

# LA BLOCKCHAIN : UNE TECHNOLOGIE AUX ENJEUX CONTROVERSÉS

**Pré-Mémoire**

**MASTER**

**DEVELOPPEMENT LOGICIEL, MOBILE  
ET INTERNET DES OBJETS**

*Année 2020 / 2021*

**Antoine ACQUART**

## Table des matières

Table des matières .....	1
Introduction.....	2
1. Comprendre la technologie blockchain.....	4
1.1. Histoire de la blockchain .....	4
1.2. Vulgarisation d'une technologie relativement complexe .....	6
1.3. Les différents composants du système : fonctionnement technique.....	8
1.3.1 Le hash.....	8
1.3.2 Les adresses.....	8
1.3.3 Le bloc.....	9
1.3.4 Le minage .....	12
1.3.5 La transaction .....	16
1.3.6 Un réseau de pair à pair .....	18
1.4. Une technologie qui sait s'adapter.....	18
2. Les enjeux de la blockchain .....	20
2.1. Un système prometteur .....	20
2.1.1. Exploiter une technologie inédite : les avantages de la blockchain.....	20
2.1.2. Diversification des utilisations de la technologie .....	22
2.2. Un système controversé.....	26
2.2.1. Des contreparties fortes : les désavantages de la blockchain.....	26
2.2.2. Les impacts et risques d'un nouveau marché financier .....	27
2.2.2.1. Une explosion de l'économie spéculative .....	27
2.2.2.2. Un nouveau moyen de paiement pour les marchés illégaux .....	28
2.2.2.3. Un impact environnemental fort.....	29
2.2.2.4. Un nouvel enjeu économique pour certains pays.....	29
2.2.2.5. L'arrivée des ordinateurs quantiques : une menace de taille .....	30
Conclusion .....	31
Problématique.....	31
Perspectives d'évolution envisagées.....	32

## Introduction

Ce document résulte de ma 4<sup>ème</sup> année de formation dans l'école Ynov Aix-en-Provence, sur le cursus Master DEVLMIOT, développement logiciel, mobile et Internet des objets.

Travaillant depuis novembre 2019 chez Atos sur le projet SICS, développant le futur système d'information de l'Armée de Terre, j'ai préféré choisir un sujet tout autre pour ce pré-mémoire, par soucis de limites liées à la confidentialité et de préférences personnelles.

La veille informatique est très importante dans un milieu comme le nôtre, car les technologies qui se développent aujourd'hui feront surement partie de notre avenir personnel et professionnel.

L'une d'entre elles prend de plus en plus de place par son impact économique grandissant, et est définie par certains comme prometteuse.

Traçant sa route depuis plus de dix ans, elle prend de plus en plus de place dans le monde qui nous entoure. Soutenue par tous types de personnes comme par l'homme le plus riche du monde pour son caractère innovant ainsi que ses perspectives d'avenir, elle a bouleversé le marché financier en ne cessant d'alimenter les débats liés à ses conséquences environnementales.

De par ses prismes tous autant soutenus que controversés, c'est le vaste concept de la blockchain que j'ai choisi d'explorer.

Je n'ai pas d'attrait particuliers pour les cryptomonnaies, principale utilisation de la blockchain, cependant notre avenir écologique, technologique et économique sont des sujets auxquels je porte beaucoup d'intérêts et la blockchain vient bousculer tous ces domaines, à plus ou moins forte échelle.

J'ai décidé de m'y intéresser afin d'en comprendre les enjeux, de me préparer à l'éventualité où j'y serai confronté dans un futur plus ou moins proche, et de partager les connaissances que m'auront apporté les recherches effectuées sur ce sujet.

Afin d'atteindre ces objectifs, nous nous confronterons plus particulièrement à l'aspect technique de la technologie.

Tout d'abord, nous tenterons de nous immiscer au cœur de la première blockchain ayant vu le jour afin d'en comprendre son fonctionnement dans les moindres détails. Pour ce faire, nous commencerons par retracer l'histoire de la technologie, et nous verrons ensuite une vue d'ensemble des différents concepts, puis nous les étudierons un à un plus en détails. Nous nous appuierons donc sur l'exemple de la blockchain Bitcoin.

La seconde partie mettra en exergue ses différents enjeux, en commençant par l'observation des différentes utilisations qu'on peut en faire. Nous verrons ensuite les inconvénients de la technologie, et nous terminerons par en explorer ses impacts ainsi que les risques qu'elle encoure.

Les références utilisées pour la recherche et la rédaction de ce document sont décrites en annexe dans une bibliographie commentée.

## 1. Comprendre la technologie blockchain

### 1.1. Histoire de la blockchain

Le concept de blockchain a été mis en pratique pour la première fois avec l'introduction du Bitcoin sous forme de livre blanc à l'automne 2008, puis publié en tant que logiciel open source en 2009. Son auteur anonyme, un programmeur ou une organisation, s'est fait connaître sous le nom de Satoshi Nakamoto.

Jusqu'en 2010, il a travaillé avec de nombreux autres développeurs open source sur le développement de Bitcoin. Cette personne ou ce groupe ne participe plus au projet et transfère le contrôle aux développeurs principaux de Bitcoin. Il existe de nombreuses théories sur l'identité de Satoshi Nakamoto, mais elles n'ont jamais été confirmées.

Citées dans son livre blanc, différentes idées et concepts ont permis à Bitcoin de voir le jour.

L'idée de connecter des blocs avec des chaînes cryptées a été proposée en 1991 par Stuart Haber et Scott Stornetta, respectivement cryptographe et chercheur à cette époque. Ils ont conçu un système dans lequel des informations ou des transactions horodatées ne peuvent pas être modifiées ou altérées.

Plus tard, rejoints par le mathématicien David Allen Bayer, Haber et Stornetta ont proposé l'utilisation d'un procédé cryptographique permettant de regrouper les données de plusieurs documents en un seul bloc pour en vérifier les transactions : il s'agit de l'arbre de Merkle. Toutefois, cette technologie ne sera pas utilisée avant l'implémentation de Bitcoin.

Un autre concept sur lequel s'est basée la première blockchain et beaucoup d'autres ensuite, est la preuve de travail. Introduite en 1998 par Wei Dai, ingénieur ayant travaillé pour Microsoft, c'était une idée destinée à servir à la création d'une monnaie virtuelle, la b-money. Invention qui sera améliorée en 2004 par l'informaticien et cryptographe Hal Finney, créant la preuve de travail réutilisable. Il sera la première personne à recevoir une transaction sur le réseau Bitcoin : Satoshi Nakamoto lui enverra 10 bitcoins le 12 janvier 2009.

