



جامعة مولود معمري تيزي وزو  
+∘Θ∧∘Πξ+ ΗΓ∞Η∞∧ ∘+ Γϋ∘Γ∞∘  
UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU

# MÉMOIRE

## DE FIN D'ÉTUDE

En vue de l'obtention d'un diplôme de Master en science économique  
Spécialité: Finance et Banque

Thème :

**La monnaie virtuelle : Mécanisme et  
fonctionnement**

Présentées par :

- HADDAD Taous

Encadrée par :

- Mme AMIAR Lila

Devant le jury :

- Mme SIMANSOUR Farida
- Mme FERRAT Massilva

Promotion 2023-2024

## Remerciement

Je remercie Dieu tout puissant de nous avoir donné la force et la Volonté pour mettre au point et achever cette recherche.

Mes remerciements les plus chaleureux et ma gratitude les plus sincères pour ma promotrice **Mme Amiar** de ma avoir encadré. Je tiens également, à lui exprimer ma profonde reconnaissance pour sa disponibilité, le temps précieux qu'elle ma a accordé ainsi, que ses encouragements.

Je remercie également les membres du jury pour l'honneur qu'ils vont me faire en acceptant de juger mon travail.

Mes sincères sentiments vont à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce projet, en particulier à ma chère famille.

## **Dédicaces**

Je tien à dédier cette modeste œuvre :

### **A ma chère mère et à mon cher père,**

En témoignages de ma gratitude et reconnaissance, si grande qu'elle puisse être, pour tous les sacrifices qu'ils ont consentis pour mon bien être et le soutien qu'ils m'ont prodigué tout long de mon éducation. Que Dieu le tout puissant, les préserve et les procure santé et langue  
vie.

### **A mes frères**

Pour leur encouragement et leur bonté qu'ils m'ont accordé, j'exprime ma profonde reconnaissance et mon grand respect. Je vous aime.

### **A tous mes amis,**

Qu'ils trouvent en ce travail, un grand hommage de ma gratitude et en témoignage de l'amitié qui nous unit et de tous les souvenirs passés je vous dédie ce travail et je vous souhaite une  
vie plein du bonheur.

### **A toute ma famille**

TAOUS

## **Liste des Abréviation**

ACCP: Accise Proportionnelle

ACCS: Accise Spécifique

ACPR:Autorité De Contrôle Prudentiel Et De Résolution

ADA :Cardano

BTC: bitcoin

DOT: Polkadot

ETH:Ethereum (crypto-monnaie)

FMI:Fonds Monétaire International

LTC:Litecoin (crypto-monnaie)

POW:Proof of Work

P2P:Peer to peer (pair à pair)

SOL :Solana

US:Union Européenne

USDT:Tether

USDC: Binance coin

XRP : Rippl

# Sommaire

## Sommaire

### Chapitre 01 :L'évolution et la genèse de la crypto-monnaie

Introduction .....	6
Section 01:la technologie blockchain: socle du bitcoin .....	6
<b>Section 02 : Socle du bitcoin : les acteurs du réseau bitcoin</b> .....	16
<b>Section 03 : gouvernance et régulation du bitcoin</b> .....	20
Conclusion .....	27
<b>Chapitre 02 : mécanisme de fonctionnement de bitcoin.</b> .....	<b>Erreur ! Signet non défini.</b>
Introduction .....	29
Section 01:création de nouveau bitcoin .....	29
Section 02 : transfert, transaction et sécurité : validation et inscription .....	37
Section 03 volatilité et valeur de bitcoin : analyses des facteurs .....	41
Conclusion: .....	48
<b>Chapitre 03 : l'illustration d'une transaction économique et commerciale par le Bitcoin: cas de Décathlon</b> .....	<b>Erreur ! Signet non défini.</b>
Introduction : .....	50
Section 01 : Introduction à Décathlon et la crypto-monnaie.....	50
Section 02 : Adoption de Bitcoin comme moyen de paiement par une entreprise en ligne .....	58
Section 03 : étude de cas : Décathlon et son expérience avec le bitcoin .....	59
Conclusion.....	63
Résumé .....	87

# **Introduction générale**

### Introduction générale

Le contrôle des autorités centrales sur la monnaie, la crise des subprimes de 2007<sup>1</sup> ainsi que les crises financières et sociales qui s'ensuivent sur toute la planète furent des éléments déclencheurs en ce qui concerne l'apparition des monnaies numériques chiffrées à l'instar du Bitcoin. En effet, à la suite de 2007, la défiance du système financier mondial et des Etats, qui protègent et tentent de sauver les banques, devient de plus en plus grande. Au point que certains se disent qu'ils vivent dans un monde très opaque où la collusion entre gouvernements et entreprises financières se fait au détriment du peuple. Ces personnes ont pour ambition d'obtenir de plus en plus de transparence et de moins en moins de contrôle de la monnaie au profit de la population mondiale. Selon eux la monnaie fiduciaire est aux mains d'une élite financière et politique se souciant bien peu de l'intérêt général et du bien-être des populations, qu'elles soient dans des pays développés ou dans des pays sous-développés n'ayant pas accès au système bancaire.

L'idéologie principale qui mena à la création de ces monnaies numériques et chiffrées, appelées crypto-monnaies, découle du mouvement libertarien dont l'un des buts est de diminuer le plus possible les pouvoirs de l'Etat.

Le commerce sur internet de nos jours passe essentiellement par les banques qui servent de tiers de confiance. En droit, les tiers de confiance sont les sociétés qui délivrent des certificats de signature, qui fournissent des outils de signature ou encore qui délivrent des infrastructures techniques. Les banques, à travers leur rôle de tiers de confiance, permettent donc le paiement électronique.

Toutefois, les banques ont d'autres activités commerciales et parfois des litiges. Leur marge économique et le coût du risque sont répercutés sur le coût des transactions, car elles sont en situation, parfois, oligopolistiques. En outre même si le système fonctionne, il y a parfois des crises de confiance, comme celle issue de la crise financière de 2007 qui va donner naissance au système Bitcoin et à l'idée de transactions à très faibles coûts pour le bien des utilisateurs, en particulier ceux des pays sous-développés n'ayant pas accès à des banques en raison de coûts prohibitifs<sup>2</sup>.

---

<sup>1</sup> WIKIPEDIA, Crise des subprimes en ligne sur(<http://WWW.Wikipedia.Org>)

<sup>2</sup>Erwan JONCHERES, «Encadrement juridique des monnaie numérique » mémoire présenté à la faculté deDroit de l'Université de Montréal, en vue de l'obtention du grade LL.M, Maitrise en droit des technologies del'information, 2015, p9

Les crypto-monnaies sont créées pour s'échanger la valeur sur internet. Ces nouvelles monnaies sont fondées sur une nouvelle technologie : la blockchain. Elle autorise une gestion décentralisée de la monnaie sans Tiers de confiance à l'opposé des systèmes hiérarchisés et centralisés des monnaies officielles. L'innovation monétaire est encore plus profonde, voir radicale. Les crypto-monnaies sont des monnaies privées, sans cours légal, sans aucun adossement physique ou financier et totalement virtuelles : elles se créent et circulent indépendamment de toute banque et sont détachées de tout compte bancaire. Ce sont des objets nouveaux, sans véritable précédent dans l'histoire. Il existe aujourd'hui plus de 2000 crypto-monnaies pour une capitalisation de marché estimée à plus de 270 milliards de dollars<sup>3</sup>.

Autrement dit, le système bancaire est le résultat du développement du réseau bancaire depuis de nombreuses années, voir depuis plusieurs siècles, organisé, encadré, centralisé, c'est un système bien construit et fort hiérarchisé qui fonctionne grâce à quelques personnes au sommet qui ont la main sur toute la pyramide du système. A l'inverse, le système du Bitcoin a été pensé et développé pour être un système de pair-à-pair, décentralisé, dans lequel chaque participant est garant de la sécurité et du bon fonctionnement de l'ensemble du réseau grâce à une responsabilité partagée.

Le système du Bitcoin jouit ainsi dans le monde de la finance et des institutions bancaires d'une plutôt mauvaise réputation et d'une très grande méfiance, quelque soit le pays. Ainsi Taiwan, la Russie et autres, y compris l'Algérie, ont déclaré illégale l'utilisation du Bitcoin sur leur territoire, aussi plusieurs autres pays, dont la France notamment, ont émis de sérieuses alertes sur les risques associés à son utilisation par l'intermédiaire de leurs banques centrales. Alors que les chiffres de son expansion et du développement du réseau sont cependant assez éloquentes. Si à peine 5000 transactions étaient réalisées en bitcoin par jour en 2011, leur nombre étaient de 50 000 en 2012, pour atteindre 4 millions de BTC par jour, le maximum historique de cet indicateur en Novembre 2017. En Janvier 2019, ce volume atteint 2.7 millions de BTC par jour<sup>4</sup>.

---

<sup>3</sup>Jean-Pierre Landau, Alban Genais, "Les crypto-monnaies" Rapport au ministre de l'Economie et des Finances, du 04/07/2018, en ligne sur (<http://www.ladocumentationfrancaise.fr>)

<sup>4</sup>Ressource Electronique, en ligne sur (<http://www.cryptoactu.com>)

### **Problématique**

Dans ce contexte, notre étude vise à explorer en profondeur le fonctionnement et les mécanismes du Bitcoin. Nous chercherons à répondre à la problématique suivante : **comment s'effectue une transaction a travers le bitcoin ?**

Afin de mieux appréhender ce sujet complexe, nous nous proposons d'examiner les sous-questions suivantes :

1. Quels sont les principaux aspects techniques du Bitcoin et comment fonctionnent-ils ?
2. Quels sont les mécanismes de sécurisation et de validation des transactions dans le cadre du Bitcoin ?
3. Quels sont les défis et les opportunités que présente le Bitcoin en termes de régulation et d'adoption à grande échelle ?

### **Hypothèses**

Pour répondre à ces questions, nous formulons les hypothèses suivantes :

Hypothèse 1 : Le Bitcoin repose sur la technologie de la blockchain, qui permet une gestion décentralisée des transactions.

Hypothèse 2 : Les mécanismes de sécurisation tels que la preuve de travail et la cryptographie sont essentiels pour garantir l'intégrité des transactions dans le cadre du Bitcoin.

Hypothèse 3 : La régulation du Bitcoin constitue un défi majeur en raison de sa nature décentralisée et transnationale, mais elle est nécessaire pour assurer la stabilité et la légitimité du système financier.

### **Choix du sujet**

Le choix d'étudier le Bitcoin comme thème de notre travail s'explique par son importance croissante dans le paysage financier mondial. En tant que spécialistes de la finance, il est essentiel pour nous de comprendre les dynamiques et les implications des crypto monnaies sur l'économie et la société.

De plus, ce choix de sujet répond à un intérêt personnel et professionnel, nous permettant d'approfondir nos connaissances dans un domaine en constante évolution et de contribuer à la production de connaissances nouvelles et pertinentes.

### **Méthodologie de recherche**

Pour explorer le fonctionnement et les mécanismes du Bitcoin, nous adopterons une méthodologie combinant une approche théorique et une approche pratique.

Dans le cadre de notre approche théorique, nous procéderons à une revue bibliographique approfondie des travaux existants sur le sujet, en nous appuyant sur des ouvrages, des articles

et des documents académiques pertinents. Cette analyse nous permettra d'acquérir une compréhension approfondie des concepts et des théories liés au Bitcoin.

Parallèlement, nous mènerons une approche pratique en examinant des cas concrets d'utilisation du Bitcoin par des entreprises y compris Décathlon et en analysant les données disponibles sur son fonctionnement et ses performances. En combinant ces deux approches, nous serons en mesure de fournir une analyse complète et éclairante du sujet.

### **Structure du travail**

Pour répondre à la problématique posée et explorer les différentes dimensions du sujet, notre travail sera structuré en plusieurs parties.

La première partie sera consacrée à la présentation des concepts clés et des théories fondamentales liés au Bitcoin, en mettant en lumière ses origines, ses caractéristiques et ses implications économiques et sociales.

Dans la deuxième partie, nous examinerons de manière détaillée les mécanismes de fonctionnement du Bitcoin, en analysant les technologies sous-jacentes telles que la blockchain et en examinant les processus de validation des transactions.

Enfin, dans la troisième partie, nous aborderons les enjeux et les défis liés à la régulation et à l'adoption du Bitcoin, en mettant en évidence les implications pour le système financier mondial et les politiques publiques.

En suivant cette structure, notre travail visera à fournir une analyse approfondie et éclairante du Bitcoin, de ses mécanismes et de son fonctionnement, tout en offrant des perspectives critiques sur les défis et les opportunités qu'il représente pour l'avenir de la finance.

## **Chapitre 01 :L'évolution et la genèse de la crypto-monnaie**

### **Introduction**

Depuis l'avènement du Bitcoin en 2009, la crypto-monnaie a progressivement émergé comme une force perturbatrice dans le paysage financier mondial. Pour comprendre pleinement cette révolution financière, il est essentiel de remonter à ses origines et d'explorer les fondements de son fonctionnement. Ce chapitre se propose donc d'analyser la genèse de la crypto-monnaie, en se concentrant particulièrement sur le Bitcoin, pionnier et archétype de cette nouvelle ère monétaire.

Ce chapitre sera divisé en trois sections, dans la première section nous allons aborder Les principes fondamentaux de la blockchain, mettant en lumière son architecture décentralisée, sa résistance à la censure et ses mécanismes de consensus qui garantissent la sécurité et l'intégrité du réseau Bitcoin. La deuxième section examinera en détail les différents acteurs qui contribuent à la robustesse et à la résilience du réseau Bitcoin. La troisième et la dernière section explorera les défis auxquels est confronté le Bitcoin en matière de gouvernance, notamment la prise de décision au sein de la communauté et l'évolution du protocole. De plus, elle abordera les perspectives futures de régulation, tant au niveau national qu'international, et les implications de ces réglementations sur l'avenir de la crypto-monnaie.

À travers l'analyse approfondie de ces différents aspects, ce chapitre vise à fournir une base solide pour la compréhension de la genèse de la crypto-monnaie, ainsi qu'à ouvrir la voie à une exploration plus approfondie des développements et des enjeux qui façonnent cet univers en constante évolution.

### **Section 01:la technologie blockchain: socle du bitcoin**

Au cœur de la révolution financière initiée par le Bitcoin se trouve une innovation technologique fondamentale : la blockchain. Conçue comme un registre distribué et sécurisé, la blockchain a révolutionné la manière dont les transactions sont enregistrées, vérifiées et sécurisées dans le monde numérique. Cette section se propose d'explorer en profondeur les principes sous-jacents de la technologie blockchain et son rôle essentiel en tant que socle du Bitcoin.

#### **1. Histoire de la monnaie et évolution vers la crypto monnaie**

Ce qui nous amène à la préhistoire des monnaies chiffrées ou cryptées. En 1982, soit une décennie avant le développement du commerce électronique, dans un papier nommé "Blind Signatures for Untraceable Payments" (Signature aveugle), David Chaum décrit le premier

système chiffré pour permettre des paiements intraquables<sup>5</sup>. Il y décrit comment parvenir à des paiements qui reposent sur la cryptographie et qui empêchent au tiers de savoir qui paye, à quel moment et quel montant. Ce système permettrait aux individus d'avoir des preuves de Paiement et d'avoir à enrayer les moyens de paiement détournés ou volés.

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

En 1996 est créé e-Gold<sup>6</sup>, considéré comme une devise électronique ayant pour but de créer une monnaie mondiale numérique et convertible en or. Cette monnaie permet de faciliter les paiements sur internet. Elle est soupçonnée d'être utilisée dans de nombreuses activités illégales, les créateurs ont donc été mis en examen pour blanchiment d'argent, transferts illégaux, etc. accusation remplacées par l'accusation d'opérer sans licence bancaire locale. Ainsi est née la première monnaie électronique non émise par un Etat et qui pouvait s'échanger contre une réserve de valeur communément acceptée à travers le monde, à savoir l'or.

En 1998, un cypherpunk<sup>7</sup> (voir annexes) du nom Wei Dai écrit le "B-money proposal"<sup>8</sup>. Dans cet article publié sur la liste de diffusion cypherpunk, tout en expliquant ne pas savoir Comment les mettre en place, il décrit deux protocoles de création et gestion monétaires non Traçable sans avoir besoin d'aide extérieure<sup>9</sup>, de tiers de confiance ou autre personne Faillible. Il décrit dans son article un système basé sur la preuve de travail (proof of work)<sup>10</sup>

---

<sup>5</sup>David Chaum, "Blind signatures for Untraceable payments", 1983, en ligne, consulté sur ([www.taler.net](http://www.taler.net)) le 10/04/2024.

<sup>6</sup>Site internet e-Gold en ligne ([www.e-gold.com](http://www.e-gold.com)) consulté le 10/04/2024.

<sup>7</sup>Cypherpunks (mot-valise composé à partir des mots anglais cipher : chiffrement, et punk sur le modèle de cyberpunk) forment un groupe informel de personnes intéressées par la cryptographie. Leur objectif est d'assurer le respect de la vie privée par l'utilisation proactive de la cryptographie

<sup>8</sup>B-money : était l'une des premières propositions de Wei Dai pour un système de paiement électronique anonyme et distribué. En ligne sur ([en.bitcoin.it](http://en.bitcoin.it)) consulté le 10/04/2024.

<sup>9</sup><http://www.bitcoin.org> consulté le 10/04/2024.

<sup>10</sup><sup>1010</sup> Preuve de travail ou en anglais "proof of work", est un des concepts les plus importants en ce qui concerne le chiffrement, et plus particulièrement celui des monnaies numériques. On demande à l'ordinateur d'effectuer

Comme mode de création monétaire, en s'appuyant sur l'hypothèse que tous les participants seraient aussi les gardiens du système.

### **2. Définition et concepts clé :**

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

#### **2.1. Définition de la cryptographie**

La cryptographie : un rempart inviolable pour la protection de l'information sensible

Dans le domaine de la sécurité de l'information, la cryptographie se présente comme une discipline cruciale visant à protéger la confidentialité, l'intégrité et l'authenticité des données. En s'appuyant sur des algorithmes mathématiques robustes et des clés secrètes, elle offre un rempart solide contre les intrusions malveillantes et les divulgations indésirables.

Étymologiquement dérivé des mots grecs anciens "kryptos" (caché) et "graphein" (écrire), le terme "cryptographie" reflète parfaitement son essence : dissimuler le contenu d'un message pour le soustraire aux regards indiscrets.

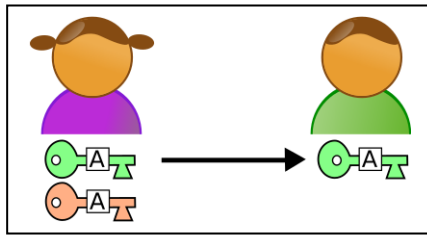
Au cœur de la cryptographie classique, ou symétrique, réside le concept de clé secrète. Cette clé sert de catalyseur pour transformer un message intelligible, désigné sous le nom de "texte clair", en un message incompréhensible pour tout individu non détenteur de la clé correspondante, nommé "texte chiffré". La force de la cryptographie symétrique réside dans l'utilisation d'une seule clé pour la double opération de chiffrement et de déchiffrement, symbolisée par une boîte à outils dont l'accès est exclusivement réservé aux parties prenantes légitimes.

L'application de la cryptographie s'étend à une multitude de domaines où la protection de l'information revêt une importance capitale. On la retrouve ainsi dans les transactions bancaires en ligne, les dossiers médicaux confidentiels, les communications gouvernementales sensibles et bien d'autres secteurs critiques.

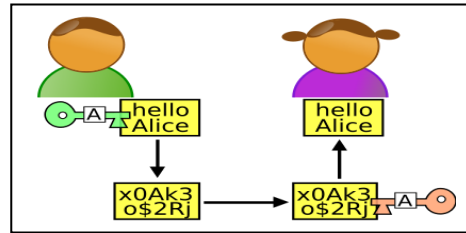
---

une tâche qui nécessite de la puissance de calcul afin de créer la preuve de travail (Son fonctionnement et son utilité seront expliqués par la suite).

Figure 01 : Le Principe De La Cryptographie Asymétrique<sup>11</sup>



1re étape : Alice génère deux clés: Sa clé publique (verte) qu'elle envoie à Bob et sa clé privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



2e et 3e étapes : Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

La cryptographie asymétrique : un atout majeur pour la sécurité des données

La cryptographie asymétrique se distingue par son système de double clé : publique et privée.

La clé publique, partageable, permet de chiffrer les messages, tandis que la clé privée, secrète, permet de les déchiffrer. Ce système offre deux avantages majeurs :

Confidentialité des messages: Seul le destinataire peut lire le message chiffré avec sa clé privée.

Authentification de l'expéditeur: Le destinataire peut vérifier l'identité de l'expéditeur en chiffrant un message avec sa clé publique.

