11. C'est dire un pont de confiance entre l'acheteur et le vendeur. [↑](#footnote-ref-12)
12. <http://blogs.worldbank.org/voices/fr/objectif-smart-agir-intelligemment-pour-reduire-le-cout-des-envois-de-fonds> [↑](#footnote-ref-13)
13. <https://www.ccn.com/bitcoin-transaction-fees-hit-three-year-low-as-lightning-network-segwit-help-btc-scale> [↑](#footnote-ref-14)
14. Bitcoin la monnaie a ne pas confondre avec Bitcoin le système (la Blockchain) [↑](#footnote-ref-15)
15. Source: The age of Cryptocurrency. [↑](#footnote-ref-16)
16. de l'ouvrage: The age of Cryptocurrency. [↑](#footnote-ref-17)
17. Source: Blockchain blueprint for a new economy (par Melanie Swan) [↑](#footnote-ref-18)
18. <https://www.01net.com/actualites/cinq-raisons-de-vous-eloigner-du-bitcoin-1322611.html> [↑](#footnote-ref-19)
19. <https://fr.coinnewstelegraph.com/bitcoins-volatility-is-still-an-issue/> [↑](#footnote-ref-20)
20. <https://www.buybitcoinworldwide.com/fr/cours-bitcoin/> [↑](#footnote-ref-21)
21. site internet qui parle des economies dans le monde digital [↑](#footnote-ref-22)
22. <https://digiconomist.net/bitcoin-energy-consumption> [↑](#footnote-ref-23)