Après ses premiers balbutiements, ce fût au tour de Bitcoin d'inspirer d'autres investisseurs et créateurs.

Le 27 novembre 2010, la première « pool de minage », traduit par ferme de minage en français, est lancée. Dans l'année 2011, ce sont les premières nouvelles cryptomonnaies, aussi appelées altcoins, qui voient le jour.

En 2015, c'est au tour de la blockchain Ethereum, qui viendra par la suite seconder Bitcoin au classement des monnaies virtuelles avec son propre jeton appelé Ether. Vitalik Buterin son créateur était développeur sur Bitcoin et souhaitait développer la technologie pour créer des applications décentralisées.

N'ayant pas réussi à convaincre la communauté, il se lance en 2013 dans le développement du réseau qui portera l'innovation jugée par beaucoup comme la plus novatrice sur une blockchain : le « smart contract », ou contrat intelligent.

Par la suite, ce sera son réseau qui portera les premières applications décentralisées basées sur sa monnaie, et qui développera également, en 2017, le marché des « Non-Fungible Tokens », ou jetons non fongibles : la vente des droits d'œuvres d'arts ou d'objets virtuels.

### 1.2. Vulgarisation d'une technologie relativement complexe

La blockchain est une technologie s'apparentant à une base de données, qui stocke tel un registre de banque, un ensemble de transactions. Cette base de données est décentralisée, ce qui veut dire qu'elle n'est pas hébergée à un seul et même endroit, mais qu'elle est distribuée à tous les utilisateurs de la technologie.

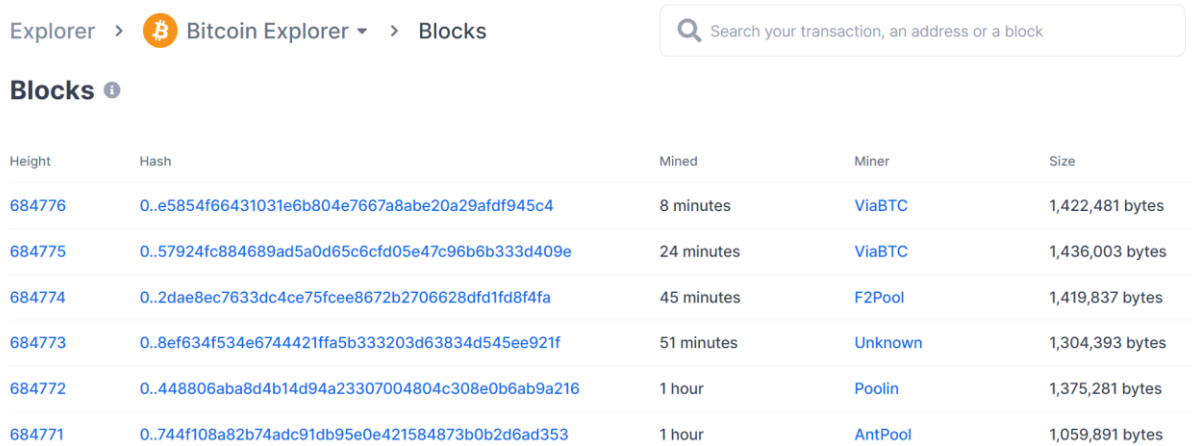
De cette manière, lorsqu'un utilisateur demande à émettre un montant, tous ceux possédant le registre vont vérifier que les deux parties incluses dans la transaction existent sur le réseau, et que l'émetteur possède les fonds qu'il s'apprête à envoyer. Si c'est le cas, la transaction va pouvoir être écrite à la suite du registre, mais pour cela il faut qu'il reste de la place sur celui-ci, nous allons voir pourquoi.

La blockchain est, comme son nom l'indique, une chaîne de blocs. Ces blocs sont les fichiers contenant l'intégralité des transactions effectuées sur le réseau, depuis la création de celui-ci : ils forment le registre évoqué plus haut. Néanmoins, afin de contrôler la taille de la blockchain, les blocs ont une taille maximale de 1 Mo (ce qui équivaut plus ou moins à 2000 transactions), et l'ajout d'un bloc sur le réseau nécessite une tâche supplémentaire : la preuve de travail.

La preuve de travail ou « Proof of Work », consiste, par un procédé de chiffage que nous expliquerons plus tard, à trouver une valeur commençant par un nombre déterminé de « 0 », à partir des données du dernier bloc de la chaîne. Cela demande une énorme puissance de calcul et en conséquence consomme beaucoup d'énergie. C'est pourquoi, l'utilisateur qui trouve cette valeur et permet d'ajouter un bloc au réseau se voit récompenser d'une certaine somme de bitcoins. Cette action est plus couramment appelée « minage ».

Une fois le bloc ajouté, c'est sur les données de celui-ci que devra se baser le calcul du suivant : on comprend donc que chaque bloc est lié au précédent, ce qui crée une chaîne : la blockchain.

Afin de visualiser à quoi cela ressemble, nous allons nous rendre sur un explorateur de blockchains, <https://blockchains.com> en l'occurrence.



The screenshot shows the Bitcoin Explorer interface. At the top, there's a navigation bar with 'Explorer', a Bitcoin icon, 'Bitcoin Explorer', and 'Blocks'. A search bar is on the right. Below the navigation bar, the title 'Blocks' is followed by an information icon. A table lists the most recent blocks with columns for Height, Hash, Mined, Miner, and Size. The table shows six blocks, with heights decreasing from 684776 to 684771. The hashes are truncated on the left. The 'Mined' column shows times from 8 minutes to 1 hour. The 'Miner' column lists 'ViaBTC', 'F2Pool', 'Unknown', 'Poolin', and 'AntPool'. The 'Size' column shows block sizes in bytes, ranging from approximately 1.3 million to 1.4 million bytes.