Autre avantage : celui de l'authenticité de l'expéditeur, qui utilise la clé publique du Destinataire pour coder un message que seul le destinataire pourra décoder, car lui seul Possède la clé privée correspondant à sa clé publique<sup>12</sup>.

### 2.2.Définition de la crypto monnaie

Les crypto monnaies sont des monnaies numériques qui n'existent que sous forme électronique. Elles offrent un moyen de paiement universel pour les biens, les services et les investissements, sans avoir recours aux systèmes bancaires traditionnels, bouleversant ainsi radicalement le fonctionnement de la finance<sup>13</sup>.

<sup>11</sup>Fr.wikipedia.org)

<sup>12</sup>Enée Bussac, "Bitcoin, Ether & Cie : guide pratique pour comprendre, anticipé et investir.", Dunod, 2018, P.9.

<sup>13</sup>[https://n26.com/fr-fr/blog/definition-](https://n26.com/fr-fr/blog/definition-cryptomonnaie#:~:text=Les%20cryptomonnaies%20sont%20des%20monnaies,le%20fonctionnement%20de%20la%20finance.)

[cryptomonnaie#:~:text=Les%20cryptomonnaies%20sont%20des%20monnaies,le%20fonctionnement%20de%20la%20finance.](https://n26.com/fr-fr/blog/definition-cryptomonnaie#:~:text=Les%20cryptomonnaies%20sont%20des%20monnaies,le%20fonctionnement%20de%20la%20finance.)

Une crypto-monnaie, ou monnaie cryptographique, monnaie numérique, monnaie digitale ou encore monnaie virtuelle (dénomination à priori péjorative) est une monnaie dont le fonctionnement et la sécurité sont fondés sur la cryptographie<sup>14</sup>. Pour être échangé sur internet, et qui, pour certaines crypto-monnaies, sont gérées de manière décentralisée<sup>15</sup>,

### **2.2.1. Les caractéristiques de la crypto-monnaies :**

**Numériques et sans autorité centrale** : contrairement aux monnaies traditionnelles, elles existent uniquement sous forme numérique et ne sont garanties par aucune institution.

**Sécurisées par la cryptographie** : la cryptographie assure la sécurité des transactions et protège l'intégrité de la monnaie.

**Décentralisées (pour la plupart)** : fonctionnement réparti entre tous les participants, sans autorité centrale, pour plus de transparence et de résistance à la censure. Les transactions sont décidées et validées par un consensus<sup>16</sup>.beaucoup, mais pas toutes, sont adossées à la technologie Blockchain<sup>17</sup>.

**Dématérialisation et absence d'ancrage territorial** : Les crypto-monnaies n'existent qu'au format numérique et ne sont liées à aucune zone géographique ou juridiction spécifique.

**Variété et distinction** : Les crypto-monnaies se différencient les unes des autres par leur capitalisation boursière (déterminée par les mécanismes de l'offre et de la demande et sujette à une forte volatilité), leur rythme d'émission (nouvelles unités créées selon un calendrier prédéfini), le fonctionnement de leur technologie blockchain sous-jacente et les objectifs spécifiques de chaque projet.

**Fonctionnement sur un réseau décentralisé** : Chaque crypto-monnaie opère sur un réseau informatique distribué, sans autorité centrale de gestion. Cette architecture permet une transparence accrue et une résistance à la censure.

**Identification unique** : Chaque crypto-monnaie est identifiée sur le réseau par un symbole unique, généralement composé de trois lettres majuscules (par exemple, BTC pour le Bitcoin).

La crypto-monnaie est couplée à un système de paiement qui permet de régler des

---

<sup>14</sup>Enée Bussac, Op.cit.p10

<sup>15</sup>Jean-Pierre Landau, Alban Genais, Op.cit.

<sup>16</sup>A revoir par la suite.

<sup>17</sup>74 Élément détaillé dans la section suivante.

Transactions de pair à pair (Peer-to-Peer)<sup>18</sup>. Elle a un fonctionnement décentralisé et est régie Par un protocole initial qui stipule le rythme et les règles de création et d'attribution de Nouveaux coins<sup>19</sup>.

### **Limites d'émission et protection contre la contrefaçon des crypto-monnaies :**

- Offre limitée et contrôlée :

Le nombre total d'unités est défini et ne peut être modifié sans un large consensus. La circulation est transparente et consultable en temps réel.

- Inviolabilité garantie :

La technologie blockchain et la cryptographie de pointe rendent la contrefaçon et la duplication d'unités extrêmement difficiles, voire impossibles.

### **2.2.2. L'innovation monétaire**

Les crypto-monnaies : une innovation monétaire radicale, rupture avec les monnaies traditionnelles, Contrairement aux monnaies bancaires, les crypto-monnaies n'ont aucune valeur intrinsèque et existent uniquement sous forme numérique. Elles se distinguent des monnaies existantes par des caractéristiques fondamentales opposées :

- Création et circulation indépendantes : Elles opèrent en dehors du système bancaire traditionnel et ne sont liées à aucun compte bancaire.
- Absence de lien avec des créances : Elles ne représentent aucune créance sur une entité physique ou morale.
- Monnaie privée sans cours légal : Elles ne bénéficient d'aucun soutien public, direct ou indirect, et n'ont pas de cours légal.
- Expérience monétaire inédite : Au-delà de l'innovation technologique et de leur ressemblance apparente aux monnaies électroniques, les crypto-monnaies incarnent une expérience monétaire sans précédent. Si les formes de monnaie ont évolué tout au long de l'histoire sous l'influence de la technologie, des institutions et des conventions sociales, toutes les monnaies qui se sont développées et imposées dans les économies capitalistes possédaient au moins l'une des caractéristiques suivantes :
  - Valeur intrinsèque : Monnaies et pièces en métal précieux.

---

<sup>18</sup>Peer-to-Peer ou pair à pair est l'un des principes de fonctionnement des crypto-monnaies (principe expliqué dans les sections qui suivent.)

<sup>19</sup> Un coin (littéralement pièce de monnaie) est une monnaie cryptographique, toujours lié à une plateforme ou système où cette monnaie sert de moyen de paiement, le bitcoin par exemple.

- Contrepartie d'un actif : Étalon-or, où la valeur est garantie par un actif physique ou financier.
- Soutien public : Cours légal et refinancement par la banque centrale.
- Absence de ces attributs fondamentaux : Les crypto-monnaies ne possèdent aucun de ces trois attributs, ce qui les classe comme des objets monétaires totalement nouveaux. Cette singularité justifie leur qualification de "virtuelles".

### **2.2.3. Les principales crypto monnaie existantes**

- a. bitcoin(BTC) : la première et la plus connue des crypto monnaies, lancée en 2009.elle se caractérisé par sa décentralisations sécurité et sa transparence.
- b. eutherland(ETH) : la deuxième plus grande crypto monnaie en termes de capitalisation boursière. Elle est connue pour sa plateforme block chaine programmable, qui permet de créer des applications décentralisées (dApps)
- c. Tether(USDT): une crypto monnaie stable liée au dollar americain.elle vise à offrir un prix stable et est souvent utilisée comme monnaie de change pour d'autre crypto monnaies.
- d. Binance coin(USDC) : une autre crypto monnaie stable liée au dollar americaine.elle est soutenue par un consortium d'entreprise, dont circle coibase.
- e. USD Coin(USDC) : Une autre crypto monnaie stable liée au dollar americain.Elle est soutenue par un consortium d'entreprises, dont circle et coinbase.
- f. Solana(SOL) : Une blockchain connue pour sa vitesse et sa scalabilité.elle vise à rivaliser avec Eutherland en tant que plateforme pour les d'Apps.
- g. Cardano(ADA) : Une blockchain basée sur la recherche académique qui vise à être plus durable et évolutive que les autres blockhains.
- h. Dogecoin (DOGE) : une crypto monnaie créée comme une blague, mais qui a gagne en popularité grâce au soutien de personnalités comme Elon Musk.
- i. Polkadot(DOT) : Une blockchain qui permet de connecter différentes block chaine entre elles. Elle vise à créer un écosystème interopérable pour les crypto monnaie.
- j. Ripple(XRP) : Une crypto monnaie conçue pour les transactions internationales rapides et peu couteuses. Elle est souvent utilisée par les institutions financières.

### **2.2.4. Les principes technologies des crypto monnaie**

Nakamoto a créé le Bitcoin pour résoudre le problème des transactions en double. Il a conçu un système garantissant qu'une somme d'argent ne puisse être présente qu'à un seul endroit à la fois, à un moment donné.

Nakamoto a résolu ce problème en créant un registre chronologique similaire à un livre de comptes, où chaque opération est enregistrée dans un bloc numéroté séquentiellement. Cette série de blocs forme la Blockchain, où chaque bloc contient le hash du bloc précédent, renforçant ainsi la sécurité. Chaque transaction est unique grâce à son numéro de séquence, les clés publiques utilisées, son propre hash, et le hash de la transaction précédente. Telle est la blockchain. Un livre de compte qui contient à tout moment l'historique complet de Toutes les transactions précédentes depuis la toute première<sup>20</sup>

#### **2.2.4.1. La blockchain et son fonctionnement**

##### **2.2.4.1.1. Définition de la blockchain**

La blockchain est une technologie équivalente à Internet qui permet le stockage décentralisé et sécurisé de données numériques à faible coût. Elle agit comme un registre inaltérable contenant l'historique des transactions entre les utilisateurs du réseau. La blockchain peut être comparé à un grand registre décentralisé accessible en ligne et partagé par un grand nombre d'utilisateur<sup>21</sup>

##### **2.2.4.1.2. Le fonctionnement de la blockchain**

La blockchain, à l'échelle d'Internet, offre un stockage décentralisé et sécurisé de données numériques à moindre coût. Elle fonctionne comme un registre immuable qui enregistre toutes les transactions entre les utilisateurs du réseau. Ainsi un utilisateur ne peut se servir de ses bitcoins qu'auprès d'un seul destinataire correspondant à une seule transaction donnée<sup>22</sup>. C'est le réseau Peer-to-Peer (P2P) qui rend la blockchain infalsifiable.

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

---

<sup>20</sup>Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P144.

<sup>21</sup>Gilles Quoistiaux, "Bitcoin et crypto-monnaie", Edition MARGADA, Bruxelles, 2019, P19.

<sup>22</sup> Blog les Echos.fr, "comprendre la blockchain en 5 points" publié le 19/01/2016, consulté sur ([lesechos.fr](http://lesechos.fr)) le 20/04/2024.

Le Peer-to-Peer (P2P) est un réseau où chaque ordinateur a des droits égaux, permettant ainsi la connexion et la collaboration entre plusieurs utilisateurs sur un pied d'égalité. C'est-à-dire d'amener les internautes connectés entre eux à s'échanger leurs propres fichiers<sup>23</sup>.

Le pair à pair est un modèle d'échange où chaque entité du réseau est à la fois client et serveur, contrairement au modèle client/serveur. Dans un réseau P2P, les nœuds interconnectés (pairs) partagent les ressources entre eux sans avoir recours à un système administratif centralisé<sup>24</sup>.

- Le minage et le consensus dans les blockchains Proof of Work (PoW) :

Le minage est un processus crucial dans les blockchains PoW, permettant de valider les transactions et de sécuriser le réseau. Il ne s'agit pas de créer de la crypto-monnaie, mais plutôt de contribuer au bon fonctionnement de la blockchain.

- Les utilisateurs effectuent des transactions :

Ces transactions sont regroupées dans des blocs. Les mineurs (des ordinateurs puissants) concourent pour résoudre des problèmes mathématiques complexes.

Le premier mineur à résoudre un problème obtient le droit d'ajouter le bloc de transactions à la blockchain. Ce mineur est récompensé par de la crypto monnaie. Tous les nœuds du réseau vérifient le bloc et l'ajoutent à leur copie de la blockchain.

Le consensus est la manière dont tous les nœuds du réseau s'accordent sur l'état de la blockchain. Dans le cas du PoW, le consensus est atteint lorsque la majorité des nœuds acceptent le bloc ajouté par le mineur qui a résolu le problème mathématique.

- La preuve de travail

Dans les blockchains utilisant le mécanisme de preuve de travail (PoW), les mineurs jouent un rôle crucial pour valider les transactions et sécuriser le réseau. Pour ce faire, ils doivent résoudre un problème mathématique complexe, ce qui implique une dépense importante en puissance de calcul.

- Le processus en détail :

Un mineur reçoit une transaction non encore validée. Il regroupe cette transaction avec d'autres transactions en attente dans un bloc.

Le mineur applique une fonction de hachage cryptographique (SHA-256) au bloc, générant un identifiant unique appelé "hash".

---

<sup>23</sup>Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P144.

<sup>24</sup>101 WIKIPEDIA, Op.cit consulté le 20/04/2024.

Le but du mineur est de trouver un hash commençant par un nombre spécifique de zéros. Cela nécessite d'essayer de nombreuses combinaisons différentes jusqu'à trouver la solution. Une fois le hash correct trouvé, le mineur a réalisé une "preuve de travail" valide. Le mineur diffuse le bloc contenant la preuve de travail au reste du réseau. Tous les nœuds du réseau vérifient la validité du bloc et de la preuve de travail. Si la preuve de travail est acceptée, le bloc est ajouté à la blockchain, et les transactions qu'il contient sont considérées comme validées. Le mineur qui a trouvé la preuve de travail reçoit une récompense, généralement sous forme de nouvelles unités de la crypto-monnaie. Ils récoltent aussi une commission, soit un pourcentage minime de la transaction qu'il a validée<sup>25</sup>.

- Le smart contract Littéralement

"Contract intelligent".

Un smart contract est un concept créé en 1993 par Nick Szabo<sup>26</sup>. Un concept né avec l'environnement Ethereum<sup>27</sup>, qui intègre dans sa boîte à outils un langage de programmation, solidity, dédié à l'écriture de ces contrats intelligents et à leur inscription sur la blockchain<sup>28</sup>.

Les contrats intelligents sont des protocoles informatiques qui permettent de vérifier et d'exécuter en temps réel un contrat juridique ou financier, ou tout type d'accord que plusieurs contreparties peuvent codifier avec peu, ou pas du tout, d'interventions humaines. Un smart contract est un contrat dit auto-exécutant. Il implique deux points fondamentaux :

Grâce à la blockchain et à son réseau de participants, le contrat pourra s'exécuter de manière automatique.

En cas de litige, les participants à la blockchain serviront d'arbitres pour la résolution du conflit.

---

<sup>25</sup>Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P148.

<sup>26</sup>Enée Bussac, Op.cit, P52

<sup>27</sup> Ethereum, créée par Vitalik Buterin aidé par Nick Szabo, a constitué la 1ère évolution majeure des crypto-monnaies. Il est ainsi considéré que le Bitcoin représente la 1ère génération de crypto-monnaie et que l'Ethereum et les monnaies basées sur lui ont constitué la seconde génération.

<sup>28</sup>Daniel Ichbiah, Jean-Martial Lefranc, Op.cit.P156.

### 2.2.4.1.3. La relation de bitcoin et la blockchain

Le bitcoin et la blockchain sont étroitement liés. En fait, la blockchain <chaîne de bloc> est une technologie qui permet de stocker des données numériques de manière décentralisée et sécurisée. C'est une sorte de registre en ligne qui contient tous les échanges effectués entre utilisateurs. Mis à jour en temps réel, ce registre est réputé infalsifiable grâce à un système cryptographique<sup>2</sup>.

Chaque transaction bitcoin est regroupée avec d'autres transactions dans un bloc, qui est ensuite ajouté à la chaîne de blocs existante. Chaque bloc contient un ensemble de données cryptographiques qui garantissent l'intégrité et la sécurité des transactions enregistrées.

La blockchain bitcoin est gérée par un réseau décentralisé de nœuds informatiques, appelés mineurs, qui vérifient et valident les transactions. Une fois qu'une transaction est validée, elle devient immuable et ne peut pas être modifiée.

## Section 02 : Socle du bitcoin : les acteurs du réseau bitcoin

Le socle du Bitcoin repose sur un écosystème dynamique d'acteurs qui soutiennent et maintiennent le réseau Bitcoin. Ces acteurs jouent des rôles variés, allant des mineurs qui sécurisent les transactions à travers la preuve de travail, aux développeurs qui travaillent sur l'amélioration du protocole, en passant par les utilisateurs qui effectuent des transactions et soutiennent l'adoption croissante de la crypto monnaie. Dans cette section, nous explorerons les différents acteurs clés du réseau Bitcoin, leur importance et leur contribution à l'évolution de cette révolution monétaire décentralisée.

### 1. Acteurs de réseaux bitcoin

Les acteurs de réseaux Bitcoin représentent les différentes entités qui participent au fonctionnement du réseau. Ils jouent des rôles clés dans le système Bitcoin en contribuant à différentes facettes de son fonctionnement. Parmi ces acteurs figurent les mineurs, les nœuds et les utilisateurs. Chacun de ces acteurs a un rôle spécifique qui contribue à la sécurité, la validation et la transmission des transactions sur le réseau Bitcoin.

#### 1.1. Les mineurs

##### 1.1.1. Définition<sup>29</sup>

Les mineurs sont des acteurs essentiels du réseau Bitcoin. Ils sont responsables de l'extraction de nouveaux blocs de transactions et de la sécurisation du réseau en validant les transactions. Les mineurs utilisent des ordinateurs puissants pour résoudre des problèmes mathématiques complexes afin de trouver la solution permettant de créer un nouveau bloc dans la blockchain.

---

<sup>29</sup><http://www.Bitpanda.com>



Tableau N 01 : La puissance de calcul du réseau se mesure actuellement en ExaHash par seconde (EH/s).

<b>Unité</b>	<b>Hash</b>	<b>Hashs par seconde</b>
H/s (Hash)	1	Un
kH/s (KiloHash)	1,000	Mille
MH/s (MegaHash)	1, 000,000	Un million
GH/s (GigaHash)	1, 000, 000,000	Un milliard
TH/s (TeraHash)	1, 000, 000, 000,000	Un billion (mille milliards)
PH/s (PetaHash)	1, 000, 000, 000, 000,000	Un billiard (un million de milliards)
<b>EH/s (ExaHash)</b>	<b>1, 000, 000, 000, 000, 000,000</b>	<b>Un trillion (un milliard de milliards)</b>

### 2.1. Les nœuds

#### 2.1.1. Définition<sup>31</sup>

Les nœuds sont des ordinateurs connectés au réseau Bitcoin qui stockent et transmettent les données du réseau. Ils assurent la diffusion des transactions et des blocs aux autres nœuds, permettant ainsi la vérification et la propagation de l'information sur le réseau. Les nœuds jouent un rôle crucial dans la décentralisation du réseau Bitcoin, en permettant à chaque utilisateur de vérifier l'intégrité des transactions et de participer à la gouvernance du réseau en exprimant leurs préférences sur les règles du système.

Les fonctions

Un nœud te donne le contrôle sur le réseau Bitcoin donc tu as accès à la MemPool de ton nœud (l'intégralité des transactions en attente de validation), tu as ton propre block explorer (tu peux regarder toutes les transactions sans faire confiance). Tu vas connecter ton

---

<sup>31</sup> <https://www.coinbase.com>

portefeuille à ton nœud, donc ton Trezor, Blue Wallet ou autre. Ainsi, lorsque ton wallet envoie ou reçoit de l'argent, c'est ton petit serveur perso (nœud) qui vérifie que ce sont bien des bitcoins. Enfin, tu pourras voter pour les future fork, hard ou soft par le consensus que tu fais tourner.

Probablement tout le monde, mais si l'on doit être plus réaliste : les marchands ou commerces qui doivent recevoir beaucoup de transactions. Les gens envieux de garder leur vie privée. Les plèbes qui ne veulent ni faire confiance ni vérifier. Les gens fortunés qui ont beaucoup de bitcoins, les régulateurs, les échanges, les mineurs, et les tech savy.

### **2.1.2. Le coût des nœuds<sup>32</sup>**

Un nœud est uniquement un logiciel et une base de données (aujourd'hui de 280G). Tu peux donc, toi aussi, avoir un nœud sur ton ordinateur (comme Bitcoin core). Tu peux l'héberger sur un Cloud type lunanode ou AWS, OVH. Finalement, la meilleure solution est un boîtier externe à côté de ton routeur de type Rapserrri Pi 4 5 solution Umbrel).

Le coût d'un nœud va donc de 0€ sur ton ordi, à 12€ par mois sur un Cloud à environ 200-300€ de matériel sur un Pi puis proche de 5€ par an en énergie.

Les nœuds sont la grande différence avec tous les autres projets : faciles, accessibles et disponibles à faible coût pour la masse. Sur le Discord, nous avons un salon dédié aux nœuds si besoin.

