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-1)

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-2), une sociétecreer par Phil ZIMMERMANN[[3]](#footnote-3)...

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-4) , 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 cette époque agé de 53 ans, était un développeur clé dans la Ste PGP[[5]](#footnote-5), une sociétaire par Phil ZIMMERMANN[[6]](#footnote-6)...

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

Contrairement à la monnaie scripturale toute les transactions effectue par la monnaie virtuelle 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 est créé autant qu’une récompense de l’énergie dépensé pour sa création Dite 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 Bitcoins récemment 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 »

Un grand livre comptable partagé et public sur lequel repose le réseau Bitcoin en entier. Toutes les transactions confirmées sont inclus 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.

Concernant les adresses et les balances du bloc Genisis[[7]](#footnote-7), la chaine des blocs est vue comme etant 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, ce qui évitera faire confiance à une tierce personne, ou un intermédiaire par exemple une banque, 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.

## 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, monitorer 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".

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)**

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-1)
2. [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. Une fiche qui decrier le fonctionnement de bitcoin [↑](#footnote-ref-4)
5. [↑](#footnote-ref-5)
6. [↑](#footnote-ref-6)
7. Le premier block de bitcoin qui’ a été créé par Nakamoto en 2009 [↑](#footnote-ref-7)