Height	Hash	Mined	Miner	Size
684776	0..e5854f66431031e6b804e7667a8abe20a29afdf945c4	8 minutes	ViaBTC	1,422,481 bytes
684775	0..57924fc884689ad5a0d65c6cfd05e47c96b6b333d409e	24 minutes	ViaBTC	1,436,003 bytes
684774	0..2dae8ec7633dc4ce75fcee8672b2706628dfd1fd8f4fa	45 minutes	F2Pool	1,419,837 bytes
684773	0..8ef634f534e6744421ffa5b333203d63834d545ee921f	51 minutes	Unknown	1,304,393 bytes
684772	0..448806aba8d4b14d94a23307004804c308e0b6ab9a216	1 hour	Poolin	1,375,281 bytes
684771	0..744f108a82b74adc91db95e0e421584873b0b2d6ad353	1 hour	AntPool	1,059,891 bytes

Figure 1 - Les derniers blocs ajoutés à la blockchain Bitcoin, le 24/05/2021 à 15h43

On peut voir ici quelques-uns des derniers blocs ajoutés à la blockchain. La première colonne correspond au numéro du bloc : à ce moment-là, la blockchain était donc composée de 684,776 blocs. Ensuite on peut voir le hash des blocs, commençant par un grand nombre de 0 (20 en l'occurrence, ils sont masqués par le site pour ne pas prendre trop de place) : ils ont été générés avec la preuve de travail.

Vient ensuite la date de minage du bloc (un bloc est miné toutes les 10 minutes en moyenne), puis le nom du mineur, et enfin la taille du bloc. Nous verrons plus tard pourquoi les tailles dépassent 1 Mo, alors que ce n'est pas censé être possible.



### 1.3. Les différents composants du système : fonctionnement technique

#### 1.3.1 Le hash

« Les fonctions de hachage sont des fonctions mathématiques qui permettent de transformer une chaîne de caractères de longueur indifférente en une autre chaîne de longueur fixe. Le changement le plus insignifiant dans la chaîne d'entrée provoque un grand changement dans la chaîne de sortie. »

(Bitcoin.fr, <https://bitcoin.fr/quest-ce-quune-fonction-de-hachage/>)

La fonction de hachage utilisée par la blockchain Bitcoin est le SHA-256, qui transforme une chaîne de caractère en une autre de 256 bits, soit 64 caractères en notation hexadécimale.

Le but de ces fonctions est de pouvoir convertir facilement une chaîne d'entrée en chaîne de sortie, mais que l'opération inverse soit impossible. Une même chaîne d'entrée donnera toujours le même résultat.

Exemple :

« bitcoin » → 6B88C087247AA2F07EE1C5956B8E1A9F4C7F892A70E324F1BB3D161E05CA107B

« bitcoin1 » → DBDBAC0B3072D7677FC94EEBAF8EBA9E81E5C3B7DE6899DAE12C98D6799B065A

#### 1.3.2 Les adresses

Sur le réseau, chaque transaction est effectuée entre deux adresses : celle de l'émetteur et celle du bénéficiaire.

Une adresse fonctionne sur le principe du chiffrement asymétrique, de clé privée et de clé publique. À la manière d'une adresse électronique, une clé publique peut être partagée, elle représente son propriétaire. La clé privée, qui elle doit rester secrète, est l'équivalent du mot de passe permettant d'accéder à l'adresse électronique.

Pour le cas du Bitcoin, c'est l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm) qui est utilisé pour générer ces clés.

Avec cet algorithme, une clé privée est générée à partir d'un nombre aléatoire. Ensuite, la clé publique est générée sur un point aléatoire d'une courbe basée sur la valeur de la clé privée.

Afin de générer une adresse Bitcoin qui sera accessible à partir de la clé privée, la clé publique va subir une suite de hachages :

1. La clé publique est hachée avec SHA-256
2. Le résultat est haché avec RIPEMD-160
3. Est ajouté un octet de version devant le résultat
4. Le résultat est haché avec SHA-256
5. Le résultat est de nouveau haché avec SHA-256
6. Sont gardés les 4 premiers octets du résultat, qui représentent le « checksum » de l'adresse, et sont ajoutés à la fin du résultat obtenu après l'étape 3
7. Le résultat est converti en base58 : on obtient alors une adresse Bitcoin.

Un utilisateur sur le réseau ne possède pas qu'une seule adresse : par soucis de sécurité et de confidentialité, la bonne pratique est de créer une adresse par transaction. Cette bonne pratique est utilisée sur tous les portefeuilles virtuels, les « wallets ».

Un wallet n'est pas comme un compte bancaire, son rôle n'est pas de stocker directement de la monnaie. Créé avec un logiciel, le portefeuille va permettre à partir d'une seule clé, de stocker toutes les adresses d'un utilisateur.

Finalement une adresse ne possède rien de concret, elle va simplement servir à authentifier une transaction : si une transaction est faite vers mon adresse, comme je possède la clé privée correspondant je vais pouvoir réémettre le montant reçu, j'en suis donc le propriétaire.

### 1.3.3 Le bloc

Le bloc est le composant qui est à la base du réseau, toutes les actions effectuées sur la blockchain touchent de près ou de loin aux données d'un ou de plusieurs blocs.

Les données contenues dans un bloc vont permettre de lister les différentes transactions effectuées sur celui-ci, tout en assurant leur intégrité.

### Block 684776 ⓘ

USD BTC

This block was mined on May 24, 2021 at 3:35 PM GMT+2 by [ViaBTC](#). It currently has 3 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC (\$236,346.63). The reward consisted of a base reward of 6.25000000 BTC (\$236,346.63) with an additional 1.16386808 BTC (\$44,012.21) reward paid as fees of the 2357 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this [address](#).

A total of 38,748.30088577 BTC (\$1,465,284,822.21) were sent in the block with the average transaction being 16.43966945 BTC (\$621,673.66). Learn more about [how blocks work](#).


Hash	00000000000000000000e5854f66431031e6b804e7667a8abe20a29afdf945c4 
Confirmations	3
Timestamp	2021-05-24 15:35
Height	684776
Miner	<a href="#">ViaBTC</a>
Number of Transactions	2,357
Difficulty	25,046,487,590,083.27
Merkle root	218cd85d806d4ec96b13b0ff494abca7d4f4ce327127125414f529a6efc69580
Version	0x20400004
Bits	386,612,457
Weight	3,993,307 WU
Size	1,422,481 bytes
Nonce	908,622,914
Transaction Volume	38748.30088577 BTC
Block Reward	6.25000000 BTC
Fee Reward	1.16386808 BTC

Figure 2 - Un bloc ajouté à la blockchain Bitcoin, le 24/05/2021 à 15h35

Un bloc est composé d'un en-tête qui va se charger de son intégrité, du nombre de transactions contenues dans celui-ci, et des transactions elles-mêmes.