### **2.1.3. Les nouvelles transactions**

Chaque nœud regroupe les nouvelles transactions dans un bloc, travaille à la résolution de la preuve de travail sur son bloc, Quand un nœud trouve une preuve de travail, il diffuse ce bloc à tous les nœuds, ils n'acceptent le bloc que si toutes les transactions qu'il contient sont valides et n'ont pas déjà été dépensées, ils expriment l'acceptation du bloc en travaillant sur un nouveau bloc dans la chaîne, ce nouveau bloc ayant comme empreinte précédente celle du bloc accepté et considèrent toujours la chaîne la plus longue comme étant la chaîne légitime, et travaillent à étendre celle-ci. Si deux nœuds diffusent deux versions différentes du bloc suivant simultanément, certains des nœuds vont recevoir l'une ou l'autre en premier. Dans cette situation, chacun travaille sur le bloc reçu en premier, mais conserve l'autre branche au cas où celle-ci devienne la plus longue. Cette liaison sera rompue quand la preuve de travail suivante sera trouvée et qu'une branche deviendra plus longue que l'autre ; les nœuds qui travaillaient alors sur l'autre branche changeront pour la plus longue.

---

<sup>32</sup> <https://.bitpanda.com>

Les diffusions de nouvelles transactions n'ont pas besoin d'atteindre tous les nœuds. A partir du moment où elles atteignent suffisamment de nœuds, elles se retrouveront dans un bloc en peu de temps. Les diffusions des blocs tolèrent la perte de messages. Si un nœud ne reçoit pas un bloc, il le demandera lors de la réception du bloc suivant, lorsqu'il réalisera qu'il lui en manque un

Je le répète encore ici : un nœud Bitcoin ne rapporte pas d'argent, il n'y a pas de staking, air drop ou minage. C'est un outil en plus de votre portefeuille, pour être encore plus souverain. Si vous cherchez à utiliser un nœud Lightning qui consiste à bloquer des Satoshi dans des canaux de liquidités alors c'est différent. Il n'y a donc pas BTC minimum.

### **2.1.4. Miner avec un nœud<sup>33</sup>**

Non, mais tous les mineurs doivent avoir un nœud pour communiquer avec le réseau, récupérer les transactions, former les blocs, confirmer les transactions, propager les blocs.

Les nœuds sont l'élément central de Bitcoin, ce sont ceux qui dirigent le réseau et les gardiens du consensus. Sans les nœuds il n'y a pas de décentralisation.

### **3.1. Les utilisateurs**

#### **3.1.1. Définition**

Les utilisateurs sont les individus qui interagissent avec le réseau Bitcoin en envoyant, recevant et en utilisant des bitcoins. Ils utilisent des portefeuilles électroniques qui leur donnent accès à une adresse Bitcoin unique, à partir de laquelle ils peuvent effectuer des transactions. Les utilisateurs peuvent envoyer des bitcoins à d'autres utilisateurs à travers le réseau, acheter des biens et des services auprès de commerçants qui acceptent Bitcoin comme mode de paiement, ou encore investir dans cette crypto-monnaie. Les utilisateurs jouent un rôle essentiel dans l'adoption et l'utilisation du Bitcoin, contribuant ainsi à son développement et à sa croissance.

## **Section 03 : gouvernance et régulation du bitcoin**

La gouvernance et la régulation du Bitcoin constituent un terrain complexe et en constante évolution, où se rencontrent les principes de décentralisation et les exigences réglementaires. Cette section examine les diverses approches adoptées par les gouvernements, les organismes de réglementation et les communautés Bitcoin pour encadrer cette crypto monnaie révolutionnaire. De la surveillance des échanges aux débats sur la légitimité du Bitcoin en tant que classe d'actifs, nous explorons les enjeux clés qui façonnent la gouvernance et la régulation du Bitcoin à l'échelle mondiale.

---

<sup>33</sup> <https://.bitpanda.com>

### **1. La régularisation des crypto monnaie <sup>34</sup>**

En raison des risques inhérents aux crypto-monnaies et de leurs multiples applications, il est crucial d'examiner comment les réglementer efficacement. L'évolution des activités basées sur ces monnaies virtuelles exige une adaptation et une modernisation du cadre juridique et réglementaire.

Les régulateurs et superviseurs financiers européens et internationaux préconisent une réglementation des activités liées aux crypto-monnaies pour quatre raisons principales :

- a. Lutte contre le blanchiment d'argent et le financement du terrorisme (BL blanchiment d'argent et du terrorisme): Il s'agit d'une priorité absolue, car les crypto-monnaies, par leur nature anonyme et décentralisée, peuvent faciliter les activités illégales.
- b. Protection des investisseurs : Les investisseurs en crypto-monnaies courent des risques importants en raison de la volatilité élevée de ces actifs et du manque de protection réglementaire adéquate. Une réglementation vise à garantir des pratiques commerciales équitables et à protéger les investisseurs contre les fraudes et les abus.
- c. Préservation de l'intégrité des marchés : L'essor des crypto-monnaies soulève des inquiétudes quant aux risques de manipulation de marché, de piratage informatique et d'autres activités illégales qui pourraient menacer la stabilité et l'efficacité des marchés financiers.
- d. Stabilité financière : Si l'adoption des crypto-monnaies continue de croître, cela pourrait avoir des implications pour la stabilité du système financier dans son ensemble. La réglementation vise à atténuer ces risques potentiels en encadrant le développement et l'utilisation des crypto-monnaies.

#### **1.1. Les institutions de régulation <sup>35</sup>**

Proposent une stratégie possible qui repose sur trois volets complémentaires :

Un volet « Régulation et coopération »

Un volet « Encadrement de l'utilisation »

Un volet « Connaissance et investigation »

---

<sup>34</sup><http://journalducoin.com>

<sup>35</sup> Dans notre travail, nous nous appuyons sur les études, analyses et propositions faites, par les institutions et autorités de contrôle françaises, sur les crypto-monnaies.

### **1.1.1. Les points clés du volet "Régulation et coopération"**

Des propositions sont formulées afin d'adapter le dispositif de lutte contre le blanchiment et le Financement du terrorisme aux risques posés par les monnaies virtuelles et l'essor de Nouvelles activités en lien avec ces dernières. A cet effet, les recommandations suivantes ont Été formulées<sup>36</sup>

#### **1.1.1.1. Réglementer des services offerts a l'interface entre l'asphère réelle et crypto-monnaie**

- Les plateformes de change de crypto-monnaies :

Un statut spécifique pour un rôle plus large. L'activité des plateformes de conversion de crypto-monnaies ayant cours légal, qui servent d'intermédiaires entre acheteurs et vendeurs, est actuellement considérée comme un service de paiement. Cependant, cette classification se base uniquement sur la gestion de comptes de tiers libellés en monnaie ayant cours légal, et ne prend pas en compte l'ensemble des services liés aux crypto-monnaies.

C'est pourquoi la Banque de France et l'ACPR préconisent la création d'un statut spécifique de "prestataire de services en crypto-monnaies" (PSAN). Ce statut permettrait d'encadrer plus largement l'activité de ces plateformes et de mieux répondre aux risques et enjeux spécifiques des crypto-monnaies.

- Ce nouveau statut regrouperait notamment les activités suivantes :

La conservation de crypto-monnaies pour le compte de tiers (activité de "wallet" ou "gardiennage") L'achat et la vente de crypto-monnaies contre des monnaies ayant cours légal (activité d'échange) L'exécution d'ordres sur des plateformes de négociation de crypto-monnaies (activité de broker) L'émission de jetons numériques (activité d'ICO)

- La mise en place d'un statut de PSAN permettrait de :

Renforcer la protection des investisseurs en imposant des obligations claires aux plateformes en matière de transparence, de lutte contre le blanchiment d'argent et le financement du terrorisme (LAB/FT), et de gestion des risques.

Favoriser un développement ordonné du marché des crypto-monnaies en créant un cadre juridique clair et stable pour les acteurs du secteur.

Préserver la stabilité financière en atténuant les risques liés aux crypto-monnaies, tels que la manipulation de marché et les cybers attaques.

---

<sup>36</sup> Mme sidhoum, mémoire, « la crypto-monnaie : Emergence, enjeux et perspectives », promotion 2018-2019

La création d'un statut de PSAN est une étape importante dans l'encadrement du marché des crypto-monnaies. Elle permettrait de mieux protéger les investisseurs, de favoriser l'innovation et de préserver la stabilité financière.

Cette évolution réglementaire pourrait s'inscrire dans le prolongement de la révision de la IVe Directive de lutte contre le blanchiment des capitaux et le financement du terrorisme en cours D'adoption par l'UE (dite "Ve" directive LCB-FT)<sup>37</sup>.

- Concrètement, la directive MiCA soumettrait à la réglementation :

Les plateformes d'échange de crypto-monnaies contre des monnaies ayant cours légal.

Les plateformes de conservation de crypto-monnaies pour le compte de leurs clients.

- Ces plateformes seraient soumises à des obligations strictes en matière de :

Lutte contre le blanchiment de capitaux et le financement du terrorisme (LAB/FT).

Sécurité des opérations.

Protection de la clientèle. La directive MiCA pourrait également couvrir les services liés aux transactions entre crypto-monnaies. La création d'un statut de "prestataire de services en crypto-monnaies" (PSAN) est envisagée pour encadrer ces activités. Ce statut permettrait de : Renforcer la protection des investisseurs.

Favoriser un développement ordonné du marché des crypto-monnaies. Préserver la stabilité financière. L'encadrement des plateformes de crypto-monnaies par la directive MiCA et la création d'un statut de PSAN constituent des étapes importantes pour la régulation du marché des crypto-monnaies.

### **1.1.1.2. Encadrer les placements en crypto-monnaies**

Un défi pour les régulateurs. L'encadrement des placements en crypto-monnaies constitue un deuxième axe majeur de l'élargissement du cadre réglementaire proposé par la Banque de France et l'ACPR. L'objectif est de limiter l'exposition des acteurs réglementés (banques, assurances, sociétés de gestion, etc.) aux crypto-actifs, afin de préserver la stabilité financière.

Interdire les activités de dépôts et de prêts en crypto-monnaies.

Soumettre les produits liés aux crypto-monnaies à des règles strictes de protection de la clientèle. Encadrer rigoureusement les placements pour compte propre des entités régulées, en déduisant par exemple la totalité de ces investissements des fonds propres.

---

<sup>37</sup> Directive LCB-FT (Lutte Contre le Blanchiment et Financement du Terrorisme) est une directive du parlement européen relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou de financement du terrorisme.

La directive MiCA : un encadrement renforcé des plateformes de crypto-monnaies

La directive MiCA (Markets in Crypto-Assets) vise à encadrer les activités liées aux crypto-monnaies, notamment celles des plateformes d'échange et de conservation.

La mise en œuvre de ces mesures nécessiterait une évolution des textes législatifs aux niveaux national, européen et même international.

### **1.1.1.3. Les enjeux de cet encadrement**

Protéger les investisseurs contre les risques élevés liés aux crypto-monnaies. Préserver la stabilité du système financier en limitant l'exposition des acteurs réglementés à ces actifs volatiles. Favoriser un développement ordonné du marché des crypto-monnaies en encourageant des pratiques saines. La recherche d'un équilibre entre innovation et protection des risques est au cœur de ce défi réglementaire. Pour sa part, l'AMF considère que l'offre de dérivés sur crypto-monnaies nécessite un agrément et ne doit pas faire l'objet de publicité par voie électronique. Par ailleurs, dans le prolongement de sa consultation publique sur les ICO, l'AMF a décidé de poursuivre le travail relatif à la définition d'un cadre juridique spécifique aux ICO prévoyant les garanties appropriées, notamment en matière d'information, qui seront nécessaires pour ce nouveau type d'offre. Ce travail sera mené en coordination avec les autres autorités publiques concernées<sup>38</sup>

#### **1.1.1.4. Une coordination internationale pour une régulation efficace des crypto-monnaies**

La Banque de France et l'ACPR estiment qu'une coordination européenne et internationale est indispensable pour garantir l'efficacité de la réglementation des crypto-monnaies.

La nature dématérialisée des crypto-monnaies et l'utilisation d'internet pour la fourniture transfrontalière de services liés à ces actifs rendent une approche hétérogène des réglementations nationales peu efficace. En effet, cela pourrait limiter la maîtrise des risques induits par ces nouvelles technologies.

Par conséquent, il est crucial d'engager un débat international sur la régulation des crypto-monnaies. C'est dans ce but que les ministres de l'Économie et des Finances français et allemands ont saisi le G20 en février 2018.

- Une harmonisation des réglementations aux niveaux communautaire et international permettrait de :

Lever l'anonymat avant la conversion des crypto-monnaies en monnaie légale. Cela faciliterait la lutte contre le blanchiment d'argent et le financement du terrorisme (LAB/FT).

Soumettre les professionnels du secteur aux obligations de vigilance renforcée en matière de LAB/FT, en particulier concernant les flux de crypto-monnaies.

- Cette coordination internationale est essentielle pour :

---

<sup>38</sup>Banque de France, Focus, Op.cit.

Assurer une protection efficace des investisseurs. Préserver la stabilité du système financier mondial. Favoriser un développement ordonné du marché des crypto-monnaies.

La mise en place d'un cadre réglementaire international harmonisé est un défi majeur, mais nécessaire pour répondre aux enjeux posés par les crypto-monnaies.

### **1.1.2. Les points clés du volet "Encadrement de l'utilisation**

Concernant l'encadrement de l'utilisation des crypto-monnaies, sans préjudice des Conclusions des débats et réflexion, au niveau national ou supranational, sur la qualification Juridique des monnaies virtuelles, des propositions ont été formulé afin de limiter :

- Lutter contre l'anonymat des utilisateurs

Mise en place d'une obligation d'identification de la clientèle ("Know Your Customer" - KYC) lors de l'ouverture d'un compte en crypto-monnaies.

Exigence de déclaration des comptes en crypto-monnaies au-delà d'un certain seuil.

Mise en place d'outils permettant de suivre les transactions et les comptes en crypto-monnaies.

- Limiter l'utilisation des crypto-monnaies comme moyen de paiement anonyme

Plafonnement des montants pouvant être payés en crypto-monnaies.

Interdiction des paiements en crypto-monnaies pour certains types de biens ou services.

- Encadrer les conversions entre espèces et crypto-monnaies

Réglementation des bornes d'échange de crypto-monnaies et des distributeurs automatiques de bitcoins. Limitation des montants pouvant être convertis entre espèces et crypto-monnaies.

Obligation d'identification de la clientèle pour les conversions importantes.

Ces mesures visent à :

- Lutter contre le blanchiment d'argent et le financement du terrorisme (LAB/FT).

Protéger les consommateurs contre les fraudes et les abus.

Préserver la stabilité du système financier.

Il est important de trouver un équilibre entre la lutte contre les risques et la préservation de l'innovation dans le domaine des crypto-monnaies.

### **1.1.3. Les points clés du volet "Connaissance et investigation**

Compte tenu du dynamisme du secteur des crypto-monnaies, de l'évolution extrêmement

Rapide des technologies et de la nécessité de renforcer la coopération internationale, des

Propositions sont également formulées afin d'assurer un suivi des risques et des opportunités

En lien avec les crypto-monnaies<sup>39</sup>:

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

Tableau N°02 : Une synthèse des trois piliers de la stratégie de lutte, proposée, contre les Risque des crypto-monnaie

Volet Régulation & Coopération	Volet Encadrement de l'utilisation	Volet Connaissance & Investigation
<ul style="list-style-type: none"><li>• Réglementer les services offerts à l'interface entre la sphère réelle et les crypto-monnaies ;</li><li>• Encadrer les placements ;</li><li>• Adapter le dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme aux risques posés par les crypto-monnaies et les activités les utilisant ;</li><li>• Harmoniser la régulation au niveau national et international.</li></ul>	<ul style="list-style-type: none"><li>• Limiter et plafonner l'utilisation des crypto-monnaies en tant que méthode de paiement ;</li><li>• Limiter et contrôler les flux espèces/crypto-monnaies ;</li><li>• Limiter l'anonymat des utilisateurs de crypto-monnaies.</li></ul>	<ul style="list-style-type: none"><li>• Disposer de ressources et d'outils d'analyse adaptés ;</li><li>• Effectuer un suivi des risques et des opportunités, notamment par des échanges avec les professionnels du secteur.</li></ul>

**Source : Rapport annuel 2014 de Tracfin ([www.economie.gouv.fr](http://www.economie.gouv.fr))**

---

<sup>39</sup>Ibid.

### **Conclusion**

La genèse de la crypto-monnaie est un récit captivant qui témoigne de l'évolution des systèmes financiers traditionnels vers des modèles décentralisés et numériques. Au cœur de cette révolution se trouve la technologie blockchain, un concept révolutionnaire qui offre une transparence inégalée, une sécurité renforcée et une décentralisation totale des transactions. La blockchain, socle du bitcoin et d'autres crypto-monnaies, représente un registre distribué et immuable, où chaque transaction est enregistrée de manière transparente et sécurisée.

Dans cet écosystème numérique, les acteurs du réseau bitcoin jouent des rôles cruciaux. Les mineurs, par exemple, sont responsables de la validation et de l'ajout de nouvelles transactions à la blockchain, tout en sécurisant le réseau via la puissance de calcul informatique. Les nœuds, quant à eux, agissent comme des points de connexion au réseau, vérifiant et transmettant les transactions. Enfin, les utilisateurs interagissent avec le réseau en envoyant, recevant et stockant des bitcoins, participant ainsi à la dynamique de l'économie virtuelle.

Dans l'ensemble, la genèse de la crypto-monnaie, alimentée par la technologie blockchain et animée par les divers acteurs du réseau bitcoin, incarne un changement de paradigme dans la façon dont nous concevons et utilisons la monnaie. Ce nouvel écosystème offre des possibilités inédites en matière de sécurité, de transparence et de liberté financière, ouvrant la voie à une ère de l'innovation et de la disruption dans le domaine financier.

## **Chapitre 02 : mécanisme de fonctionnement de bitcoin.**

## **Introduction**

Depuis sa création en 2009, le Bitcoin a captivé l'imagination du monde entier en tant que phénomène financier révolutionnaire. Au cœur de cette révolution se trouvent des mécanismes sophistiqués qui régissent la création, la transmission et la valorisation de cette crypto monnaie décentralisée. Le présent chapitre, intitulé "Mécanisme de fonctionnement du Bitcoin", se propose d'explorer en détail ces processus fondamentaux, répartis en trois sections distinctes.

La première section, dédiée à la création et à l'émission de nouveaux Bitcoins, mettra en lumière le concept de "minage". Cette activité, à la fois complexe et cruciale, consiste en la résolution de problèmes mathématiques complexes par des mineurs, garantissant ainsi la sécurité et l'intégrité du réseau Bitcoin. Nous plongerons dans les détails techniques du minage, examinant son rôle dans la mise en circulation de nouvelles unités de Bitcoin et son impact sur l'écosystème global de la crypto monnaie.

La deuxième section se concentrera sur les processus de transfert, de transaction et sur les aspects sécuritaires inhérents au Bitcoin. Nous explorerons notamment le fonctionnement de la blockchain, ce registre décentralisé qui enregistre toutes les transactions effectuées avec la cryptomonnaie. En mettant l'accent sur la validation et l'inscription des transactions sur la blockchain, nous évaluerons les protocoles et les technologies employés pour assurer la sécurité et la confidentialité des échanges Bitcoin.

Enfin, la troisième section se penchera sur la volatilité et la valeur du Bitcoin, en analysant les multiples facteurs économiques, sociaux et géopolitiques qui influent sur son cours. Nous examinerons les tendances historiques du Bitcoin, les événements majeurs qui ont façonné sa perception et sa valeur, ainsi que les défis persistants liés à sa stabilité financière. À travers cette analyse approfondie, nous chercherons à décrypter les mécanismes de valorisation du Bitcoin et à anticiper son évolution future dans le paysage financier mondial. !

## **Section 01:création de nouveau bitcoin**

La création de nouveaux Bitcoins, un processus fondamental du fonctionnement du réseau Bitcoin, repose sur un mécanisme complexe et novateur connu sous le nom de "minage". Cette première section se propose d'explorer en profondeur ce processus essentiel, qui joue un rôle crucial dans la mise en circulation et la sécurisation de cette cryptomonnaie révolutionnaire.

Au cours de cette section, nous plongerons dans les rouages du minage, explorant les défis mathématiques complexes auxquels les mineurs sont confrontés, ainsi que les récompenses et incitations qui les motivent à participer à ce processus. Nous examinerons également l'impact environnemental et énergétique du minage, ainsi que les innovations technologiques visant à rendre cette activité plus efficace et durable à long terme.

En comprenant les mécanismes de création de nouveaux Bitcoins, les lecteurs seront mieux équipés pour appréhender la dynamique de l'offre et de la demande dans l'écosystème Bitcoin, ainsi que pour saisir les enjeux liés à la sécurité et à la stabilité du réseau. En explorant les complexités du minage, nous serons en mesure d'apprécier pleinement le fonctionnement et le potentiel révolutionnaire de cette cryptomonnaie décentralisée.

### **1. Définition de minage**

Le minage de Bitcoin est une façon de gagner de nouveaux bitcoin en exécutant le processus de validation des transactions de bitcoins. Chaque mineur qui valide un bloc de transactions est récompensé avec une certaine quantité de bitcoins. En d'autres termes, c'est un double processus qui génère à la fois de nouveaux coins et permet aux coins en circulation d'être utilisés en toute sécurité.

