Introduction

## 1.1 Une brève histoire de la monnaie.

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

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

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

## 1.2 La valeur de la monnaie.

Prenons une feuille de 20 Dirham ou n'importe quelle monnaie... Et observons là profondément. On se posera la question suivante; combien vaut cette feuille ? La première réponse logique est ... Et bien 20 Dirham, c'est sans doute correct mais combien vaut *réellement* cette feuille de 20 Dirham, quelle est la valeur intrinsèque de cette feuille ? Lorsque on remarque bien on trouve que cette feuille n'a aucune valeur en elle-même, malgré ses jolis dessins et ses numéros de séries écrit dans cette dernière, et pourtant cette feuille qui ne contient en elle-même aucune valeur intrinsèque possède réellement une valeur; car je peux acheter l'équivalent de 20 dirham de marchandise avec cette feuille. Alors qui, ou quelle est l'entité qui lui confère ce pouvoir ?

Cette pièce ou cette feuille contient une affirmation de la BAM que je lui dois 20 dirham, de même l'épicier ou le boulanger à qui je vais dépenser cette somme est obligé d'accepter cette pièce comme moyen de paiement, donc en gros et dans un jargon légal, un Dirham constitue un prêt pour le système bancaire , qui établis les droits au futures porteurs de cette pièce de monnaie, la BAM ainsi que tout le circuit monétaires est obligé de reconnaitre la valeur de cette pièce, plus simplement si vous mettez un dirham dans votre compte bancaire, la banque vous doit un dirham.

On peut facilement remarquer que pour que ce système marche il faut avoir des base de confiance dans la statut de la BAM, car si tous les marocains décident du jours au lendemain et en commun accord que le dirham ne vaut plus rien, que peut la BAM faire ? Hormis mettre en place des garanties pour retrouver la confiance de la société; cette approche qui stipule que la monnaie sans la confiance n'est **rien** est fondamentale.

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

## 1.3 Les chartistes et les matérialistes.

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

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

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

## 1.3 Les rôles des banques centrales.

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

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

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

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

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

## 1.4 Le problème du système centrale.

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

cette dépendance bien que auparavant, avait permis à l'humanité de faire des grands pas en avant, a commencé vu le développement technologique à poser pas mal de problèmes et de limitations, citons par exemple :

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

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

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

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

-les périodicités financières, l'alternance entre périodes d'expansion et de crises (2008) issus de notre dépendance totale des banques, cette périodicité ne pourra jamais être éliminée tant qu'on utilise le système central classique.

On remarque d'or et déjà que ce système présente plusieurs failles et limites auquel les économistes en longtemps critiqué, ainsi plusieurs méthodes alternative ont commencés à voir le jour, jusqu'à ce qu'un jour un certain *Satoshi NAKAMOTO* ( d'où on ne connait ni le visage ni l'identité autre que son pseudonyme )publie en 2008 une recherche sur un système qui marrie entre les procédés de cryptage et la monnaie, de LA **crypto-monnaie**; qu'il a décidé de baptiser le **Bitcoin**, bien que la crypto-monnaie existait déjà bien avant cette date ( elle est apparu aussi tôt que les années 70) *Satoshi* a réussi à familiariser le Bitcoin avec le grand public et son système est devenu maintenant LE système standard de référence de la crypto-monnaie, utiliser par des millions d'internautes partout dans le monde.

## 1.5 L’ère du bitcoin et de la crypto-monnaie.

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

Par la création d'une infrastructure qui permet aux étrangers de s’engager entre eux sans l’intervention des banques centrales, grâce à un réseau des ordinateurs autonomes, moyennant l'utilisation d'un système décentralisé de confiance qui ne serait Controller par aucune institution. À son noyau la crypto- monnaie est construit autour d'un système élégant et fort ingénieux:

Le principe d’un journal des transactions universel, difficile à frauder , public et, constamment vérifié par des 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 sécurité.

Le potentiel de la technologie, étant ça transparence et ça responsabilité, va bien au-delà de l'argent et des paiements, car il permet d'éliminer de nombreuses autres formes d'intermédiation qui contrôlent l'information - lors d'élections, par exemple, où les enthousiastes des crypto-monnaies voient la capacité de mettre fin au bridage de vote-. 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 remettants 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...

Le Bitcoin et les crypto-monnaies serait-elle la clé du futur?

Peut-il rendre les banques classiques obsolètes ?

Chapitre 1 : 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[[1]](#footnote-1) , 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[[2]](#footnote-2), une sociétaire par Phil ZIMMERMANN[[3]](#footnote-3)...

À partir du 10 janvier 2009, le duo à commencer à travailler ensemble sur un projet intensive, qui a duré 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[[4]](#footnote-4), 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.

## 2.3 Le potentiel de la blockchain

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

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

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

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

La chaine des blocs est grand livre décentralisé avec l’historique complet des transaction dès la création du ce dernier, la base de donne est partage par toutes les nœuds du système, mis à jours par les mineurs, surveille 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. Une fiche qui décrit le fonctionnement de bitcoin [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. Le premier block de bitcoin qui’ a été créé par Nakamoto en 2009 [↑](#footnote-ref-4)