L'en-tête du bloc, d'une taille de 80 octets, est composée de :

- Un numéro de version :

Au cours de la vie du Bitcoin, sa blockchain a reçu différentes améliorations par les développeurs de sa communauté. Il existe quatre versions du bloc Bitcoin, introduites respectivement en janvier 2009, septembre 2012, février et novembre 2015. Afin de respecter le système qui assure l'intégrité de la blockchain, le changement de version d'un bloc se fait

de manière non rétroactive : seuls les blocs créés à partir de la mise en ligne de la nouvelle version la prendrons en compte.

- Le hash de l'en-tête du bloc précédent :

Afin de s'assurer que le bloc précédent ne soit pas modifié, on enregistre son hash dans le bloc suivant.

- Le hash de l'en-tête du bloc, ou « merkle root hash » :

Ce hash est généré à partir de toutes les transactions incluses dans le bloc, de manière à ce qu'aucune d'entre elles ne puisse être modifiée sans modifier également l'en-tête du bloc.

- L'heure Unix, ou « unix time » :

L'heure à laquelle le mineur a commencé à hacher l'en-tête. Elle doit être strictement supérieure à la médiane de l'heure des onze blocs précédents, et ne peut pas être acceptée par les autres nœuds si elle est plus de deux heures dans le futur de leurs propres horloges.

- Le seuil de difficulté encodé, ou « target nBits » :

C'est une valeur tenant sur quatre octets qui va définir la difficulté qu'aura le bloc à être miné : on va calculer un seuil à partir de cette valeur, la valeur du hash du header qui validera l'ajout du bloc dans la blockchain devra être égale ou inférieure à ce seuil.

- Le « nonce » :

Tenant également sur quatre octets, c'est cette valeur qui va devoir être déterminée et changée par le mineur, afin que la valeur du hash du header du bloc soit inférieure au seuil. Si jamais toutes les valeurs des trente-deux bits sont testées sans que le hash ne soit valide, l'heure va pouvoir être mise à jour, ou alors la valeur de la première transaction du bloc, celle destinée à rémunérer le mineur, pourra être modifiée. Et cela dans le but de changer le « merkle root » et donc le hash du header, ce qui permettra de pouvoir re-tester l'intégralité des valeurs possibles sur trente-deux bits.

La taille d'un bloc varie en fonction de la taille et du nombre de transactions qu'il contient, mais son format sérialisé, format utilisé dans les requêtes permettant la transmission de données d'un nœud à un autre, ne doit pas dépasser 1 Mo.

À l'origine, la taille d'un bloc était limitée à 36 Mo, mais a été fixée en 2010 à 1 Mo afin de renforcer la sécurité des blocs contre les attaques de spams. Cela ne causait pas vraiment de problèmes car les blocs n'atteignaient pas les 1 Mo, jusqu'en 2015 où cette limite commençait à être atteinte de manière quotidienne.

Cette règle est à l'origine d'un grand nombre de débats, car c'est une caractéristique qui influe sur la rapidité des transactions : depuis ce jour, on compte entre 2 à 7 transactions par seconde. En effet, écrire dans un bloc est une opération très rapide, mais ajouter un bloc au réseau demande bien plus de temps : environ 10 minutes. Si la limite était augmentée, le réseau ne serait plus restreint aux 2000 transactions toutes les 10 minutes en moyenne.

Cependant, aujourd'hui il est courant de voir sur le réseau des blocs d'une taille supérieure, car un protocole permettant de réduire les données contenues dans une transaction a vu le jour. En passant certaines données de transactions comme données « témoins » qui ne sont pas comptées dans la taille du bloc mais qui restent toutefois valides, elles permettent la validation et l'ajout de blocs sur le réseau pouvant atteindre les 2 Mo. Il s'agit du protocole Segwit.

### 1.3.4 Le minage

Le minage est une étape primordiale dans le cycle de vie de la blockchain. C'est elle qui va permettre de générer de la monnaie virtuelle, de valider que les nouvelles transactions sont cohérentes, ou plus globalement d'assurer l'intégrité de la blockchain.

Dans le cas de Bitcoin et comme dans la majorité des blockchains, le minage est également appelé « preuve de travail » car il s'agit d'une action complexe à réaliser. Cette action qui porte tant de responsabilités se doit d'être très bien pensée, de sorte qu'elle remplisse toutes ses fonctions, sans jamais être remise en cause, au risque de voir effondrer la chaîne de confiance.

En premier lieu, nous allons voir qui sont les mineurs, ce qui les pousse à œuvrer pour la blockchain, et en quoi consiste leur travail. Nous verrons par la suite en quoi le minage permet d'assurer l'intégrité de la blockchain.

Si aujourd'hui il existe des millions de mineurs à travers le monde, c'est que cette action est bien souvent rentable, et même accessible à tous.

Tous les utilisateurs d'une blockchain ne sont pas mineurs, mais il est assez simple de le devenir.

Un mineur de cryptomonnaie peut être défini par une machine, ou plus largement la personne qui la possède, effectuant des calculs afin de générer de la monnaie virtuelle.

Un particulier peut très bien miner directement avec son ordinateur personnel grâce à la puissance de son processeur ou de sa carte graphique. Néanmoins, les plus gros mineurs, ceux qui génèrent le plus de cryptomonnaies sont en fait des « pools », des salles remplies d'ordinateurs appartenant la majorité du temps à des entreprises, n'ayant pour seul objectif que d'être les premiers à résoudre les problèmes liés à la blockchain qu'ils exploitent, afin d'en valider les blocs et en conséquence de générer de la monnaie.

Nous allons voir comment cette monnaie est générée.

Quand un bloc est ajouté à la blockchain, l'ensemble des mineurs du réseau vont être mis en concurrence : le premier qui arrive à résoudre le problème du bloc suivant aura le droit d'en valider les transactions, et sera récompensé d'une certaine somme de cryptomonnaie, en plus des frais que tous les émetteurs de ces transactions ont payés afin qu'elles soient validées le plus rapidement possible.

Une fois que le mineur diffuse le nouveau bloc sur le réseau, il va devoir être validé par la majorité de celui-ci : vont être vérifié le hash créé, les transactions que composent le bloc, et l'ensemble des métadonnées de son en-tête.