### **2. Importance de la création et l'émission de nouveau bitcoin<sup>40</sup>**

La création et l'émission de nouveaux bitcoins également connue sous le nom de mining, sont cruciales pour maintenir le fonctionnement du réseau bitcoin et ont plusieurs implications importantes :

#### **2.1. Sécurisation du réseau :**

Les mineurs sont les gardiens de la sécurité du réseau Bitcoin. En résolvant des problèmes mathématiques complexes, ils valident les transactions et ajoutent de nouveaux blocs à la chaîne de blocs, garantissant ainsi l'intégrité et la résistance à la manipulation du registre public.

En échange de leur travail de sécurisation du réseau, les mineurs reçoivent une récompense sous forme de nouveaux bitcoins nouvellement créés. Cela incite les mineurs à participer au réseau et à maintenir sa sécurité.

#### **2.2. Introduction de nouveaux bitcoins dans l'économie :**

La création de nouveaux bitcoins est le mécanisme par lequel la quantité de bitcoins en circulation augmente. Le taux d'émission est défini par le protocole Bitcoin et diminue de manière prédéterminée au fil du temps, ce qui confère au Bitcoin une quantité totale limitée

---

<sup>40</sup> Mme sidhoum, mémoire, « la crypto-monnaie : Emergence, enjeux et perspectives », promotion 2018-2019

de 21 millions d'unités. Cette émission progressive de nouveaux bitcoins vise à contrer l'inflation et à maintenir la valeur de la monnaie.

### **2.3. Facilitation des transactions :**

Les frais de transaction minimes payés par les utilisateurs pour inclure leurs transactions dans la blockchain servent de compensation aux mineurs pour leur travail de sécurisation du réseau. Ces frais de transaction constituent une incitation supplémentaire pour les mineurs à maintenir le réseau en bon état et à traiter les transactions rapidement et efficacement.

### **2.4. Impact sur le prix du Bitcoin :**

Le taux d'émission de nouveaux bitcoins peut influencer le prix du Bitcoin. Une augmentation du taux d'émission peut entraîner une augmentation de l'offre, ce qui peut conduire à une pression à la baisse sur le prix. Inversement, une diminution du taux d'émission peut réduire l'offre, ce qui peut contribuer à une augmentation du prix.

Il est important de noter que la création et l'émission de nouveaux bitcoins sont des sujets complexes avec des implications économiques et techniques importantes. Il est crucial de bien comprendre ces aspects avant de s'engager dans l'achat, la vente ou le mining de bitcoins.

## **3. Fonctionnement du minage du bitcoin<sup>41</sup>**

Le minage consiste à valider les transactions sur le réseau de transfert bitcoin en contrepartie d'une récompense en fractions de BTC. À noter que, les informations relatives aux opérations de transfert sont enregistrées sous la forme de hash value. Le minage est donc un moyen de mettre de nouveaux jetons en circulation.

### **4. Le processus de minage de Bitcoin**

Maintenant que vous comprenez le fonctionnement de la blockchain, vous vous doutez bien que le minage est un processus très complexe qui doit passer par plusieurs étapes :

#### **4.1. Les transactions**

Avant d'être ajoutées à la base de données de la blockchain, les opérations de transfert vont d'abord passer par un processus de validation. Le processus de minage commence à partir de ce moment.

Supposons que A effectue un transfert de bitcoin vers le portefeuille de B. L'opération de transfert est d'abord intégrée dans une unité de validation. Ce dernier va collecter et regrouper plusieurs transactions par des nœuds miniers. Il arrive que plusieurs mineurs collectent les mêmes transactions. Mais elles ne seront pas confirmées jusqu'à ce que l'unité de validation soit minée.

---

<sup>41</sup> <http://journalducoin.com>

## **4.2. La création d'un bloc<sup>42</sup>**

L'ensemble des mineurs vérifient la validité de l'opération transfert et la confirment. Ils choisissent ensuite l'entête du bloc le plus récent afin de l'intégrer dans le nouveau en tant que hash.

Les mineurs doivent résoudre des problèmes mathématiques complexes encore et encore via un "nonce". Il s'agit d'un nombre aléatoire qui change continuellement jusqu'à ce que les contributeurs au processus de consensus trouvent la sortie ou le hachage valide, selon la condition. Une fois la solution trouvée, le bloc est ajouté à la chaîne et sera publié sur l'ensemble du réseau. B recevra alors la transaction de A.

Pour que le bloc puisse être miné, il doit répondre à des caractéristiques précises. Le hachage de l'entête de la section de chaîne ne doit pas être supérieur à la cible, faute de quoi il ne sera pas valide. Cet ensemble de données doit avoir une taille maximale de 2 Mo. L'horodatage du bloc ne doit pas excéder deux heures dans le futur.

Rôles des mineurs dans le nouveau bitcoin

Dans le réseau Bitcoin, les mineurs jouent un rôle crucial dans la vérification des transactions et les ajoutant à la blockchain. Ils sont responsables de la résolution de problèmes mathématiques complexes en utilisant la puissance de calcul, ce qui crée de nouveaux blocs dans la blockchain. Ce processus est appelé preuve de travail et est un aspect fondamental du réseau Bitcoin qui permet la confiance et la sécurité dans le domaine numérique. D'un point de vue économique, les mineurs sont incités à participer au réseau en recevant des récompenses pour leurs efforts de calcul. Sans mineurs, le réseau Bitcoin ne pourrait pas fonctionner comme il le fait aujourd'hui.

## **5. le rôle des mineurs dans le réseau Bitcoin:**

### **5.1. Vérification des transactions:**

Les mineurs sont responsables de la vérification des transactions au sein du réseau. Chaque transaction est diffusée au réseau et ajoutée à un pool de transactions non confirmées. Les mineurs sélectionnent ensuite les transactions qu'ils souhaitent inclure dans le bloc suivant.

### **5.2. Preuve de travail:**

Le processus de résolution de problèmes mathématiques complexes à l'aide de la puissance de calcul est appelé preuve de travail. Les mineurs rivalisent pour résoudre le problème, et le premier à le résoudre ajoute le bloc suivant à la blockchain. Ce processus crée la confiance et

---

<sup>42</sup><https://www.cointribune.com/minage-bitcoin-comment-ca-marche-vraiment/>

la sécurité au sein du réseau car il est extrêmement difficile pour les acteurs malveillants de falsifier la blockchain.

### **5.3. Récompenses de blocs:<sup>43</sup>**

Le terme “Block reward” signifie “Récompense de bloc” en français et désigne une récompense qui est attribuée aux mineurs de crypto monnaies en échange de leur travail.

La récompense du bloc Bitcoin a récemment été réduite de 6,25 BTC à 3,125 BTC lors du halving au bloc 840 000 le 20 avril, ce qui signifie que le bloc 841 286 valait environ 200 000 \$ à l'époque. Halving réduction de moitié des récompenses le plus important du réseau Bitcoin, le halving, pourrait légitimer le bitcoin en tant qu'actif de réserve de valeur pour l'ère numérique, à la recherche d'actifs plus liquides que l'immobilier ou l'or.

Le quatrième halving du bitcoin s'est produit il y a quelques heures aux 840 000 e blocs. Le halving est considéré comme le mécanisme économique le plus important influençant l'offre du bitcoin

BTC €62 578 La récompense du bloc Bitcoin a récemment été réduite de 6,25 BTC à 3,125 BTC lors du halving au bloc 840 000 le 20 avril, ce qui signifie que le bloc 841 286 valait environ 200 000 \$ à l'époque. Et créant la rareté de l'actif.

Le quatrième halving du réseau Bitcoin a réduit les récompenses d'émission de blocs de 6,25 BTC à 3,125 BTC par bloc miné, réduisant ainsi de moitié le taux d'émission de bitcoin.

Le halving est un mécanisme crucial pour la rareté du bitcoin et la valorisation du marché, selon Karim Chaib, le PDG de la plateforme de crypto monnaie Dopamine App. M. Chaib a déclaré à Cointelegraph :

« La rareté est un principe économique fondamental qui affecte la valeur d'un actif. En s'assurant de manière programmatique que l'offre de bitcoin augmente à un rythme plus lent au fil du temps, les halving soulignent la rareté du bitcoin. »

Le halving est intégré dans le code de base de Bitcoin, ce qui se produit tous les 210 000 blocs minés, soit environ tous les quatre ans.

Le réseau Bitcoin a connu son premier halving en 2012, lorsque le taux d'émission des bitcoins a été réduit de 50 BTC à 25 BTC par bloc miné. Les deux derniers halving ont eu lieu en 2016 et 2020, réduisant considérablement le taux d'émission du bitcoin à 3,125 BTC actuellement.

Les mineurs sont incités à participer au réseau en recevant des récompenses de bloc pour leurs efforts de calcul. Par exemple, en 2021, la récompense du bloc pour résoudre un bloc est de

---

<sup>43</sup><https://fr.cointelegraph.com/news/solo-bitcoin-miner-solves-valid-block-post-halving>

6,25 BTC, ce qui vaut plus de 200 000 \$ USD aux prix actuels du marché. Cette récompense incite les mineurs à continuer de contribuer à la puissance de calcul pour maintenir le réseau.

#### **5.4. Pools d'exploitation:**

Certains mineurs rejoignent les piscines minières pour augmenter leurs chances de résoudre le problème mathématique et de recevoir la récompense du bloc. Les pools miniers sont des groupes de mineurs qui combinent leur pouvoir de calcul pour résoudre le problème plus rapidement et partager les récompenses.

Les mineurs sont un composant essentiel du réseau Bitcoin car ils vérifient les transactions, les ajoutent à la blockchain et maintiennent la sécurité du réseau. Sans mineurs, le réseau ne serait pas en mesure de fonctionner comme il le fait aujourd'hui, et la confiance et la sécurité apportées par Bitcoin seraient compromises.

### **6. implémentation et fonctionnement**

Le BTC est implémentée comme un logiciel Open-source. Cela signifie que n'importe qui peut télécharger et exécuter le logiciel bitcoin. Le logiciel BTC est disponible pour une variété du système d'exploitation, y compris Windows, MacOS et Linux.

Le BTC fonctionne sur un réseau mondial d'ordinateurs qui utilisent la cryptographie pour sécuriser les transactions et contrôler la création de nouveau BTC. Chaque ordinateur du réseau BTC possède une copie du block chaine, qui est un registre public de toutes les transactions BTC.

#### **6.1. Algorithmes de chiffrement<sup>44</sup>**

Les algorithmes de chiffrement sont essentiels pour la sécurité et le fonctionnement du BTC ECDSA, SHA-256. Ces algorithmes sont unanimement considérés comme les plus sûrs, ils sont utilisés dans la banque, l'armée, le renseignement. S'ils étaient craqués tous les systèmes électroniques de la planète tomberaient. Une adresse bitcoin est de la forme : 175Twpb8k1s7Mh4Zx6rewF9wQrcPv245W. Il existe plus de  $10^{48}$  adresses possibles, soit que d'atomes sur terre.

- SHA-256 est une fonction de hachage cryptographique qui est utilisée pour créer des résumés de messages. Les résumés de message sont utilisés pour vérifier l'intégrité des transactions et pour identifier les bitcoins.
- ECDSA est un algorithme de signature numérique qui est utilisée pour signer la transaction. Les signatures numériques permettent de vérifier l'authenticité des transactions et de protéger les bitcoins contre la contrefaçon.

---

<sup>44</sup> Banque de France, Focus, Op.cit

## **6.2. Réseau décentralisée**

Le BTC est un réseau décentralisée, ce qui signifie qu'il n'y a pas d'autorité centrale qui contrôle le réseau. Au lieu de cela, le réseau est géré par un groupe d'ordinateurs volontaires répartis dans le monde entier.

Un système décentralisée dans lequel chaque participant est responsable de sa clé privée évite ce risque ; il n'existe tout simplement pas <un> mot de passe qui permettrait de craquer le réseau bitcoin. Il existe un site officiel du projet (bitcoin.org) mais il est distincte du réseau proprement dit : le fait de hacker ce site ne donnerait aucun accès aux comptes, bien sûr.

## **6.3. Minage et récompenses<sup>45</sup>**

Cette étude vise à analyser les différents aspects du minage de crypto-monnaies, notamment les techniques utilisées, les coûts associés et les récompenses potentielles. De plus, elle examinera l'impact du minage sur la consommation d'énergie, l'environnement et la sécurité des réseaux blockchain. En comprenant l'importance croissante du minage dans l'économie numérique actuelle, cette étude fournira des éclairages précieux pour les acteurs du secteur financier, les chercheurs et les décideurs politiques, afin de contribuer à une compréhension plus globale et nuancée de ce phénomène en constante évolution.

La montée en popularité des crypto-monnaies, telles que le Bitcoin et l'Ethereum, a suscité un intérêt croissant pour le minage et les récompenses associées. Ce phénomène a entraîné des changements significatifs dans le paysage financier mondial, avec des implications pour les investisseurs, les mineurs et les régulateurs. Par conséquent, il est crucial de comprendre l'évolution du minage et des récompenses dans le domaine des crypto-monnaies, afin d'appréhender les défis et opportunités qui en découlent.

Donc, le contexte et l'importance de l'étude sur l'évolution du minage et des récompenses dans les crypto-monnaies. Il souligne les liens étroits avec les discussions plus larges sur la décentralisation, la sécurité et la durabilité de la monnaie numérique. En analysant les tendances historiques et les innovations actuelles, on peut mieux comprendre les défis et les opportunités de l'écosystème des crypto-monnaies. Cette connaissance est essentielle pour prendre des décisions éclairées sur les stratégies d'investissement, l'élaboration de politiques et les progrès technologiques dans l'industrie.

---

<sup>45</sup> Banque de France, Focus, Op.cit

## **7. Impact et perspective d'avenir<sup>46</sup>**

### **7.1. Adoption mondiale**

L'adoption mondiale du bitcoin est en constante augmentation. De plus en plus d'entreprises et d'individus utilisent le BTC pour effectuer des paiements et transférer des fonds.

#### **7.1.1 Facteurs d'adoption**

Plusieurs facteurs contribuent à l'adoption mondiale du BTC, notamment :

- La hausse des prix : le prix du BTC a connu une augmentation importante ces dernières années. Cela attire l'attention des investisseurs et des spéculateurs, qui ont contribué à stimuler la demande de BTC.
- L'inflation : est un problème croissant dans de nombreux pays du monde. Le BTC est souvent considéré comme une protection contre l'inflation, car sa quantité est limitée et ne peut pas être contrôlée par les gouvernements.
- Les transferts de fonds internationaux : le BTC peut être utilisé pour effectuer des transferts internationaux à moindre coût et plus rapidement que les méthodes traditionnelles. Cela est particulièrement intéressant pour les personnes qui envoient de l'argent à des parents ou des amis dans d'autres pays.
- La censure et le contrôle des capitaux : le BTC est une monnaie décentralisée, ce qui signifie qu'il n'est pas soumis au contrôle des gouvernements ou des institutions financières. Cela rend le BTC attrayant pour les personnes qui vivent dans des pays où la censure et le contrôle des capitaux sont importants.

#### **7.1.2. Défis à l'adoption**

Malgré sa croissance rapide, l'adoption mondiale du bitcoin reste encore limitée. Il existe plusieurs facteurs qui freinent l'adoption du BTC, notamment :

- La volatilité : le prix du BTC est très volatile, ce qui peut dissuader les gens de l'utiliser comme monnaie.
- La réglementation : la réglementation du BTC varie d'un pays à l'autre. Dans certains pays, le BTC est autorisé, tandis que dans d'autres, il est interdit ou fortement réglementé. L'incertitude réglementaire peut dissuader les entreprises et les individus d'utiliser le BTC.
- L'adoption par les commerçants : le nombre de commerçants qui acceptent le BTC est encore relativement faible. Cela peut être un obstacle pour les personnes qui souhaitent utiliser le BTC pour effectuer des paiements quotidiens.

---

<sup>46</sup><https://libertex.com>

### 7.1.3. Perspectives d'avenir

Les perspectives d'avenir du BTC sont incertaines. Certains experts pensent que le BTC pourrait devenir une monnaie mondiale dominante, tandis que d'autres pensent qu'il finira par échouer.

L'avenir du BTC dépendra de plusieurs facteurs, notamment de l'évolution de son prix, de la réglementation gouvernementale et de l'adoption par les commerçants.

## Section 02 : transfert, transaction et sécurité : validation et inscription

Le bitcoin est une crypto-monnaie très populaire et de plus en plus utilisée. Mais comprenez-vous réellement son agissement ? En effet, il faut savoir que cette monnaie numérique est gérée par une chaîne de bloc ou blockchain qui répertorie l'ensemble des transactions effectuées en bitcoins depuis sa création. Toute transaction est consultable par tous et l'envoi de bitcoin n'est pas si simple. En effet, un échange de bitcoin fait jouer un processus complexe comprenant une large série d'étape permettant de transférer la crypto monnaie d'un portefeuille à un autre. Ici, nous vous expliquons pas-à-pas comment fonctionne une transaction en bitcoin et tout ce que cela laisse entendre.

### 1. Le fonctionnement des transactions en Bitcoin<sup>47</sup>

Pour comprendre le fonctionnement des transactions en BTC, il est préférable de se faire une idée de ce à quoi ressemble une transaction Bitcoin. Imaginez que vous vouliez envoyer de l'argent à un de vos amis. Si vous choisissez Bitcoin, la transaction se compose de trois parties :

- Une entrée : Un enregistrement de votre adresse.
- Un montant : Le montant précis de Bitcoin que vous envisagez de lui envoyer.
- Une sortie : La clé publique de votre ami – ou l'adresse du portefeuille Bitcoin.

Pour envoyer des bitcoins, vous devez avoir accès aux clés publiques et privées qui sont associées à la quantité spécifique de bitcoins que vous souhaitez envoyer. En principe, une personne qui possède des Bitcoins a deux paires de clés, qui comprennent :

- Une clé publique à laquelle des bitcoins ont été envoyés auparavant.
- Une clé privée qui permet d'envoyer ce bitcoin ailleurs.

Ces montants reçus lors d'une transaction précédente et non dépensés dans une nouvelle transaction sont appelés UTXO, ou Unspent Transaction Outputs et sont indivisibles. La

---

<sup>47</sup> <https://coinacademy.com>

totalité des UTXO qu'il est nécessaire d'additionner pour atteindre 1 BTC seront donc dépensés, et la différence lui sera retournée.

Lorsqu'un UTXO est consommé par la création d'une nouvelle transaction, on parle d'input. L'UTXO dépensé est détruit, un nouvel UTXO est créé à destination du wallet récepteur, et un UTXO représentant le change de la transaction est créé pour l'expéditeur. Le solde de votre portefeuille représente en réalité l'agrégation de tous les UTXO dont votre adresse est la destination.

Les UTXO représentent un élément central du fonctionnement de Bitcoin. D'autres blockchains comme Ethereum s'appuient au contraire sur un système de comptes. Au sein de telles architectures, les wallets sont assimilables à des comptes bancaires contenant un certain solde de crypto monnaies.

## **2. Les étapes d'une transaction**

- Un utilisateur émet une transaction

La transaction est diffusée à tous les ordinateurs participants au réseau Bitcoin, ces ordinateurs sont appelés nœuds. Toutes les transactions sont publiées dans le mempool.

- Les mineurs vérifient la transaction par rapport à certaines règles de validation définies par les créateurs du réseau blockchain spécifique. Les transactions validées sont stockées dans un bloc et sont scellées avec une clé appelée hash.
- Ce nouveau bloc est ajouté à la blockchain Bitcoin et devient partie intégrante de la blockchain lorsque les autres ordinateurs du réseau vérifient si la clé du bloc est correcte.
- La transaction est terminée et ne peut plus être modifiée de quelque manière que ce soit.

## **3. Le rôle des mineurs dans la transaction<sup>48</sup>**

Chaque mineur tente d'être le premier à produire le prochain bloc afin d'obtenir une récompense en bitcoins. Pour cela, ils doivent résoudre une énigme mathématique nécessitant une puissance de calcul conséquente : c'est le principe du Proof-of-Work.

### **3.1. L'énigme à résoudre est la suivante :**

Tenter de trouver un nombre dont le hash commence par un nombre de zéros défini à l'avance. Ainsi, le mineur doit tester aléatoirement toutes les possibilités jusqu'à tomber sur la bonne. Ce chiffre aléatoire est appelé nonce. Le premier mineur à trouver un nonce satisfaisant produit le bloc suivant.