Ensuite, si le bloc est accepté, tous ses concurrents le prennent en compte, arrêtent d'essayer de valider leurs blocs avec le hash du précédent, et prennent celui-ci comme dernier bloc valide de la chaîne.

Pour revenir sur le principe de cette « preuve de travail », nous garderons l'exemple de la première ayant vu le jour, à savoir celle de Bitcoin.

Comme évoqué dans la description du header d'un bloc, c'est la valeur de la propriété « nBits » qui va déterminer le seuil que devra respecter le hash du header, afin d'être valide. On dit souvent que ce hash doit commencer par un certain nombre de « 0 » pour en simplifier la compréhension, car effectivement plus il y aura de « 0 » au début du hash plus sa valeur sera petite, mais en réalité les mineurs se basent exclusivement sur la valeur de la propriété « nBits ».

Nous allons maintenant aborder deux règles immuables de la blockchain Bitcoin, relatives au minage. La première découle directement de ce que nous venons de voir : la difficulté à miner un bloc. En place depuis 2008, la blockchain conserve un temps moyen de minage de 10 minutes, comment cela est-il possible, alors que la puissance de calcul des machines ne cesse d'augmenter ?

La difficulté, donc le « nBits », est recalculé tous les 2016 blocs. En effet, un calcul est effectué en prenant le temps moyen de minage des 2016 derniers blocs ayant eu la même difficulté, afin de déterminer la difficulté qu'auront les 2016 blocs suivants, de manière à ce qu'en moyenne on se rapproche le plus possible des 10 minutes.

La seconde règle concerne la création de nouveaux bitcoins. Il ne pourra pas y avoir, à terme, plus de 21 millions de bitcoins circulant entre les différents utilisateurs du réseau.

Si on regarde le bloc n°684776 exposé plus haut, on voit que la récompense obtenue par le mineur, équivalant aux nouveaux jetons ajoutés au réseau, est de 6.25 bitcoins. À l'origine, cette récompense s'élevait à 50 bitcoins : c'est là que la règle intervient : tous les 200 000 blocs, la récompense se voit réduite de moitié.

Si on prend en compte ces deux règles, avec la génération de nouveaux blocs toutes les 10 minutes environ et la dégression exponentielle du nombre de bitcoins générés, on se rend compte que la production de bitcoins cessera aux alentours de 2140. À partir de cette date, le seul gain qu'auront les mineurs sera constitué des frais de transactions donnés par les émetteurs.

Maintenant que nous avons vu ces concepts, il est plus simple de comprendre en quoi le minage permet d'assurer l'intégrité de la blockchain.

Le minage (ou la recherche du hash respectant le seuil donné d'un bloc prend en moyenne 10 minutes) et le hash se basent sur celui du bloc précédent. Si on souhaite modifier un bloc, on doit modifier tous les blocs suivants, et donc recalculer un hash pour chacun d'entre eux.

La blockchain compte toujours comme valide la plus longue chaîne de blocs, ce faisant, si deux blocs se basant sur le même bloc précédent sont ajoutés, c'est celui dont le prochain bloc sera ajouté en premier qui verra sa branche être confirmée par le réseau.

Sur le schéma ci-dessous, quand les blocs 3 et 3' vont respectivement être ajoutés, en prenant le premier des deux blocs qu'ils ont vu apparaître sur la chaîne, les mineurs du monde entier vont commencer à calculer le hash du bloc suivant. Cela peut arriver sans forcément qu'il y ait de mauvaises intentions, quand deux hash sont trouvés simultanément par exemple.

Dans ce cas, le réseau fonctionnant de pair-à-pair, les mineurs les plus proches de chacun des blocs travailleront dessus. Si jamais il y a aussi une égalité sur le bloc 4, chacune des branches vont se prolonger jusqu'à ce que l'une d'entre elles se démarque. Les cas de simultanéités restent tout de même assez rares étant donné le caractère aléatoire important de la preuve de travail.

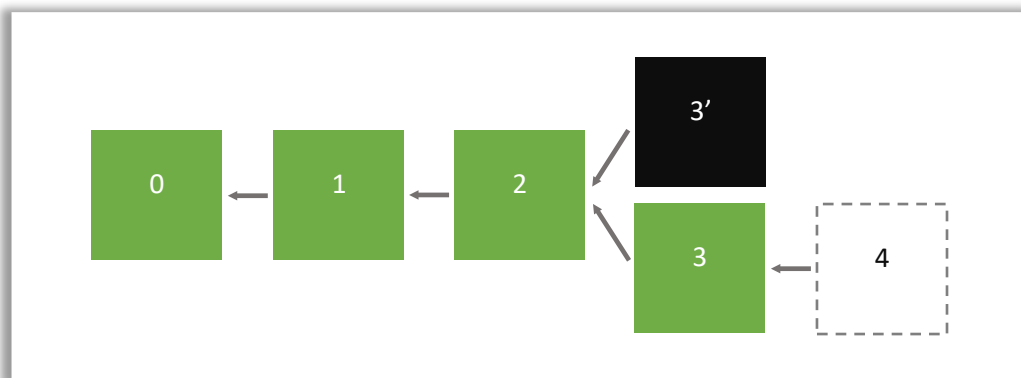


Figure 3 - Visualisation d'un conflit entre deux blocs ajoutés



Si quelqu'un voulait corrompre la chaîne, il devrait posséder plus de la moitié de la puissance de calcul du réseau afin de modifier un bloc, de rattraper le minage de la « vraie » chaîne et de valider tous les blocs qu'il ajouterait.

C'est ce qu'on appelle « l'attaque à 51% ». Bien que cela soit extrêmement dur à atteindre étant donné qu'aujourd'hui il existe plus d'un million de mineurs répartis à travers le monde pour la blockchain Bitcoin uniquement, si cela arrivait ce ne serait pas rentable pour l'attaquant : le coût de l'attaque serait extrêmement élevé au vu de la puissance de calcul nécessaire et cela décrédibiliserait la monnaie, faisant perdre de la valeur aux potentiels bitcoins gagnés par celui-ci.

Néanmoins, le risque existe toujours et pourrait être un problème pour les victimes de l'attaque. C'est pourquoi un bloc possède un nombre de « confirmations ». Une confirmation correspond à un bloc validé après celui en question, et mathématiquement, plus il y'a de confirmations, plus les chances qu'un bloc se fasse attaquer sont infimes.