---

<sup>48</sup> <https://www.coinbase.com>

### **3.2. Le bloc :**

Contient les transactions incluses par le mineur, le nonce, et un hash du bloc précédent. Ce hash permet de lier les blocs entre eux, créant ainsi une blockchain. Ce mécanisme constitue un élément essentiel à la sécurité du réseau. En effet, si un acteur mal intentionné tente de modifier les transactions d'un bloc, le hash de ce dernier sera également altéré. Puisque ce hash est inclus dans le bloc suivant, le hash du bloc suivant changerait également, et ainsi de suite. Grâce à ce système, il est impossible de modifier un bloc sans devoir recalculer tous les suivants, ce qui nécessiterait une puissance de calcul impossible à fournir en pratique. Ce procédé donne à Bitcoin son caractère sécurisé et immuable.

### **4. L'enregistrement des transactions dans une application**

Il existe une application officielle gratuite, qui contient toutes les clés privées. Elle repose sur un Fichier, qui est appelé "wallet"(porte-monnaie électronique ou porte feuille).

La clé privée sert à signer un message, tandis que la clé publique permet aux autres utilisateurs de vérifier ce message. Cette vérification repose sur une relation mathématique et cryptographique entre les deux clés. On peut comparer l'adresse à un coffre-fort et la clé privée à la clé qui l'ouvre. Lorsqu'une personne envoie des bitcoins, elle émet un message de transaction comprenant des détails comme le montant, la clé publique, l'adresse du destinataire, et une signature effectuée avec la clé privée. Les mineurs vérifient ces transactions en confirmant que les fonds sont disponibles, que la clé publique correspond à l'adresse bitcoin, et que la signature est valide.

### **5. La transparence du Bitcoin<sup>49</sup> :**

Un registre public pour des transactions sécurisées le Bitcoin se distingue des systèmes monétaires traditionnels par sa transparence inhérente. En effet, toutes les transactions Bitcoin sont enregistrées de manière permanente et accessible à tous sur un registre public appelé la blockchain.

Imaginez un immense registre consultable par tous, où chaque page correspond à un bloc de transactions Bitcoin. Chaque transaction est horodatée et crypto graphiquement liée à la précédente, créant ainsi une chaîne chronologique infalsifiable.

#### **5.1. Ses avantages majeurs :**

- Sécurité des transactions: Chaque transaction est vérifiée et validée par le réseau Bitcoin, ce qui la rend extrêmement difficile à falsifier.

---

<sup>49</sup> <https://www.paymium.com>

- Visibilité des transactions: N'importe qui peut consulter l'historique de n'importe quelle adresse Bitcoin et suivre le mouvement des fonds. Cela permet de lutter contre la fraude et d'accroître la confiance dans le système.
- Responsabilité: Les utilisateurs sont responsables de leurs transactions, car celles-ci sont publiquement enregistrées sur la blockchain.

L'accès à ce registre public se fait par le biais des explorateurs de blocs Bitcoin. Ces outils en ligne permettent de visualiser l'ensemble des transactions Bitcoin, de rechercher des adresses ou des transactions spécifiques et d'explorer les données du block chain.

Il est important de noter que la transparence du Bitcoin ne signifie pas que l'identité des Utilisateurs est nécessairement publique. Les adresses Bitcoin ne sont pas directement liées à l'identité réelle des utilisateurs, et il existe des techniques pour améliorer la confidentialité des transactions. Cependant, la transparence inhérente au Bitcoin pose également des questions concernant la confidentialité des utilisateurs. C'est un sujet de débat constant, et des solutions sont développées pour trouver un équilibre entre transparence et confidentialité dans le réseau Bitcoin.

## **6. Evolution des transactions en bitcoins<sup>50</sup> :**

Au-delà de la spéculation le Bitcoin, initialement perçu comme un outil de spéculation, s'est progressivement diversifié vers d'autres usages, dont deux principaux :

### **6.1. Transferts internationaux entre particuliers :**

Le Bitcoin offre une alternative aux transferts d'argent internationaux traditionnels, souvent lents et coûteux. Ses frais de transaction faibles et sa rapidité d'exécution en font un choix attractif pour les transferts de fonds entre particuliers, notamment vers des pays où l'accès aux services financiers traditionnels est limité. L'utilisation du Bitcoin à cette fin est particulièrement notable dans les pays en développement, où il permet aux migrants d'envoyer de l'argent à leurs familles à moindre coût.

### **6.2. Monnaie de paiement pour les commerces :**

De plus en plus de commerces acceptent le Bitcoin comme moyen de paiement, bien que son adoption reste encore limitée.

Cette tendance est particulièrement visible dans certains secteurs comme le e-commerce, les jeux vidéo et les services en ligne. L'utilisation du Bitcoin comme monnaie de paiement offre

---

<sup>50</sup> <https://fr.statista.com>

certains avantages aux commerçants, tels que des frais de transaction moins élevés et une protection contre la fraude.

### **6.3. Outil de développement dans les pays émergents :**

Dans les pays en développement, où l'accès aux services financiers traditionnels est souvent restreint, le Bitcoin peut jouer un rôle important pour l'inclusion financière. Il permet aux personnes non bancarisées d'accéder à un système de paiement et de transfert d'argent sécurisé et abordable. Le Bitcoin peut également être utilisé pour l'épargne et la micro finance, offrant aux populations défavorisées de nouvelles opportunités économiques.

### **6.4. Valeur refuge contre les fluctuations monétaires :**

Dans certains pays confrontés à une inflation élevée ou à une instabilité monétaire, le Bitcoin est considéré comme une valeur refuge. Sa valeur étant non corrélée aux monnaies nationales, il peut permettre de protéger l'épargne contre la dépréciation. Il est important de noter que cette utilisation du Bitcoin comporte des risques importants, liés notamment à sa volatilité élevée.

Donc, l'utilisation du Bitcoin va bien au-delà de la simple spéculation. Son potentiel pour faciliter les transferts internationaux, promouvoir l'inclusion financière et servir de valeur refuge en fait un outil aux multiples facettes, dont l'impact ne cesse de croître.

## **Section 03 volatilité et valeur de bitcoin : analyses des facteurs**

La volatilité et la valeur du Bitcoin ont été des sujets d'intérêt majeur dans le domaine des cryptomonnaies et au-delà. Alors que le Bitcoin continue de gagner en popularité et de s'affirmer comme une classe d'actifs à part entière, comprendre les facteurs qui influencent sa volatilité et sa valeur revêt une importance cruciale pour les investisseurs, les chercheurs et les observateurs du marché.

Dans cette section, nous explorerons en profondeur les divers éléments qui contribuent à la volatilité du Bitcoin et à son évolution de valeur. Nous examinerons les facteurs économiques, technologiques, réglementaires et psychologiques qui façonnent le paysage du Bitcoin, ainsi que les méthodes d'analyse utilisées pour évaluer ces facteurs.

En analysant les dynamiques complexes qui entourent la volatilité et la valeur du Bitcoin, nous chercherons à fournir des perspectives éclairantes sur la manière dont cette crypto monnaie unique interagit avec les marchés financiers mondiaux et son potentiel en tant que réserve de valeur et moyen d'échange à l'avenir.

## **1. les facteurs des cours du bitcoin**

### **1.1. Envoi et réception d'argent dans le monde entier<sup>51</sup>**

Le Bitcoin permet d'envoyer et de recevoir de l'argent partout dans le monde, sans restrictions géographiques. Contrairement aux transferts bancaires traditionnels, qui peuvent être soumis à des délais et des frais importants pour les transactions internationales, le Bitcoin offre une solution rapide et économique.

### **1.2. Disponibilité 24/7 :**

Le Bitcoin peut être utilisé à tout moment, sans interruption due aux jours fériés ou aux heures d'ouverture des banques. Cette flexibilité est particulièrement appréciée par les utilisateurs qui ont besoin d'effectuer des transactions urgentes ou en dehors des heures ouvrables traditionnelles.

### **1.3. Vitesse des transactions :**

Les transactions en Bitcoin sont généralement traitées très rapidement, souvent en quelques secondes ou minutes. Cette rapidité d'exécution est un atout majeur pour les paiements en ligne et les transferts d'argent urgents.

### **1.4. Absence de limitations :**

Contrairement aux comptes bancaires traditionnels, qui peuvent être soumis à des plafonds de transaction quotidiens ou mensuels, le Bitcoin offre une liberté totale en matière de montants transférés.

Les utilisateurs peuvent envoyer et recevoir des sommes importantes sans restrictions imposées par les institutions financières.

### **1.5. Indépendance des politiques monétaires:**

Le Bitcoin n'est pas soumis aux politiques d'émission de monnaie des autorités centrales.

Sa valeur n'est pas influencée par les décisions des banques centrales, ce qui peut être un avantage pour les utilisateurs qui souhaitent se protéger contre l'inflation ou les interventions gouvernementales.

Il est important de noter que ces avantages allégués du Bitcoin s'accompagnent également de certains risques, tels que la volatilité élevée, la vulnérabilité aux piratages et l'absence de régulation.

Donc, le Bitcoin offre une série d'avantages en matière de flexibilité et de rapidité des transactions, ce qui en fait un outil attractif pour de nombreux utilisateurs. Cependant, il est essentiel de prendre en compte les risques associés à cette technologie avant de l'utiliser.

---

<sup>51</sup> <https://bitpanda.com>

## **2. Risques potentiels associés au Bitcoin:**

### **2.1. Risques pour le porteur <sup>52</sup>**

#### **2.1.1. Volatilité élevée :**

Le cours du Bitcoin est sujet à des fluctuations importantes, pouvant subir des variations considérables en un court laps de temps. Cette volatilité élevée fait du Bitcoin un investissement risqué, susceptible de générer des pertes importantes pour les utilisateurs.

#### **2.1.2. Sensibilisation et compréhension du protocole :**

L'utilisation efficace du Bitcoin requiert une compréhension adéquate de son fonctionnement et de son protocole. La complexité technique peut rebuter certains utilisateurs et limiter son adoption à grande échelle.

#### **2.1.3. Irréversibilité des transactions :**

Une fois effectuée, une transaction en Bitcoin est irréversible. Cela signifie qu'il est impossible d'annuler une transaction en cas d'erreur ou de fraude, ce qui peut poser des problèmes pour les utilisateurs.

#### **2.1.4. Dépendance à Internet :**

Le fonctionnement du Bitcoin repose sur le protocole IP et Internet. En cas de coupure d'Internet ou de restriction par un gouvernement, le réseau Bitcoin pourrait être ralenti ou bloqué.

#### **2.1.5. Gigantisme et limites techniques :**

- Taille croissante du block chaine : La taille de la base de données Bitcoin augmente rapidement, nécessitant une capacité de stockage importante. Des solutions pour optimiser l'espace disque sont en discussion.
- Besoins en bande passante : La synchronisation de l'ensemble du block chaine peut s'avérer gourmande en bande passante, ce qui pose des problèmes pour les utilisateurs avec des connexions Internet lentes.
- Limites des "super-nœuds" : Les "super-nœuds", conçus pour faciliter la propagation d'informations sur le réseau, peinent à suivre l'augmentation de la taille du block chaine.
- Donc, le Bitcoin présente des avantages potentiels, mais il est crucial de prendre en compte ses limites et ses défis avant de l'utiliser. La compréhension du protocole, la volatilité, l'irréversibilité des transactions, la dépendance à Internet et les contraintes techniques sont des facteurs importants à considérer.

---

<sup>52</sup> <https://www.cmcmarkets.com>

## **2.2. Risques liés aux plateformes d'échange de crypto monnaies<sup>53</sup>**

L'utilisation d'établissements pour convertir des cryptomonnaies en devises fiat comporte des risques spécifiques qu'il est important de connaître :

### **2.2.1. Défaillance ou faillite des plateformes :**

Les plateformes d'échange de cryptomonnaies sont des entreprises privées qui peuvent être sujettes à des défaillances ou à des faillites. En cas de problème, les utilisateurs risquent de perdre leurs fonds déposés sur la plateforme. L'exemple de MtGox, une plateforme d'échange majeure qui a fait faillite en 2014, illustre ce risque. Des milliers d'utilisateurs ont perdu des bitcoins à cette occasion.

### **2.2.2. Piratage informatique :**

Les plateformes d'échange de cryptomonnaies peuvent être la cible de piratages informatiques, entraînant le vol de fonds des utilisateurs.

La sécurité des plateformes est donc un élément crucial à prendre en compte avant de choisir une plateforme pour convertir ses cryptomonnaies.

### **2.2.3. Manipulation des prix :**

Certaines plateformes d'échange ont été accusées de manipuler les prix des cryptomonnaies afin de profiter de mouvements de marché favorables.

Cette pratique, connue sous le nom de "pump and dump", peut entraîner des pertes importantes pour les utilisateurs qui ne sont pas informés.

### **2.2.4. Manque de régulation :**

Le marché des cryptomonnaies est encore largement non réglementé, ce qui signifie que les plateformes d'échange ne sont pas soumises aux mêmes exigences que les institutions financières traditionnelles.

Ce manque de régulation peut accroître les risques pour les utilisateurs, car il n'y a pas d'organisme officiel pour les protéger en cas de problème.

### **2.2.5. Fraude et blanchiment d'argent :**

L'anonymat relatif des transactions en crypto monnaies peut les rendre attrayantes pour les activités illégales telles que la fraude et le blanchiment d'argent.

Les utilisateurs doivent être vigilants et choisir des plateformes qui mettent en place des mesures pour lutter contre ces activités.

---

<sup>53</sup> <https://www.lafinancepourtous.com>

Il est important de choisir une plateforme d'échange de crypto monnaies fiable et sécurisée avant de convertir ses crypto monnaies en devises fiat. Il est également crucial de se renseigner sur les risques encourus et de prendre des précautions pour protéger ses fonds.

### **2.3. Impact et risques environnementaux du Bitcoin :**

Un examen approfondi. Le Bitcoin, tout en étant une innovation technologique et financière majeure, soulève des préoccupations importantes concernant son impact environnemental. L'extraction de Bitcoin, processus gourmand en énergie connu sous le nom de "minage", est souvent critiquée pour sa consommation d'électricité excessive et ses émissions de gaz à effet de serre<sup>54</sup>.

#### **2.3.1. Consommation d'énergie élevée :**

Le minage de Bitcoin nécessite des ordinateurs puissants qui fonctionnent en permanence pour résoudre des problèmes mathématiques complexes. Cette activité consomme une quantité massive d'électricité, comparable à la consommation annuelle de certains pays.

#### **2.3.2. Sources d'énergie et impact sur le climat :**

L'électricité utilisée pour le minage de Bitcoin provient souvent de sources non renouvelables, telles que le charbon et le gaz naturel, ce qui contribue aux émissions de gaz à effet de serre et au changement climatique.

#### **2.3.3. Impact local sur l'environnement :**

Les centres de minage de Bitcoin sont souvent concentrés dans des régions où l'électricité est bon marché, ce qui peut entraîner des impacts environnementaux locaux importants, tels que la pollution de l'air et de l'eau, le bruit et les déchets électroniques.

#### **2.3.4. Comparaison avec d'autres systèmes:**

Si le Bitcoin est souvent critiqué pour son impact environnemental, il est important de le comparer à d'autres systèmes financiers. L'extraction de l'or et les transactions par carte bancaire ont également un impact environnemental non négligeable.

#### **2.3.5. Recherche de solutions et alternatives :**

Des efforts sont en cours pour développer des méthodes de minage de Bitcoin plus éco-énergétiques et pour identifier des sources d'énergie renouvelables pour alimenter les centres de minage.

---

<sup>54</sup> <https://hellocarbo.com>

### **3. Débat en cours et nécessité d'une réglementation <sup>55</sup>:**

L'impact environnemental du Bitcoin fait l'objet d'un débat public et politique important. Il est crucial de mener des recherches plus approfondies et de mettre en place une réglementation adéquate pour minimiser les effets négatifs du Bitcoin sur l'environnement.

Risques éthiques du Bitcoin : Questions sur la distribution de la richesse.

Le Bitcoin, tout en étant une innovation technologique et financière, soulève des questions éthiques concernant sa philosophie et son impact sur la distribution de la richesse.

#### **3.1. Inégalité de la répartition de la richesse :**

Certains critiques affirment que le Bitcoin favorise les premiers acquéreurs ("earlyadopters") de la monnaie, qui ont pu acheter des bitcoins à un prix très bas et profiter de l'augmentation de sa valeur. Cette concentration de richesse chez un petit nombre d'individus soulève des questions d'équité et de justice sociale.

#### **3.2. Comparaison avec les monnaies traditionnelles et l'étalon-or :**

Les partisans du Bitcoin soulignent que la répartition de la richesse dans les systèmes monétaires traditionnels n'est pas non plus optimale, avec des inégalités importantes entre les individus et les pays.

Ils affirment que le Bitcoin, en tant que système décentralisé et transparent, pourrait contribuer à une répartition plus équitable de la richesse.

#### **3.3. Études et débats en cours :**

Des études ont montré que la répartition de la richesse en Bitcoin est effectivement très inégalitaire, avec une concentration importante chez un petit nombre d'individus.

Cependant, d'autres études ont nuancé ces conclusions, en soulignant que la distribution de la richesse est en constante évolution et que le Bitcoin est encore une technologie relativement jeune.

#### **3.4. Nécessité d'une analyse approfondie et d'un débat public :**

L'impact éthique du Bitcoin sur la distribution de la richesse est un sujet complexe qui nécessite une analyse approfondie et un débat public éclairé.

Il est important de prendre en compte les différents points de vue et de mener des recherches plus approfondies pour mieux comprendre les implications de cette technologie sur la société.

#### **3.5. Réflexion sur les objectifs et les valeurs sociétales :**

Le débat sur le Bitcoin nous invite à réfléchir aux objectifs et aux valeurs que nous souhaitons privilégier dans nos systèmes économiques.

---

<sup>55</sup> <https://www.bfmtv.com>

## **Faut-il privilégier l'efficacité et la liberté individuelle ou chercher à promouvoir une répartition plus équitable de la richesse ?<sup>56</sup>**

Ces questions fondamentales méritent une attention particulière dans le cadre du développement de nouvelles technologies financières.

Risques de fraude, risques systémiques et risques spéculatifs liés au Bitcoin : Une analyse approfondie

Le Bitcoin, tout en étant une innovation technologique et financière, présente des risques de fraude, systémiques et spéculatifs qui ne doivent pas être négligés.

### **3.5.1. Risque de fraude :**

L'anonymat relatif des transactions en Bitcoin peut le rendre attractif pour des activités frauduleuses telles que le blanchiment d'argent et le financement du terrorisme.

Il est important de choisir des plateformes d'échange et des services de stockage de crypto monnaies fiables et sécurisés pour minimiser ce risque.

### **3.5.2. Risque systémique :**

L'adoption croissante du Bitcoin pourrait avoir un impact sur la stabilité du système financier mondial. En cas de chute brutale du cours du Bitcoin, cela pourrait entraîner des pertes importantes pour les investisseurs et des perturbations sur les marchés financiers.

### **3.5.3. Risque spéculatif :**

Le Bitcoin est souvent considéré comme un investissement hautement spéculatif en raison de sa volatilité élevée et de son caractère non réglementé.

Les investisseurs doivent être conscients des risques encourus et ne pas investir plus d'argent qu'ils ne peuvent se permettre de perdre

## **3.6. Mises en garde des banques centrales :**

Certaines banques centrales, comme la Banque centrale européenne, la Banque de France et la Banque de Chine, ont émis des mises en garde concernant les risques liés au Bitcoin.

Elles soulignent son caractère spéculatif et son utilisation potentielle à des fins illégales.

Le Bitcoin présente des avantages potentiels en termes d'innovation financière, mais il est crucial de prendre en compte ses risques. Il est important d'investir prudemment et de se renseigner sur les risques encourus.

---

<sup>56</sup> <https://shs.cairn.info>

**Conclusion:**

En conclusion, le mécanisme de fonctionnement du Bitcoin repose sur plusieurs concepts clés qui le distinguent des monnaies traditionnelles. Au cœur de son système se trouve la blockchain, une technologie de registre distribué qui enregistre de manière transparente et immuable toutes les transactions effectuées avec la cryptomonnaie. Les mineurs utilisent leur puissance de calcul pour valider et sécuriser ces transactions, en les regroupant dans des blocs qui sont ensuite ajoutés à la blockchain. Ce processus de validation, appelé preuve de travail, assure la sécurité et l'intégrité du réseau Bitcoin.

La décentralisation est un principe fondamental du Bitcoin, ce qui signifie qu'aucune autorité centrale n'a le contrôle sur le réseau. Au lieu de cela, les règles du Bitcoin sont déterminées par un consensus entre ses utilisateurs. Cela permet une autonomie et une résistance à la censure, mais pose également des défis en termes de sociabilité et de gouvernance.

Le mécanisme de fonctionnement du Bitcoin repose sur une combinaison de technologie avancée, de consensus communautaire et de principes décentralisés, qui ensemble créent un système financier numérique unique et innovant.<sup>57</sup>

---

<sup>57</sup> <https://fr.wikipedia.org>

**Chapitre 03 : l'illustration d'une transaction  
économique et commerciale par le Bitcoin: cas de  
Décathlon**

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

### **Introduction :**

La montée en puissance des crypto monnaies, et en particulier du Bitcoin, a suscité un intérêt croissant dans le monde des affaires et du commerce. Ces monnaies numériques offrent un potentiel révolutionnaire en termes de transactions économiques, avec des implications profondes pour les entreprises de toutes tailles et dans tous les secteurs.

Dans ce chapitre, nous examinerons de près un cas concret illustrant l'utilisation du Bitcoin dans le contexte d'une transaction commerciale.

Dans la première section nous explorerons l'histoire de Décathlon en tant qu'entreprise, Nous examinerons également les principales fonctionnements de décathlon ainsi l'acceptation de bitcoin par les entreprises y compris décathlon, mettant en lumière a l'évolution du cours de bitcoin notamment en matière de réglementation, de sécurité et d'acceptation générale.

Dans la deuxième et la dernière section de notre chapitre, nous nous plongerons dans l'expérience pratique de Décathlon avec le Bitcoin. Nous détaillerons les circonstances qui ont conduit l'entreprise à envisager l'intégration de cette crypto monnaie dans ses opérations commerciales, les défis rencontrés lors de sa mise en œuvre et les résultats obtenus jusqu'à présent.

### **Section 01 : Introduction à Décathlon et la crypto-monnaie**

#### **1. Présentation de Décathlon**

Décathlon est une marque de renommée mondiale spécialisée dans la vente d'équipements sportifs de qualité supérieure. Reconnue pour sa vaste gamme de produits, Décathlon propose des équipements pour tous les sports, adaptés à tous les niveaux de compétence. Vêtements: Utilisez votre carte-cadeau pour acheter des vêtements de sport de qualité.

#### **2. Historique de décathlon<sup>58</sup>**

Le premier magasin Décathlon voit le jour à Lille en 1976. Fondée par Michel Leclercq, un cousin germain de la famille Mulliez, l'enseigne proposait initialement des articles de sport dans dix disciplines, d'où son nom. Elle est à l'origine des marques comme Tribord, Quechua, Inesis, etc.

Décathlon est un distributeur d'articles sportifs détenu majoritairement par la famille Mulliez. Son fondateur, Michel Leclercq et ses héritiers détiennent près de 40% de l'entreprise. Considéré au départ comme un distributeur, Décathlon devient aujourd'hui une véritable

---

<sup>58</sup> <https://www.e-marketing.fr>

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

marque. Au-delà de la commercialisation d'articles de sport, l'enseigne propose d'autres services comme la location, la réparation de matériel, le conseil, etc. Comptant plus de 325 magasins en France, l'entreprise a collaboré avec les plus grands du sport de haut niveau à l'instar de Teddy Riner et Gaël Monfils.

Décathlon : un début mouvementé ; L'histoire de Décathlon commence par un voyage de Michel Leclercq aux États-Unis. Ce dernier remarque les magasins de grande taille destinés exclusivement aux sports. Il constate que le concept est encore inexistant en Europe.

À l'époque, Michel travaillait chez Auchan, l'entreprise de son cousin. Le monde de la grande distribution n'a plus de secret pour lui. Il souhaite répliquer le modèle Auchan au sport.

Dès son retour, Michel et six autres collègues passionnés de Sport décident de lancer leur magasin à Lille, le fief d'Auchan.

Réaliser une opération de naming

Ainsi, il quitte l'entreprise familiale à 35 ans pour fonder sa propre entreprise. Avec ses acolytes, ils souhaitent mettre en pratique un concept : « vendre des articles de sport à un prix compétitif ».

Le premier magasin, ouvert en 1976, rencontre immédiatement le succès. Néanmoins, les prix pratiqués ne sont pas du goût des fournisseurs, Adidas en premier. Seulement un mois après son ouverture, les rayons commencent à se vider. Aucun fournisseur ne souhaite approvisionner le magasin.

Pour contourner ce problème, les approvisionneurs se font passer pour des présidents de clubs pour acheter chez les fournisseurs. En parallèle, Décathlon décide de porter plainte contre Adidas et d'autres marques pour refus de vente.

L'entreprise trouve une solution avec les vélos. Elle décide de prendre des vélos artisanaux et y appose son logo. Constatant le succès de cette politique, Décathlon décide de fabriquer d'autres modèles, cette fois-ci dans une véritable usine.

Dès l'hiver de l'année 1977, les rayons commencent à se remplir puisque l'enseigne obtient gain de cause dans l'affaire l'opposant à ses fournisseurs. Dès le début des années 80, Décathlon peut enfin commencer son développement en ouvrant des magasins sur l'ensemble du territoire.

Décathlon rencontre le succès grâce au vélo

Chez Décathlon, le vélo fait partie de son histoire et lui a permis de conquérir le marché du sport. Au départ, la marque était contrainte de fabriquer son propre vélo à cause des fournisseurs qui rechignent à l'approvisionnement. C'est ainsi que le premier modèle est né

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

dans les années 70. Ce modèle artisanal représente le premier produit ayant porté les couleurs de la marque.

Nicolas Favre, directeur marketing de Team Vitality : "LeSport, c'est la recette magique"

Quarante ans plus tard, l'enseigne est devenue le premier distributeur de vélos en France. La politique reste la même, vendre les produits à un prix abordable. Le prix des vélos ne dépasse pas les 300 euros.

Les vélos sont désormais développés sous la marque B'twin dont le plus grand magasin se trouve à Lille. 130 modèles y sont exposés.

Décathlon : plus de 80 marques développées

L'aventure a commencé par les vélos siglés dans les années 80. Décathlon a ensuite étendu son activité à tous les sports pour devenir un véritable équipementier sportif. Actuellement, l'enseigne recense 80 marques, une par discipline. Orao est dédié au kitesurf, Tribord à la voile, Quechua à la randonnée, Kalenji pour les amateurs de course, Nabaiki pour la natation, etc. Il s'agit du plus grand pôle de design derrière l'automobile.

D'après les estimations, ces marques pèsent 70% sur le chiffre d'affaires du distributeur. Ce chiffre fait grincer les dents des fournisseurs. Certains estiment qu'ils sont utilisés comme un faire-valoir des propres produits de Décathlon. D'autres se demandent si l'enseigne est réellement un distributeur ou un concurrent. Néanmoins, des marques plus puissantes s'accommodent à cette réalité.

Des marques qui s'apparentent à de véritables PME

Contrairement aux idées reçues, les 80 marques de Décathlon n'évoluent pas à son siège à Villeneuve-d'Ascq. Chacune d'entre elles possède leur propre siège, leur équipe R&D et ses chefs de produit.

Ainsi, la plupart des marques ont choisi des sièges éloignés de la maison mère. Tribord, par exemple, se trouve à Hendaye sur la côte atlantique. De son côté, Quechua a élu domicile dans la ville de Sallanches. Caperlan se situe en Gironde. Néanmoins, certaines marques comme Kips ta et Domyos ont préféré demeurer dans le Nord.

Une marque pour chaque discipline

Décathlon n'a jamais caché son objectif de proposer une marque dans chaque discipline sportive. Cette politique s'inscrit dans la philosophie du groupe de proposer des articles à un prix moins cher. En commercialisant ses propres produits, l'enseigne demeure compétitive puisqu'elle contrôle la chaîne de valeur. Pour les experts, le distributeur est devenu le Zara du sport.

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

Décathlon ne rechigne pas à développer ses propres marques en raison de la concurrence d'Amazon. L'enseigne est consciente que le géant américain est imbattable dans la diversité des offres et la livraison. Vendre d'autres marques ne suffit plus, l'enseigne souhaite se différencier. Pour cela, elle s'est muée en équipementier.

En dehors de la France, Décathlon adopte même une politique extrême. Les marques étrangères sont peu représentées aux profits des marques propres. Ce pari risqué a marché puisque l'enseigne a amorcé son internationalisation dès 1986.

Dans les années 90, Décathlon investit les pays européens. À partir des années 2000, la marque part à la conquête de l'Asie. Présente dans plus de 40 pays, elle réalise deux tiers de son chiffre d'affaires à l'étranger. Notons que la Chine est même devenue le deuxième marché de l'enseigne.

Puma célèbre le "Made in France" avec une nouvelle collection

Adidas court en faveur de la préservation des océans .Une crédibilité et légitimité auprès des disciplines moins populaires

Pour Décathlon, assurer une présence dans des disciplines moins populaires est devenu une spécialisation. Prenons l'exemple d'Aptonia, une marque dédiée au triathlon. Cette dernière propose les équipements complets pour pratiquer cette discipline : sacs à dos, combinaisons, produits nutritifs, etc.

Pourtant, le triathlon recense seulement 160 000 pratiquants en France. Cette présence renforce la crédibilité de Décathlon dans le domaine du sport. La marque a compris qu'il était difficile de rivaliser avec Adidas et Nike dans une discipline comme le football ou le basket, elle a préféré séduire les sportifs dans d'autres disciplines.

Développer ses propres marques n'est pas toujours un pari réussi. Go Sport, une autre enseigne sportive en a payé les frais. Elle peine à suivre ses concurrents, dont Décathlon sur le marché. De son côté, Sport 2000, le distributeur sportif allemand préfère commercialiser exclusivement de grandes marques.

L'innovation au cœur de son succès

Pour accompagner ses marques dans le domaine de l'innovation, l'enseigne a mis en place le « Sports ab ». Le laboratoire existe depuis vingt ans et se trouve dans son siège à Villeneuve d'Ascq.

Consacré à la recherche et développement, le laboratoire emploie une cinquantaine de chercheurs dans des domaines comme la science sensorielle, la biomécanique, etc. Les ingénieurs travaillent dans un local de plus de 1500 m<sup>2</sup> pour tester les futurs produits.

Les secrets de la réussite chez Décathlon

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

Après plus de 40 ans d'existence, Décathlon est restée pendant des années l'enseigne préférée des Français. Au-delà de ses prix défiant toute concurrence, la marque doit sa réussite à d'autres facteurs.

La diversité des produits proposés fait la force de l'enseigne. Les consommateurs y trouvent des produits à la fois ludiques et innovants. Près de 100 000 références sont en vente chez Décathlon, certaines en magasin et d'autres en ligne. Ce chiffre inclut les références de la Marketplace. Par ailleurs, près de 500 marques internationales sont représentées ainsi que 80 marques propres.

L'enseigne ne ménage pas son effort dans le service client. Dans les magasins, les vendeurs sont de véritables passionnés et amateurs de sport. Les consommateurs se trouvent ainsi entre de bonnes mains avec un vendeur qui maîtrise son sujet. D'ailleurs, plusieurs athlètes de haut niveau travaillent pour l'entreprise lorsqu'ils ne participent pas à une compétition internationale.

Développer ses propres marques permet également à Décathlon de dégager une marge plus importante. En effet, distribuer sa propre marque offre la possibilité de proposer les produits à un prix inférieur à celui des concurrents.

L'innovation se trouve au cœur de l'enseigne. Son centre de recherche et développement « Corporate Décathlon » dépose des brevets régulièrement. Les produits sont directement testés par des clients sélectionnés.

Décathlon : chiffres et résultats en 2022

En 2022, le chiffre d'affaires de Décathlon en France s'élève à 4,7 milliards d'euros, soit une hausse de 12% par rapport à l'année précédente. Pour les dirigeants, il s'agit d'une année de retrouvailles avec les clients. Par ailleurs, le marché du sport connaît un dynamisme en raison des compétitions sportives internationales. La période motive les gens à faire du sport.

Le e-commerce gagne du terrain puisqu'il pèse désormais 15% sur les ventes. Ce chiffre a augmenté de 135% par rapport à 2019. De leur côté, les chiffres stagnent dans les 325 magasins physiques qui se trouvent en France.

La vente de seconde main, une nouvelle politique de la marque gagne en popularité. Plus de 300 000 produits de cette catégorie sont écoulés en 2022. De son côté, la location a généré plus de 21 600 abonnements.

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

### **3. Fonctionnement de décathlon<sup>59</sup>**

La fonction principale de Décathlon est de proposer une large gamme d'articles de sport et d'équipements pour différents types d'activités sportives telle que

Chaussures: Des chaussures pour tous les sports sont disponibles.

Matériel de sport: Que ce soit pour le football, le cyclisme, la randonnée ou tout autre sport, Décathlon a ce qu'il vous faut.

Accessoires: Des accessoires pour améliorer vos performances sportives sont aussi disponibles.

### **4. Avantage et défis d'utilisation du bitcoin par Décathlon**

#### **4.1. Avantages<sup>60</sup>**

Financement alternatif : Les ICO offrent une alternative aux méthodes traditionnelles de levée de fonds pour les entreprises, permettant à quiconque de soutenir un projet en investissant des cryptomonnaies.

Accessibilité : Les ICO sont ouvertes à un large éventail d'investisseurs, ce qui permet à des individus du monde entier de participer à des projets qu'ils trouvent prometteurs, sans les restrictions des marchés traditionnels.

Transparence et engagement : Les entreprises utilisant des ICO sont tenues de fournir un whitepaper détaillé exposant leur projet, leur équipe et leurs objectifs. Cela favorise la transparence et permet aux investisseurs de prendre des décisions éclairées.

Potentiel de rendement : Comme pour tout investissement, les participants aux ICO ont la possibilité de réaliser des gains importants si la valeur des jetons augmente après l'ICO.

#### **4.2. Inconvénients :**

Risque élevé : Les ICO sont des investissements spéculatifs avec un risque élevé de perte totale de l'investissement. De nombreux projets ICO échouent, et il peut être difficile de distinguer les projets légitimes des arnaques.

Manque de régulation : Les ICO sont largement non réglementées, ce qui expose les investisseurs à des risques de fraude et de manipulation du marché.

Volatilité : La valeur des jetons émis lors d'une ICO peut être extrêmement volatile, ce qui rend difficile la prévision des rendements futurs.

Protection insuffisante des investisseurs : En raison du manque de régulation, les investisseurs peuvent avoir peu ou pas de recours en cas de fraude ou de perte d'investissement.

---

<sup>59</sup> <https://engagements.decathlon.fr>

<sup>60</sup> <http://www.murielle-cahen.fr>

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

### **5. évolution de l'acceptation du bitcoin par les entreprises y compris Décathlon**

Décathlon est l'un des détaillants d'articles de sport les plus populaires et les plus importants, basé en France. Actuellement, il possède environ 1000 magasins dans 30 pays à travers le monde. Elle est considérée comme la plus grande organisation au monde en matière d'articles de sport. La société a vu le jour en 1976 et, à ce jour, elle propose plus de 35 000 produits différents. Si vous souhaitez acheter des produits Décathlon de haute qualité et d'un bon rapport qualité-prix, la meilleure solution est d'opter pour des cartes cadeaux Décathlon. En effet, de cette façon, vous n'aurez pas besoin d'associer vos informations de paiement où que ce soit. Vous pouvez acheter vos cartes-cadeaux Décathlon sur Coinsbee même avec votre crypto-monnaie.

Oui, vous avez bien entendu. Coinsbee vous permet d'acheter des cartes-cadeaux Décathlon avec plus de 200 crypto-monnaies différentes, notamment Bitcoin, Litecoin, Dogecoin, Bitcoin Cash, Ethereum, et plus encore.

### **6. Evolution du cours de bitcoin depuis sa création à ce jour (2009-2024)**

Tableau : Evolution du cours de bitcoin depuis sa création à ce jour (2009-2024)

2009	<ul style="list-style-type: none"><li>• Lancement du Bitcoin le 3 janvier 2009 avec un prix initial de 0 USD.</li><li>• Le prix reste relativement stable autour de 0 USD pendant les premiers mois.</li><li>• Décembre 2009 : Premier échange connu de Bitcoin, 1 000 BTC échangés contre 50 USD.</li></ul>
2010	<ul style="list-style-type: none"><li>• Le prix commence à fluctuer, atteignant un pic de 0,39 USD en juillet 2010.</li><li>• Premier crash en novembre 2010, le prix tombe à 0,06 USD.</li></ul>
2011	<ul style="list-style-type: none"><li>• Année de forte croissance, le prix atteint un pic de 32 USD en avril 2011.</li><li>• Premier "bull run" suivi d'un crash en novembre 2011, le prix retombe à 2 USD.</li></ul>
2012	<ul style="list-style-type: none"><li>• Relativement stable autour de 10 USD.</li></ul>
2013	<ul style="list-style-type: none"><li>• Deuxième "bull run" majeur, le prix atteint un pic de 1 242 USD en novembre 2013.</li></ul>

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

	<ul style="list-style-type: none"><li>•Crash en décembre 2013, le prix retombe à 600 USD.</li></ul>
2014	<ul style="list-style-type: none"><li>•Année de baisse, le prix oscille entre 300 et 800 USD.</li></ul>
2015	<ul style="list-style-type: none"><li>•Relativement stable autour de 200 USD.</li></ul>
2016	<ul style="list-style-type: none"><li>•Légère hausse, le prix atteint un pic de 900 USD en novembre 2016.</li></ul>
2017	<ul style="list-style-type: none"><li>•Année record, le prix explose, passant de 900 USD à 20 000 USD en décembre 2017.</li><li>•"Bull run" historique alimenté par une spéculation croissante.</li></ul>
2018	<ul style="list-style-type: none"><li>•Année de "bearmarket", le prix chute de 20 000 USD à 3 200 USD en décembre 2018.</li></ul>
2019	<ul style="list-style-type: none"><li>•Légère reprise, le prix atteint un pic de 13 800 USD en juin 2019.</li></ul>
2020	<ul style="list-style-type: none"><li>•Année de croissance importante, le prix atteint un pic de 29 000 USD en décembre 2020.</li></ul>
2021	<ul style="list-style-type: none"><li>•Année record, le prix atteint un pic historique de 68 789 USD en novembre 2021.</li><li>•"Bull run" alimenté par l'adoption croissante du Bitcoin par les institutions et les investisseurs particuliers.</li></ul>
2022	<ul style="list-style-type: none"><li>•Année de baisse importante, le prix chute à 17 000 USD en juin 2022.</li><li>•"Bearmarket" causé par divers facteurs, dont le resserrement monétaire de la Fed et l'incertitude économique mondiale.</li></ul>
2023	<ul style="list-style-type: none"><li>•Légère reprise, le prix atteint un pic de 25 000 USD en août 2023.</li></ul>
2024(jusqu'à 01 juin)	<ul style="list-style-type: none"><li>•Le prix est actuellement autour de 23 000 USD.</li></ul>

Sources : JDN ([journalduner.fr](http://journalduner.fr)) et bitcoin ([bitcoin.fr](http://bitcoin.fr))

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

Il est important de noter que l'évolution du cours du Bitcoin est très volatile et peut subir des Fluctuations importantes sur de courtes périodes.

### **Section 02 : Adoption de Bitcoin comme moyen de paiement par une entreprise en ligne**

#### 1. Contexte :

Une entreprise de commerce électronique spécialisée dans la vente de produits électroniques décide d'adopter Bitcoin comme moyen de paiement pour ses clients. Cette décision est motivée par plusieurs facteurs, notamment la demande croissante des clients pour des options de paiement alternatives, la réduction des frais de transaction et l'attrait pour l'aspect novateur de la technologie blockchain.

#### 2. Étapes du processus :

Intégration du système de paiement Bitcoin : L'entreprise engage un développeur ou utilise un service tiers pour intégrer un système de paiement Bitcoin à son site web de commerce électronique. Cela permettra aux clients de choisir Bitcoin comme option de paiement lors du processus d'achat.

#### 3. Communication avec les clients :

L'entreprise informe ses clients de l'ajout de Bitcoin comme option de paiement via différents canaux de communication, tels que les réseaux sociaux, les newsletters et les annonces sur son site web. Elle explique également les avantages de l'utilisation de Bitcoin, tels que la sécurité, la rapidité des transactions et la réduction des frais de transaction.

Formation du personnel : Le personnel de l'entreprise, y compris le service clientèle, est formé sur les bases du Bitcoin, du processus de paiement et sur la manière d'aider les clients qui choisissent cette option de paiement.

#### 4. Exécution des transactions Bitcoin :

Lorsqu'un client choisit de payer avec Bitcoin, le système de paiement de l'entreprise génère une adresse Bitcoin unique pour cette transaction. Le client envoie alors le montant requis depuis son portefeuille Bitcoin vers cette adresse.

#### 5. Confirmation de la transaction :

Une fois que la transaction Bitcoin est confirmée sur le réseau, l'entreprise reçoit une notification et peut traiter la commande du client. Comme pour les autres modes de paiement, l'entreprise attend que la transaction soit confirmée pour expédier les produits.

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

### 6. Suivi et support :

L'entreprise assure un suivi régulier des transactions Bitcoin et offre un support clientèle pour résoudre tout problème ou questionnement lié au processus de paiement.

Résultats attendus :

### 7. Augmentation des ventes :

L'adoption de Bitcoin comme option de paiement pourrait attirer de nouveaux clients et fidéliser les clients existants qui préfèrent utiliser cette monnaie virtuelle.

### 8. Réduction des frais de transaction :

En utilisant Bitcoin, l'entreprise peut réduire les frais de transaction associés aux méthodes de paiement traditionnelles telles que les cartes de crédit.