Il est donc conseillé d'attendre qu'une transaction soit sur un bloc confirmé un certain nombre de fois avant de vouloir en être bénéficiaire.

### 1.3.5 La transaction

Les transactions sont au cœur du réseau, c'est autour d'elles qu'est construit toute la blockchain.

La monnaie étant totalement virtuelle, il n'existe pas réellement de pièces, billets ou jetons : tout est transaction.

Dans le but de bien comprendre comment cela fonctionne, nous allons nous mettre en situation : à l'origine de la blockchain et en partant d'un nouvel utilisateur qui viendrait miner un bloc, nous allons voir comment il va pouvoir utiliser sa monnaie à travers le réseau.

Un utilisateur mine un bloc : une transaction de création de monnaie est inscrite dans ce bloc et donc dans l'immense registre qu'est la blockchain : tout le réseau va voir que son adresse est bénéficiaire de la somme générée, 50 bitcoins.

Maintenant cet utilisateur souhaite envoyer un certain montant à une autre adresse, 10 bitcoins par exemple.

Jusqu'à maintenant il possède une seule adresse. En lisant le registre on voit qu'une transaction a été effectuée vers celle-ci, envoyant 50 bitcoins : elle va donc pouvoir être utilisée en tant qu'émettrice.

Une transaction fonctionne avec le principe d'entrées et de sorties : les entrées sont des transactions précédentes authentifiées par des adresses qui contiennent les bitcoins allant être envoyés, et les sorties sont les adresses qui vont en être bénéficiaires. Une entrée est donc la sortie d'une transaction précédente, et une sortie sera dans le futur l'entrée d'une prochaine transaction.

Sur ce principe et comme nous allons le voir, quand une sortie est utilisée elle l'est dans son intégralité : c'est pourquoi le surplus est envoyé à une autre adresse de l'émetteur.

Une nouvelle transaction va donc être construite avec différentes données :

- Entrée 1 : La sortie de la transaction précédente contenant 50 bitcoins, authentifiée par l'adresse émettrice
- Sortie 1 : l'adresse bénéficiaire avec le montant à envoyer, soit 10 bitcoins
- Sortie 2 : l'adresse sur laquelle le surplus va être envoyé avec la valeur du surplus, soit 39 bitcoins

À première vue on pourrait croire qu'il y a une erreur dans le calcul : il y a 50 bitcoins en entrée, mais seulement 49 en sortie. C'est en fait comme ça que les frais sont comptés, il s'agit de la différence entre le total des entrées et le total des sorties. L'émetteur va donc jouer avec la sortie de surplus qu'il se réattribue pour définir la prime qu'il laisse au mineur, et ainsi démarquer sa transaction sur le réseau.

En effet, plus une transaction a de frais, plus les mineurs vont vouloir l'ajouter à un bloc en priorité. Le bloc étant limité par sa taille, les frais vont être calculés par rapport à la valeur du bitcoin sur le marché, mais aussi et surtout par la taille de la transaction : plus il y a d'entrées et de sorties plus la transaction va être lourde, et en conséquence plus les mineurs vont attendre un montant élevé.

Tout ça dans le but de miner des blocs les plus lucratifs, avec le taux de satochis par bit le plus haut.

À noter qu'on parlait jusqu'ici de bitcoins entiers pour en simplifier la compréhension, mais il s'avère qu'aujourd'hui la plupart des transactions contiennent des centièmes, millièmes et des parts de bitcoins plus infimes encore.

Pour gérer plus simplement ce genre de montants à virgule, c'est une autre unité qui est utilisée dans le corps des transactions : le satoshi. Un bitcoin équivaut à 100 millions de satochis et donc un satochi correspond à 0,000.000.01 bitcoin, soit le plus petit montant échangeable par transaction.

### 1.3.6 Un réseau de pair à pair

« Le pair-à-pair ou système pair à pair (en anglais peer-to-peer, souvent abrégé « P2P ») est un modèle d'échange en réseau où chaque entité est à la fois client et serveur, contrairement au modèle client-serveur. Les termes « pair », « nœud » et « utilisateur » sont généralement utilisés pour désigner les entités composant un tel système. » (Wikipédia, <https://fr.wikipedia.org/wiki/Pair-%C3%A0-pair>)

Utilisant le pair-à-pair, la blockchain Bitcoin est un système décentralisé, ce qui implique qu'il n'y a pas d'autorité définie qui gouverne le réseau.

Afin de rentrer sur ce réseau, il suffit de télécharger un logiciel ou une application dédiée, qui connaît les adresses IP d'utilisateurs « connus » sur le réseau. En effectuant une requête vers l'une d'entre elles, le logiciel va récupérer les adresses d'autres utilisateurs actifs.

De cette manière, on pourrait retrouver l'ensemble des adresses utilisées sur le réseau, comme le fait le site <https://bitnodes.io/> par exemple. Cependant, il n'est pas nécessaire d'en connaître la liste exhaustive, seules quelques-unes suffisent : quand un utilisateur va effectuer une transaction, il va la diffuser à toutes les adresses qu'il connaît, qui vont elles-mêmes la retransmettre à toutes leurs connaissances, jusqu'à ce que tout le réseau en soit informé.

### 1.4. Une technologie qui sait s'adapter

Nous venons de voir l'ensemble des concepts les plus importants de la blockchain Bitcoin, qui, les uns liés aux autres, forment un système robuste qui ne cesse de se populariser sans jamais être vraiment remis en question. Nous parlons ici de la première blockchain, qui est également la plus populaire et dont le fonctionnement reste le plus utilisé sur la majorité des autres systèmes.

Toutefois, d'autres ont vu le jour en reprenant certains concepts, tout en ajoutant leurs lots d'innovations qui ont permis à la technologie de se développer et de proposer toujours plus d'utilisations différentes.

Les principales évolutions ont été apportées par la blockchain Ethereum, avec l'ajout des « smart contracts », notamment.

Le contrat intelligent est un script lié à une adresse qui va pouvoir être déployé sur le réseau à la manière d'une transaction. Il peut comporter un ensemble de fonctions, qui vont prendre des transactions en entrée et effectuer des actions à partir de celles-ci.

Face aux problèmes liés à la forte consommation électrique pour valider les blocs, Ethereum a travaillé sur un autre moyen, beaucoup moins impactant pour l'environnement : la « proof of stake », ou preuve de possession. Au lieu d'être validés par les premiers à trouver un hash, les blocs seront attribués aléatoirement à des utilisateurs du réseau, possédant un certain nombre de jetons, 32 en l'occurrence. Ce principe permet de s'abstraire de la charge environnementale qu'a la preuve de travail, et permet de rémunérer directement les utilisateurs faisant confiance au réseau.