### 9. Image de marque innovante :

En adoptant une technologie émergente comme Bitcoin, l'entreprise renforce son image de marque en tant que pionnière dans son secteur.

Ce cas pratique illustre comment une entreprise peut intégrer Bitcoin comme moyen de paiement dans ses opérations commerciales, les étapes à suivre et les résultats attendus

## **Section 03 : étude de cas : Décathlon et son expérience avec le bitcoin**

### **1. Cas pratique : Adoption de Bitcoin comme moyen de paiement par une entreprise**

#### 1.1. Contexte :

Une entreprise de commerce électronique spécialisée dans la vente de produits électroniques décide d'adopter Bitcoin comme moyen de paiement pour ses clients. Cette décision est motivée par plusieurs facteurs, notamment la demande croissante des clients pour des options de paiement alternatives, la réduction des frais de transaction et l'attrait pour l'aspect novateur de la technologie blockchain.

#### 1.2. Étapes du processus :

Intégration du système de paiement Bitcoin : L'entreprise engage un développeur ou utilise un service tiers pour intégrer un système de paiement Bitcoin à son site web de commerce électronique. Cela permettra aux clients de choisir Bitcoin comme option de paiement lors du processus d'achat.

#### 1.3. Communication avec les clients :

L'entreprise informe ses clients de l'ajout de Bitcoin comme option de paiement via différents canaux de communication, tels que les réseaux sociaux, les newsletters et les annonces sur

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

son site web. Elle explique également les avantages de l'utilisation de Bitcoin, tels que la sécurité, la rapidité des transactions et la réduction des frais de transaction.

### 1.4. Formation du personnel :

Le personnel de l'entreprise, y compris le service clientèle, est formé sur les bases du Bitcoin, du processus de paiement et sur la manière d'aider les clients qui choisissent cette option de paiement.

### 1.5. Exécution des transactions Bitcoin :

Lorsqu'un client choisit de payer avec Bitcoin, le système de paiement de l'entreprise génère une adresse Bitcoin unique pour cette transaction. Le client envoie alors le montant requis depuis son portefeuille Bitcoin vers cette adresse.

### 1.6. Confirmation de la transaction :

Une fois que la transaction Bitcoin est confirmée sur le réseau, l'entreprise reçoit une notification et peut traiter la commande du client. Comme pour les autres modes de paiement, l'entreprise attend que la transaction soit confirmée pour expédier les produits.

### 1.7. Suivi et support :

L'entreprise assure un suivi régulier des transactions Bitcoin et offre un support clientèle pour résoudre tout problème ou questionnement lié au processus de paiement.

### 1.8. Résultats attendus :

#### 1.8.1. Augmentation des ventes :

L'adoption de Bitcoin comme option de paiement pourrait attirer de nouveaux clients et fidéliser les clients existants qui préfèrent utiliser cette monnaie virtuelle.

#### 1.8.2. Réduction des frais de transaction :

En utilisant Bitcoin, l'entreprise peut réduire les frais de transaction associés aux méthodes de paiement traditionnelles telles que les cartes de crédit.

#### 1.8.3. Image de marque innovante :

En adoptant une technologie émergente comme Bitcoin, l'entreprise renforce son image de marque en tant que pionnière dans son secteur.

Ce cas pratique illustre comment une entreprise peut intégrer Bitcoin comme moyen de paiement dans ses opérations commerciales, les étapes à suivre et les résultats attendus

### **Cas pratique : Adoption de Bitcoin par Décathlon**

Ce rapport vise à examiner la question de l'adoption de Bitcoin par Décathlon en tant que moyen de paiement. L'objectif est de fournir une analyse approfondie des implications, des défis et des avantages potentiels associés à cette décision. En examinant le contexte du

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

commerce de détail et du fonctionnement de Bitcoin, ce rapport offre des recommandations pratiques à l'entreprise pour une éventuelle adoption réussie de cette crypto-monnaie.

Contexte :

L'Adoption de Bitcoin dans le Domaine du Commerce

Le contexte de l'adoption de Bitcoin dans le domaine du commerce est complexe, comprenant des facteurs tels que la volatilité du marché des crypto-monnaies, les tendances de consommation changeantes et les défis réglementaires. De plus, l'évolution rapide des technologies de paiement nécessite une évaluation approfondie de l'opportunité d'intégrer Bitcoin dans les options de paiement de Décathlon. Comprendre ces facteurs est essentiel pour une étude approfondie de l'adoption de Bitcoin par l'entreprise

Décathlon, une grande chaîne de magasins spécialisée dans la vente d'articles de sport, décide d'explorer de nouvelles options de paiement pour répondre aux besoins de sa clientèle diversifiée et à l'évolution des tendances technologiques. En réponse à la demande croissante de certains clients pour des méthodes de paiement alternatives, ainsi que pour capitaliser sur l'aspect innovant de la technologie blockchain, Décathlon décide d'adopter Bitcoin comme moyen de paiement dans certains de ses magasins en ligne

Objectifs et Portée de l'Étude

L'objectif principal de cette étude est d'évaluer les motivations, les défis et les risques potentiels associés à l'adoption de Bitcoin par Décathlon. La portée de l'étude englobe une analyse approfondie du fonctionnement de Bitcoin, des tendances actuelles dans le commerce de détail, ainsi que des implications légales et réglementaires de l'utilisation de cette crypto-monnaie. Les recommandations formulées visent à fournir à Décathlon une base solide pour prendre une décision éclairée concernant l'adoption de Bitcoin comme moyen de paiement.

Étapes du processus :

Intégration du système de paiement Bitcoin : Décathlon engage une équipe de développeurs spécialisés dans les technologies blockchain pour intégrer un système de paiement Bitcoin à son site web de vente en ligne. Cette équipe travaille en étroite collaboration avec les équipes informatiques internes de Décathlon pour s'assurer que l'intégration se déroule de manière

fluide et sécurisée.

Communication avec les clients : Décathlon lance une campagne de communication multicanale pour informer ses clients de l'ajout de Bitcoin comme option de paiement. Cette campagne comprend des annonces sur le site web de Décathlon, des publications sur les réseaux sociaux, des newsletters envoyées aux abonnés, ainsi que des affiches dans les

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

magasins physiques. Décathlon explique également les avantages de l'utilisation de Bitcoin, notamment la sécurité, la rapidité des transactions et la réduction des frais de transaction

**Formation du personnel :** Les employés de Décathlon, notamment ceux travaillant dans les centres d'appels et les magasins physiques, reçoivent une formation approfondie sur les bases du Bitcoin, le processus de paiement et sur la manière d'aider les clients qui choisissent cette option de paiement. Décathlon veille à ce que son personnel soit bien informé et en mesure d'assister les clients tout au long du processus d'achat.

**Exécution des transactions Bitcoin :** Lorsqu'un client choisit de payer avec Bitcoin lors de son achat en ligne, le système de paiement de Décathlon génère automatiquement une adresse Bitcoin unique pour cette transaction. Le client utilise alors son portefeuille Bitcoin pour envoyer le montant requis à cette adresse.

**Confirmation de la transaction :** Une fois que la transaction Bitcoin est confirmée sur le réseau, Décathlon reçoit une notification et peut traiter la commande du client. Comme pour les autres modes de paiement, Décathlon attend que la transaction soit confirmée avant d'expédier les produits.

**Suivi et support :** Décathlon assure un suivi régulier des transactions Bitcoin et offre un support clientèle dédié pour résoudre tout problème ou questionnement lié au processus de paiement. Le service clientèle de Décathlon est disponible pour répondre aux questions des clients et les guider tout au long de leur expérience d'achat avec Bitcoin.

**Résultats attendus :**

**Augmentation des ventes :** L'adoption de Bitcoin comme option de paiement pourrait attirer de nouveaux clients vers Décathlon, notamment ceux qui préfèrent utiliser cette monnaie virtuelle pour leurs achats en ligne. De plus, cela pourrait fidéliser les clients existants qui apprécient la possibilité d'utiliser Bitcoin comme méthode de paiement.

**Réduction des frais de transaction :** En acceptant Bitcoin, Décathlon peut réduire les frais de transaction associés aux méthodes de paiement traditionnelles telles que les cartes de crédit et les virements bancaires internationaux.

**Image de marque innovante :** En adoptant une technologie émergente comme Bitcoin, Décathlon renforce son image de marque en tant qu'entreprise innovante et à la pointe de la technologie. Cela pourrait attirer l'attention des médias et susciter l'intérêt des consommateurs pour Décathlon en tant que pionnier dans son secteur

## L'ILLUSTRATION D'UNE TRANSACTION ECONOMIQUE ET COMMERCIALE PAR LE BITCOIN : CAS DE DECATHLON

En suivant ces étapes, Décathlon peut intégrer avec succès Bitcoin comme moyen de paiement dans ses opérations commerciales en ligne, offrant ainsi à ses clients une nouvelle option de paiement tout en renforçant son positionnement sur le marché.

### **Conclusion :**

En conclusion, l'exploration de l'utilisation du Bitcoin par Décathlon dans le cadre de transactions commerciales met en lumière les défis et les opportunités associés à l'adoption des crypto monnaies par les entreprises. À travers cette étude de cas, nous avons observé comment Décathlon, en tant qu'acteur majeur du commerce de détail, a navigué à travers les complexités réglementaires, les considérations de sécurité et les fluctuations de la valeur du Bitcoin. Bien que cette initiative ait présenté des défis techniques et opérationnels, elle a également ouvert de nouvelles perspectives en matière de transactions internationales et de diversification des méthodes de paiement. En définitive, l'expérience de Décathlon avec le Bitcoin illustre un potentiel transformateur pour le secteur du commerce, incitant d'autres entreprises à réfléchir à l'intégration de ces technologies émergentes dans leurs stratégies commerciales futures.

## **Conclusion générale**

## Conclusion générale

L'étude des crypto-monnaies représente un domaine de recherche complexe et en évolution constante. Les avancées technologiques, notamment l'avènement d'Internet, ont donné naissance à cette nouvelle forme de monnaie, souvent désignée sous divers noms tels que monnaie virtuelle, digitale ou crypto-monnaie. Fondées sur des protocoles cryptographiques de pair à pair, ces monnaies électroniques se distinguent par leur caractère privé, numérique et décentralisé, bouleversant ainsi les paradigmes traditionnels de la monnaie.

Cette émergence a suscité un vif intérêt et alimenté un débat animé quant à la reconnaissance des crypto-monnaies en tant que véritables formes de monnaie. Ce débat repose largement sur la capacité de ces monnaies à remplir les trois fonctions fondamentales de la monnaie : servir de moyen d'échange, d'unité de compte et de réserve de valeur. D'échange car certains magasins ou commerçants les acceptent comme moyen de payer les transactions. Mais cette crypto-monnaie n'est pas parvenue à se placer sur un pied d'égalité avec les devises traditionnelles car le prix, par exemple, est encore souvent exprimé en devise de référence (dollar, euro). Comme le dit la Banque Nationale de Belgique (BNB), "il n'existe pas pour l'argent virtuel de garantie légale qu'il puisse être échangé directement à sa valeur initiale"<sup>61</sup>

Cependant, leur forte volatilité, leur manque de stabilité en tant qu'unité de compte et leur nature spéculative remettent en question leur aptitude à remplir ces fonctions. Les positions des autorités monétaires internationales reflètent cette incertitude, allant de la considération des crypto-monnaies comme des bulles spéculatives à leur potentiel en tant que monnaies émergentes.

Malgré ces défis, certains économistes envisagent un avenir où les crypto-monnaies pourraient évoluer vers des formes de monnaie légitimes. Cependant, il est clair que cela nécessitera une stabilisation du cours et une adoption plus large pour que leur qualité monétaire se renforce. La crypto-monnaie, à la tête Bitcoin, a, dans une faible mesure, réussi à servir comme moyen de paiement.

---

<sup>61</sup>Charlotte de Montpellier, " Le Bitcoin est-il vraiment une monnaie ?", publié le 28/05/2019 consulté en ligne sur ([www.ing.be](http://www.ing.be))

Cette définition de l'économiste français Pascale Salin dans son ouvrage les systèmes monétaires implique que "la monnaie peut être échangée contre n'importe quoi, à n'importe quel moment et auprès de n'importe qui"<sup>62</sup>.

En conclusion, bien que les crypto-monnaies représentent une innovation majeure dans le domaine monétaire, leur statut et leur potentiel restent sujets à débat. Leur évolution future dépendra de divers facteurs, notamment de leur capacité à surmonter les défis actuels et à gagner en légitimité dans l'économie mondiale.

Les difficultés rencontrées (les limites)

Comme tous les travaux de recherche, le mien contient un certains nombre de limites, nous citons essentiellement :

Difficulté du sujet : La première difficulté majeure que nous avons rencontrée dans ce travail a été celle de travailler sur un sujet récent et peu connu, ou pas du tout surtout en Algérie. Le Bitcoin a été créé en 2009 et n'a réellement commencé à être connu qu'à partir de 2012 ou 2013. La littérature académique sur le sujet est donc encore peu abondante et peu variée, même inexistante en Algérie. Il m'a été difficile de trouver le nombre demandé minimum d'articles académiques, mais surtout de livres. Très peu d'ouvrages sont encore consacrés à ce sujet, la plupart ne l'évoquent qu'au cours d'un chapitre ou de quelques paragraphes. La recherche d'informations nouvelles a donc été minutieuse. Elle consistait la plupart du temps à cibler la petite information spécifique à un article parmi ses multiples pages, qui apportait un point supplémentaire à l'ensemble des connaissances déjà accumulées.

Ecueil de la répétition : tout au long de ce mémoire il m'a été difficile de ne pas tomber dans le piège de la répétition. En effet, certaines informations recueillies dans l'analyse des articles académiques pouvaient parfois apporter un élément de réponse à une de mes hypothèses.

Un peu de technique dans le travail de recherche : Nous ne pouvons pas éluder un peu de technique ou de science dans notre travail sachant que la crypto-monnaie en générale et le bitcoin en particulier, chef d'œuvre d'agencement de plusieurs idées, n'est pas proprement dit une révolution scientifique. Donc des explications techniques et un peu de vocabulaire, juste ce qu'il faut, sont nécessaires pour comprendre l'écosystème de ce nouveau né avant de toute réflexion et de critique.

La stratégie de recherche adoptée s'appuyant uniquement sur l'étude théorique.

---

<sup>62</sup>En ligne sur ([www.usbeketrica.com](http://www.usbeketrica.com)) publié le 07/01/2019

Vu la nouveauté du sujet et de par le caractère innovant de la crypto-monnaie, il n'existe pas de situation empirique spécifique à étudier puisque la tendance de cette monnaie est globale. A la fin de ce travail de recherche, notre mérite est que nous avons pu aborder, traiter et analyser le sujet de manière approprié, claire, et pu également apporter des éclaircissements concernant une forme de monnaie inédite. Bien que ce soit encore un thème qui demande encore d'autres investigations qui laisse la porte ouverte à de plus ample travaux de recherche afin d'aborder des points qui n'ont pas fait l'objet de la présente étude mais également de confirmer ou infirmer nos premiers résultats. Nous espérons que ce travail soit utile et pratique et d'une importance qui permettra aux autres de connaître au mieux la crypto-monnaie.

## **Références bibliographiques**

## Références bibliographiques:

### 1. Ouvrages

- Erwan JONCHERES, «Encadrement juridique des monnaie numérique » mémoire présenté à la faculté de Droit de l'Université de Montréal, en vue de l'obtention du grade LL.M, Maitrise en droit des technologies de l'information
- Enée Bussac, "Bitcoin, Ether & Cie : guide pratique pour comprendre, anticipé et investir.", Dunod
- Jean-Pierre Landau, Alban Genais, Op.cit.
- Daniel Ichbiah, Jean-Martial Lefranc, Op.cit
- Gilles Quoistiaux, "Bitcoin et crypto-monnaie", Edition MARGADA, Bruxelles, 2019.

### 2. Revues périodiques et rapport

- Jean-Pierre Landau, Alban Genais, "Les crypto-monnaies" Rapport au ministre de l'Economie et des Finances, du 04/07/2018, en ligne sur (<http://www.ladocumentationfrançaise.fr>)
- Ressource Electronique, en ligne sur (<http://www.cryptoactu.com>)
- David Chaum, "Blind signatures for Untraceable payments",1983, en ligne, consulté sur ([www.taler.net](http://www.taler.net)) le10/04/2024.
- Site internet e-Gold en ligne ([www.e-gold.com](http://www.e-gold.com)) consulté le 10/04/2024.
- Cypherpunks (mot-valise composé à partir des mots anglais cipher : chiffrement, et punk sur le modèle de cyberpunk) forment un groupe informel de personnes intéressées par la cryptographie. Leur objectif est d'assurer le respect de la vie privée par l'utilisation proactive de la cryptographie
- B-money : était l'une des premières propositions de Wei Dai pour un système de paiement électronique anonyme et distribué. En ligne sur ([en.bitcoin.it](http://en.bitcoin.it)) consulté le 10/04/2024.
- Preuve de travail ou en anglais "proof of work", est un des concepts les plus important en, ce qui concerne le chiffrement, et plus particulièrement celui des monnaies numériques. On demande à l'ordinateur d'effectuer une tâche qui nécessite de la puissance de calcul afin de créer la preuve de travail (Son fonctionnement et son utilité seront expliqués par la suite).
- Peer-to-Peer ou pair à pair est l'un des principes de fonctionnement des crypto-monnaies (principe expliqué dans les sections qui suivent.)
- Un coin (littéralement pièce de monnaie) est une monnaie cryptographique, toujours lié à une plateforme ou système où cette monnaie sert de moyen de paiement, le bitcoin par exemple.

-Directive LCB-FT (Lutte Contre le Blanchiment et Financement du Terrorisme) est une directive du parlement européen relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou de financement du terrorisme.

-La directive MiCA : un encadrement renforcé des plateformes de crypto-monnaies

La directive MiCA (Markets in Crypto-Assets) vise à encadrer les activités liées aux crypto-monnaies, notamment celles des plateformes d'échange et de conservation.

-Banque de France, Focus, Op.cit.

-Les Echos.fr, "comprendre la blockchain en 5 points" publié le 19/01/2016, consulté sur ([lesechos.fr](http://lesechos.fr)) le 20/04/2024.

-WIKIPEDIA, Op.cit consulté le 20/04/2024.

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

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

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

-En ligne sur ([www.usbetrice.com](http://www.usbetrice.com)) publié le 07/01/2019

### **3. thèses et mémoires**

-Mme Sidhoum, mémoire, « la crypto-monnaie : Emergence, enjeux et perspectives » Université UMMTO de Tizi Ouzou, promotion 2018-2019

### **4. Sites internet**

<https://www.cointribune.com/minage-bitcoin-comment-ca-marche-vraiment/>

<https://fr.cointelegraph.com/news/solo-bitcoin-miner-solves-valid-block-post-halving>

<https://www.e-marketing.fr>

<http://WWW.murielle-cahen.fr>

<https://n26.com/fr/blog/definitioncryptomonnaie#:~:text=Les%20cryptomonnaies%20sont%20des%20monnaies,le%20fonctionnement%20de%20la%20finance>

<http://www.ladocumentationfrançaise.fr>

<http://www.cryptoactu.com>

# **Annexes**

**Annexes :**

**Annexes N 01 : l'évolution des cours du bitcoin depuis sa naissance a nos jours (2009-2024)**

+

## Les montagnes russes du Bitcoin

Évolution du cours du Bitcoin depuis janvier 2020, en dollars US



En date du 5 mars. Valeurs quotidiennes à la clôture.  
Source : Coingecko



statista

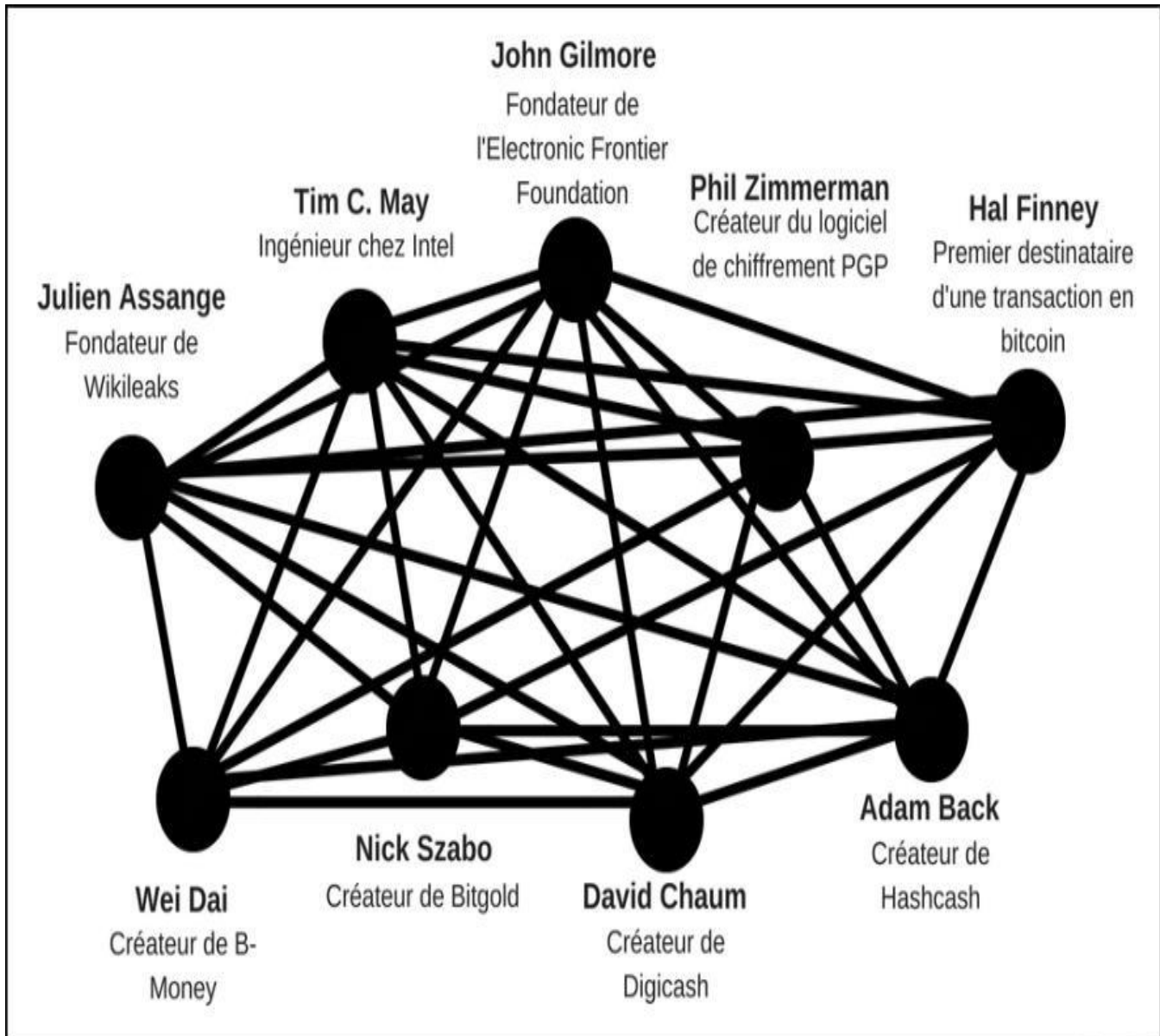


## Annexe N° 02 : La Distribution Globale De Nœuds dans le Monde entier

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

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

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



Source: <http://www.bitcoin.org>

**Listes des figures :**

Figure 01 : Le Principe De La Cryptographie Asymétrique

**Liste des tableaux :**

Tableau N 01 : La puissance de calcul du réseau se mesure actuellement en ExaHash par seconde (EH/s).

Tableau N°02 : Une synthèse des trois piliers de la stratégie de lutte, proposée, contre les Risque des crypto-monnaie

# Lexique

## **Lexique:**

### **A**

**Algorithme de consensus** : protocole par lequel les nœuds d'un réseau blockchain arrivent à un consensus pour valider les transactions ou d'autres engagements sur la chaîne de blocs.

Les algorithmes de consensus les plus souvent employés sont Pow (preuve de travail) et Pos (preuve d'enjeu).

**Altcoin** : crypto-monnaie alternative, un autre coin que le bitcoin.

### **B**

**BCE** : la Banque Centrale Européenne regroupe les 19 pays de l'Union européenne utilisant l'euro

**Bloc** : composant principal de la blockchain, un bloc est un regroupement de plusieurs transactions effectuées par les utilisateurs du réseau. Dans le cas de Bitcoin, la création d'un nouveau bloc est faite par les mineurs qui résolvent des calculs compliqués et vérifient les transactions du bloc.

**Blockchain publique** : une Blockchain publique suit un mode de gouvernance décentralisé, l'intégrité de la donnée étant garantie par les nœuds qui la conservent et les mineurs qui la valident

**Blockchain à consortium** : ce type de Blockchain se situe sur la limite entre chaînes publiques et privées, combinant des éléments des deux côtés. La différence la plus notable par rapport à chaque système peut être observée au niveau du consensus. Au lieu d'un système ouvert où n'importe qui peut valider des blocs ou d'un système fermé où seule une seule entité nomme les producteurs de blocs, une chaîne à consortium comporte une poignée de parties équitablement puissantes qui fonctionnent simultanément en tant que validateurs

**Bull Run** : période de temps durant laquelle les marchés des crypto monnaies connaissent un fort moment haussier, constituant ainsi une opportunité de faire des bénéfices

### **C**

**Clé privé** : La clé privé est comparable à un code PIN : elle est gardée secrète et permet de signer des transactions et transférer des crypto monnaies. Grace à la clé privée, on peut calculer la clé publique (l'inverse n'est pas possible)

**Clé publique** : cette clé permet de calculer l'adresse

**Cryptographie** : c'est l'art de chiffrer des informations pour les rendre inintelligibles sauf à ceux qui ont la clé pour la décoder

**Cypherpunk** : Composé à partir de deux mots anglais que sont « cipher » (ou cypher) signifiant chiffrement et « punk » désignant un esprit rebelle, les cypherpunks forment un groupe informel de personnes intéressées par la cryptographie. Leur objectif est d'assurer le respect de la vie privée par l'utilisation proactive de la cryptographie

## **E**

**Ethereum** : protocole d'échanges décentralisés permettant la création par les utilisateurs de contrats intelligents « Smart-Contracts ». L'Ethereum utilise une unité de compte dénommée Ether comme moyen de paiement de ces contrats. L'Ethereum est la deuxième plus importante crypto monnaie avec une capitalisation supérieure à 448 milliards d'euros en octobre 2021

## **H**

**Hachage** : le hachage cryptographique génère une chaîne de caractères de longueur fixe à partir d'un ensemble de données de n'importe quel volume. Cet ensemble de données peut être un mot, une phrase, un texte plus long ou un fichier entier. Le hachage cryptographique peut être utilisé à des fins de sécurité. Il transforme un input de données aléatoire (clés) en une chaîne d'octets de longueur et de structure fixes (valeur de hachage). Le hash d'une transaction facilite l'identification de cette dernière sur la Blockchain

**Hashcash** : système de preuve de travail (POW – Proof of Work – voir définition ci-dessous) conçu pour limiter le spam et les dénis de service, et plus récemment est connu pour son utilisation dans le Bitcoin

## **L**

**Livre blanc du Bitcoin** : article scientifique technique qui établit les bases théoriques de la structure du réseau de Bitcoin. Le livre blanc est composé de neuf pages

## **M**

**MiCA** : « Markets in Crypto-Assets » - le projet de règlement européen a pour but de réguler les acteurs du marché des crypto monnaies

## **N**

**Noeuds** : points de connexion au réseau

## **P**

**Pairs** : point de connexion égaux

**Peer-to-Peer ou Pair-à-Pair** : permet à plusieurs ordinateurs ou nœuds de communiquer via un réseau, en y partageant des simplement et directement des informations. La singularité des systèmes Peer-to-Peer réside dans le fait que les données peuvent être transférées directement entre les deux nœuds connectés au réseau, sans transiter par un serveur central

**POS** : « Proof of stake » ou preuve d'enjeu accorde généralement, selon un système de tirage aléatoire pondéré, le droit de créer le prochain bloc à un validateur actif sur le réseau ayant mis en dépôt des unités de la crypto monnaie de la Blockchain. Avec le POS, les possibilités d'attribution de nouvelles pièces ne se mesurent pas en fonction de la performance de travail, mais en fonction du «stake» personnel, c'est-à-dire de la part actuelle dans la crypto monnaie correspondante. Ainsi, plus une personne possède des pièces, plus elle a des chances d'être sélectionné aléatoirement pour valider des transactions

**POW** : « Proof of work » ou preuve de travail – Une blockchain utilisant la POW fait appel à des mineurs pour vérifier les données entrantes sur le registre, valider l'authenticité des transactions et créer de nouveaux blocs. Pour récompenser l'ensemble des mineurs pour leur travail, la preuve de travail doit établir des règles permettant de choisir le mineur qui aura le droit d'émettre le prochain bloc de la chaîne

**PSAN** : « Prestataire de services sur actifs numériques ». Depuis l'entrée en vigueur de la loi PACTE le 22/05/2019, et de l'ordonnance n° 2020-1544 le 09/12/2020 renforçant le cadre de la LCB-FT applicable aux actifs numériques, les prestataires exerçant dans certains secteurs relatifs aux crypto-monnaies doivent remplir des conditions particulières pour exercer leurs activités. Ces acteurs répondant au nouveau statut de PSAN doivent s'enregistrer auprès de l'AMF, qui vérifie notamment qu'ils sont en mesure de respecter le dispositif légal relatif à la Lutte contre le Blanchiment et le Financement du Terrorisme (LCB-FT)

## S

**SHA-256**: Dans le cas du Bitcoin, par exemple, le protocole est basé sur un algorithme de hashing (une fonction mathématique) qui s'appelle SHA-256.

SHA est une fonction qui, à partir d'un nombre donné (ou d'une suite de caractère) renvoie un hash, soit une très longue séquence de chiffres de 256 bits.

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

d8f65e96e482a37e047634e3a087f6fd6 a88a636587d7d3b622bb2e123b546fb

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

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

```
01100100 00111000 01100110 00110110 00110101 01100101 00111001
00110110 01100101 00110100 00111000 00110010 01100001 00110011
00110111 01100101 00110000 00110100 00110111 00110110 00110011
00110100 01100101 00110011 01100001 00110000 00111000 00110111
01100110 00110110 01100110 01100100 00110110 01100001 00111000
```

00111000 01100001 00110110 00110011 00110110 00110101 00111000  
00110111 01100100 00110111 01100100 00110011 01100010 00110110  
00110010 00110010 01100010 01100010 00110010 01100101 00110001  
00110010 00110011 01100010 00110101 00110100 00110110 01100110  
01100010

En fait, la séquence ci-dessus correspond à cette suite de 0 et 1. Si l'on change une seule lettre au message d'origine, on obtient un hash qui n'a absolument rien à voir avec le premier.

Notons que SHA-256 pourrait aussi bien être appliqué à un fichier entier

**Smart-Contracts ou Contrats Intelligents** : contrats informatiques autonomes (morceaux de codes) qui permettent de fixer les conditions et les règles d'interaction et ainsi exécuter automatiquement une négociation ou une transaction sur la blockchain. Ils s'exécutent selon certaines conditions prédéfinies

## **W**

**Wallet** : un wallet crypto, en français un portefeuille crypto monnaie, est une solution permettant de stocker et de gérer en toute sécurité une monnaie virtuelle. À l'instar d'un compte bancaire classique, le portefeuille permet à son utilisateur de dépenser, de recevoir, mais aussi d'échanger des crypto monnaie.

## Table des matières :

Introduction générale .....	01
Chapitre 01 : L'évolution et la genèse des cryptomonnaies	
Introduction .....	06
Section 01 : La technologie blockchain : socle du bitcoin.....	06
1. Historique de la monnaie et évolution .....	06
2. Définition et concept clé .....	08
2.1 Définition de la cryptographie.....	08
2.2. Définition de la cryptomonnaie.....	09
2.2.1. Les caractéristiques de la cryptomonnaie.....	10
2.2.2. L'innovation monétaire.....	11
2.2.3. Les principales crypto monnaie existante.....	12
2.2.4. Les principes technologie cryptomonnaies.....	12
2.2.4.1. La blockchain et son fonctionnement.....	13
2.2.4.1.1. Définition de la blockchain.....	13
2.2.4.1.2. Le fonctionnement de la blockchain.....	13
2.2.4.1.3. La relation de bitcoin et la blockchain.....	16
Section 02 : socle du bitcoin .....	16
1. les acteurs du réseau bitcoin .....	16
1.1. Les mineurs.....	17
1.1.1. Définition .....	17
1.1.2. Le rôle des mineurs .....	17
2.1. Les nœuds .....	18
2.1.1. Définition.....	19
2.1.2. Le cout des nœuds.....	19
2.1.3. Les nouvelles transactions.....	19
2.1.4. Mineur avec nœud.....	20

3.1. Les utilisateurs.....	20
3.1.1. Définition.....	20
Section 03 : gouvernance et régulation du bitcoin.....	20
1. la régulation des cryptomonnaies.....	20
1.1. Les institutions de régulation.....	21
1.1.1. Les points clé du volet : régulation et coopération .....	21
1.1.1.1. Réglementer les services offerts a l'interface entre l'asphère réel et cryptomonnaie.....	22
1.1.1.2. Encadrer les placements en cryptomonnaie .....	23
1.1.1.3. Les de cette encadrement .....	23
1.1.1.4. Une coordination internationale pour une régulation efficace des cryptomonnaies.....	24
1.1.2. Les points clé du volet : encadrement du l'utilisation .....	25
1.1.3. Les points clé du volet : connaissance et investigation .....	25
Conclusion.....	27

## Chapitre 02 : mécanisme de fonctionnement de bitcoin.

Introduction .....	29
Section 01:création de nouveau bitcoin .....	29
1. Définition de minage .....	30
2. Importance de la création et l'émission de nouveau bitcoin .....	30
2.1. Sécurisation du réseau : .....	30
2.2. Introduction de nouveaux bitcoins dans l'économie : .....	30
2.3. Facilitation des transactions : .....	31
2.4. Impact sur le prix du Bitcoin : .....	31
3. Fonctionnement du minage du bitcoin.....	31
4. Le processus de minage de Bitcoin.....	31
4.1. Les transactions .....	31
4.2. La création d'un bloc .....	32
5. le rôle des mineurs dans le réseau Bitcoin .....	32
5.1. Vérification des transactions: .....	32
5.2. Preuve de travail:.....	32
5.3. Récompenses de blocs:.....	33
5.4.Pools d'exploitation: .....	34
6. implémentation et fonctionnement .....	34
6.1. Algorithmes de chiffrement.....	34
6.2. Réseau décentralisée.....	35
6.3. Minage et récompenses .....	35
7. Impact et perspective d'avenir .....	35
7.1. Adoption mondiale .....	35
7.1.1 Facteurs d'adoption .....	36
7.1.2. Défis à l'adoption.....	36
7.1.3. Perspectives d'avenir .....	36
Section 02 : transfert, transaction et sécurité : validation et inscription.....	37
1. Le fonctionnement des transactions en Bitcoin .....	37
2. Les étapes d'une transaction .....	38
3. Le rôle des mineurs dans la transaction.....	38
3.1. L'énigme à résoudre est la suivante : .....	38
3.2. Le bloc : .....	38
4. L'enregistrement des transactions dans une application .....	39

5. La transparence du Bitcoin :	39
5.1. Ses avantages majeurs :	39
6. Evolution des transactions en bitcoins :	40
6.1. Transferts internationaux entre particuliers :	40
6.2. Monnaie de paiement pour les commerces :	40
6.3. Outil de développement dans les pays émergents :	40
6.4. Valeur refuge contre les fluctuations monétaires :	40
Section 03 volatilité et valeur de bitcoin : analyses des facteurs	41
1. les facteurs des cours du bitcoin	41
1.1. Envoi et réception d'argent dans le monde entier.	41
1.2. Disponibilité 24/7 :	41
1.3. Vitesse des transactions :	42
1.4. Absence de limitations :	42
1.5. Indépendance des politiques monétaires:	42
2. Risques potentiels associés au Bitcoin:	42
2.1 Risques pour le porteur	42
2.1.1. Volatilité élevée :	42
2.1.2. Sensibilisation et compréhension du protocole :	42
2.1.3. Irréversibilité des transactions :	43
2.1.5. Gigantisme et limites techniques :	43
2.2. Risques liés aux plateformes d'échange de crypto monnaies	43
2.2.1. Défaillance ou faillite des plateformes :	43
2.2.2. Piratage informatique :	44
2.2.3. Manipulation des prix :	44
2.2.4. Manque de régulation :	44
2.2.5. Fraude et blanchiment d'argent :	44
2.3. Impact et risques environnementaux du Bitcoin :	44
2.3.1. Consommation d'énergie élevée :	44
2.3.2. Sources d'énergie et impact sur le climat :	45
2.3.3. Impact local sur l'environnement :	45
2.3.4. Comparaison avec d'autres systèmes:	45
2.3.5. Recherche de solutions et alternatives :	45
3. Débat en cours et nécessité d'une réglementation :	45
3.1. Inégalité de la répartition de la richesse :	45

3.2. Comparaison avec les monnaies traditionnelles et l'étalon-or :	45
3.3. Études et débats en cours :	46
3.4. Nécessité d'une analyse approfondie et d'un débat public :	46
3.5. Réflexion sur les objectifs et les valeurs sociétales :	46
3.5.1. Risque de fraude :	46
3.5.2. Risque systémique :	46
3.5.3. Risque spéculatif :	46
3.6. Mises en garde des banques centrales :	48
Conclusion :	48

### Chapitre 03 : illustration d'une transaction économique et commerciale par décathlon

Introduction.....	50
Section 01 : Introduction a décathlon et a la cryptomonnaie .....	50
1. Présentation de décathlon .....	50
2. Historique décathlon .....	50
3. Fonctionnement de décathlon .....	55
4. Avantage et déficit d'utilisation du bitcoin par décathlon .....	55
4.1. Avantages .....	55
4.2. Inconvénients.....	55
5.évolution de l'acceptation du bitcoin par des entreprises y compris décathlon.....	56
6.évolution du cours du bitcoin depuis sa création a nos jours (2009-2024).....	57
Section 02 : Adoption du bitcoin comme moyen de paiement par une entreprise en ligne.....	58
1. Contexte .....	58
2. Etape du processus .....	58
3. Communication avec le client.....	58
4. Exécution des transactions bitcoin .....	58
5. Confirmation de la transaction .....	58
6. Suivi et support .....	59
7. Augmentation des ventes .....	59
8. Réduction des frais de transaction .....	59
9. Image de marque innovante .....	59
Section 03 : étude de cas : décathlon et son expérience avec le bitcoin .....	59
1. Cas pratique adoption de bitcoin comme moyen de paiement par une entreprise.....	59
1.1. Contexte.....	59
1.2. Etape de processus .....	59

1.3. Communication avec le client .....	60
1.4. Formation du personnel .....	60
1.5. Exécution des transactions bitcoin .....	60
1.6. Confirmation de la transaction .....	60
1.7. Suivi et support .....	60
1.8. Résultat attendu .....	60
1.8.1. Augmentation des ventes .....	60
1.8.2. Réduction des frais de transaction .....	60
1.8.3. Image de marque innovante .....	60
Conclusion.....	62
Conclusion générale .....	63
Référence et bibliographique .....	68

# Résumé

## **Résumé**

L'innovation financière a entraîné la création d'une immense quantité d'argent non contrôlée par les banques centrales appelées « les crypto monnaies », une monnaie qui circule virtuellement sur un réseau appelé « blockchain », un registre de transactions distribué, une base de données décentralisée qui repose sur un réseau pair à pair destiné au stockage et au transfert de données.

Aujourd'hui, alors que leur valeur est passée de quelques centimes en 2009 à des milliers d'euros, les crypto monnaies sont considérées par certains comme une menace et reconnues par d'autres comme une occasion de renouveler le système financier.

Cette nouvelle technologie intéresse désormais les banques, les assurances et les autres auteurs du secteur financier qui tentent de monter sur la vague d'innovation pour survivre à la désintermédiation et pour regagner la confiance des clients et en tirer les multiples avantages qu'elle offre au service d'une efficacité renforcée, d'une maîtrise des coûts et d'une plus grande pertinence dans les produits et services proposés à leurs clients.

### **Mots clés :**

Blockchain, registre de transactions, innovation financière, innovation technologique, monnaie, monnaie numérique, monnaie virtuelle crypto monnaie, cryptographique, système de paiement, banque, confiance, unité de compte, réserve de valeur, moyen de paiement, système décentralisé, anonymat, pair à pair.

### **Abstract**

Financial innovation has led to the creation of a huge amount of money not controlled by central banks called “cryptocurrencies”, a currency that circulates virtually on a network called “blockchain”, a distributed transaction register, a decentralized database based on a peer-to-peer network for data storage and transfer.

Today, while their value has gone from a few cents in 2009 to thousands of euros, cryptocurrencies are considered by some as a threat and recognized by others as an opportunity to renew the financial system.

This new technology interest now banks, insurance companies and the other authors in the financial sector who are trying to ride the wave of innovation to survive disintermediation and to regain customer trust and reap the multiple benefits it offers in the service of increased efficiency, cost control and greater relevance in the products and services offered to their customers.

**Word keys:**

Blockchain, transaction register, financial innovation, technological innovation, currency, digital currency, cryptocurrency, cryptographic, payment system, bank, trust, unit of account, value reserve, means of payment, decentralized system, anonymity, peer to peer.