La dernière innovation marquante de la blockchain Ethereum est son développement des applications décentralisées. Basées sur sa monnaie ces applications vont directement utiliser les « smart contracts » pour proposer à leurs utilisateurs toutes sortes de services.

L'une des applications les plus en vogue est un système d'enchère permettant aux acheteurs de posséder virtuellement les droits d'une œuvre, ou de toute sorte de création numérique : il s'agit des NFT, les « Non-Fongible Tokens ».

## 2. Les enjeux de la blockchain

### 2.1. Un système prometteur

Depuis la mise en place de la première blockchain, la popularisation de la technologie ne cesse d'augmenter, et ses utilisations se diversifient. Beaucoup de secteurs d'activité essaient d'en exploiter les bénéfices, attirés par ses divers avantages.

#### 2.1.1. Exploiter une technologie inédite : les avantages de la blockchain

Tout d'abord, le système est décentralisé et distribué, ce qui signifie qu'il se débarrasse de tous les intermédiaires. Ces tiers servent dans la plupart des cas à connecter des utilisateurs à certains services. Cependant, les intermédiaires facturent des commissions pour chaque service qu'ils fournissent. Même si le montant de ces micropaiements peut sembler insignifiant, lorsqu'un service nécessite un processus en plusieurs étapes, ils s'additionnent.

De plus, il n'y a aucun moyen de juger si l'intermédiaire traite ses services de manière honnête et transparente. Dans de nombreux cas, ces intermédiaires ont tendance à abuser des entreprises et des consommateurs à des fins personnelles. Par conséquent, en se débarrassant de ces derniers le problème de confiance est résolu.

Avec la distribution des données, la technologie blockchain fournit un processus de consensus qui permet de filtrer toutes les informations de manière à ne garder que celles qui sont utiles, en éliminant toutes les données inutiles ou erronées. De plus, comme chaque information est vérifiée par un grand nombre d'observateurs, cela permet d'éliminer tous problèmes liés à l'erreur humaine. Ainsi, la qualité des données s'en trouve considérablement améliorée.

La blockchain offre à ses données une durabilité et une robustesse très forte. Parce que tous les blocs sont stockés et contrôlés par chaque nœud du réseau et non par une seule entité, s'il devait y avoir une défaillance sur l'un des nœuds, les informations resteraient intactes sur tous les autres. Cela rend le système intrinsèquement durable.

De plus, puisque personne ne peut éditer les blocs, la plateforme reste fiable et sécurisée. De part ces qualités, elle est également très efficace pour repousser les tentatives de piratage. Il est donc très difficile de neutraliser ce réseau.

Un autre grand avantage très lié est son niveau d'intégrité. Toutes les données sont toujours correctes, et une fois dans le registre personne ne peut les modifier, grâce au système de hash et de preuve de travail. En conséquent, il fournira des données précises et fiables chaque fois qu'une transaction sera effectuée.

Ensuite vient la transparence et l'immutabilité. La blockchain a un système de stockage immuable, et comme dit précédemment on ne peut modifier aucune forme de données, et encore moins les supprimer complètement. Le hachage cryptographique joue un rôle important dans le maintien de la structure.

Étant donné que chaque bloc a un hash servant d'identifiant, toute modification des données d'un bloc modifiera complètement son identifiant. Comme il est impossible de recréer le même hash, si quelqu'un essaie de modifier les données, tous les autres utilisateurs le remarqueront immédiatement.

La suppression des intermédiaires, le libre accès pour tous et l'absence d'autorité gouvernante œuvrent pour la simplicité du système. Étant donné que tout est en ligne, il n'y a pas de notion d'administratif. La seule chose à conserver pour l'utilisateur est souvent la clé qui va lui permettre de s'authentifier sur le réseau, comme la clé d'accès à un wallet pour le cas d'une blockchain monétaire par exemple. Ces différents points rendent la technologie facile d'utilisation.

Enfin, la blockchain offre une traçabilité exhaustive de l'ensemble des actions qui se passent sur son réseau, tout en pseudonymisant ses utilisateurs. Cela signifie que chaque action est traçable et ne peut pas être perdue, mais que l'identité des acteurs n'est pas accessible.

### 2.1.2. Diversification des utilisations de la technologie

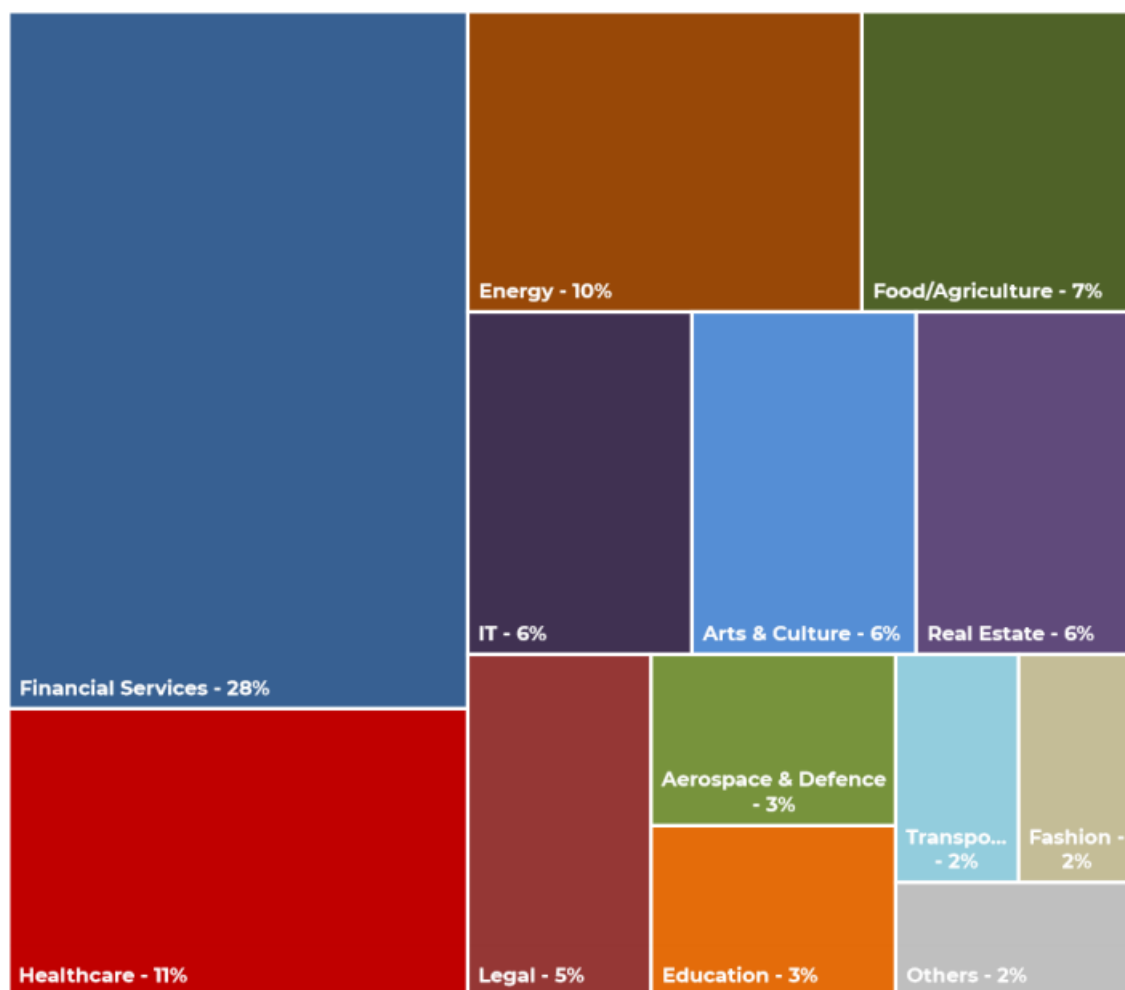


Figure 4 - Domaines d'application de la blockchain en 2020, par LeadBlock Partners

La première catégorie d'utilisations reste largement le domaine financier, avec les cryptomonnaies notamment. C'est l'utilisation originale de la technologie et de ce fait elle n'a pas forcément besoin d'être réinventée pour fonctionner. Bitcoin, Ethereum et plus généralement tous les altcoins (autres monnaies virtuelles basées sur Bitcoin) gardent le principe de blockchain publique, accessible à tous.

Or, ce principe n'est pas applicable à tous les domaines, car certaines données ne doivent pas être rendues publiques. C'est pourquoi d'autres types de blockchains commencent à se développer : les blockchains privées et permissionnées.

Dans une blockchain publique, tout le monde est libre de rejoindre et de participer aux activités principales du réseau de la blockchain. Tout le monde peut lire, écrire et vérifier les activités en cours sur le réseau blockchain public, ce qui permet à une blockchain publique de conserver sa nature autogérée, décentralisée, démocratisée et sans autorité.

La principale distinction entre les blockchains publiques et privées est que les blockchains privées contrôlent qui est autorisé à participer au réseau, qui peut prendre des décisions liées aux protocoles de consensus, qui décide des droits d'exploitation et des récompenses et qui maintient le registre partagé. Le propriétaire a le droit d'annuler, de modifier ou de supprimer les entrées nécessaires sur la blockchain selon ses besoins.

La troisième catégorie de blockchains est celle des blockchains permissionnées. Les blockchains permissionnées permettent un mélange entre les blockchains publiques et privées et prennent en charge de nombreuses options de personnalisations. Elles permettent notamment à quiconque de rejoindre le réseau après une vérification de son identité, et l'attribution de permissions sélectionnées et désignées pour effectuer uniquement certaines activités sur le réseau.

De telles blockchains sont construites de manière à accorder des permissions spéciales à chaque participant. Cela donne aux utilisateurs la possibilité d'exécuter des fonctions spécifiques telles que la lecture, l'accès et l'écriture d'informations sur les blockchains. Les entreprises optent de plus en plus pour des réseaux permissionnés, car cela leur permet de placer des restrictions de manière sélective lors de la configuration des réseaux, et de contrôler les activités des différents participants dans les rôles souhaités.

Ces nouvelles façons de voir et d'utiliser la blockchain offrent une porte d'entrée à différents secteurs d'activités.

Si on regarde la répartition des domaines d'application exposée plus haut, on peut voir que le secteur de la santé se situe à la deuxième place, prêt à investir dans les blockchains lui aussi.

C'est bien grâce au développement des blockchains privées et permissionnées que la collaboration est possible entre cet univers aux données très sensibles qu'est celui de la santé, et la technologie blockchain, basée à l'origine sur un principe de transparence totale.



Les dossiers médicaux personnels sont des données sensibles et doivent être traités avec une grande sécurité. Aujourd'hui, encore beaucoup de dossiers médicaux sont éparpillés, dû aux transferts entre différentes institutions médicales, ce qui entrave l'informatique liée à la santé. La blockchain offre une opportunité de créer une plateforme d'enregistrement fiable. Avec la blockchain, les dossiers de soins de santé très fragmentés peuvent être regroupés pour faciliter leurs suivis.

Ces dossiers peuvent être chiffrés et stockés à l'aide de blockchain et fournir une clé privée qui ne permettrait qu'à des personnes spécifiques d'accéder à ceux-ci. Les praticiens de santé pourraient envoyer les dossiers médicaux aux parties concernées en toute sécurité. Cela pourrait également aider à mener des recherches où les dossiers personnels seraient utilisés.

Les problèmes de confidentialité, la fragmentation et la complexité inhérente aux dossiers médicaux rendent le diagnostic basé sur l'historique coûteux. Avec la blockchain, le suivi continu des dossiers par l'ensemble des acteurs médicaux autorisés pourrait être réalisé à moindre coût. De plus, certains affirment que la combinaison de l'intelligence artificielle et de la blockchain pourrait conduire à des solutions à de nombreux problèmes de santé.

Cependant, l'accès aux dossiers de santé constitue un dilemme éthique : en plus des obstacles techniques tels que l'accès et le stockage des données dans la blockchain, il y a aussi des obstacles liés aux politiques nationales et à la protection de la vie privée.

On peut voir que d'autres domaines sont eux aussi très intéressés par la blockchain. D'autres technologies sont utilisées et combinées avec celle-ci par certains de ces domaines pour se développer : L'IoT (internet des objets) est exploité à différents niveaux :

Pour le transport de marchandises : c'est un processus complexe impliquant différentes parties. Une blockchain compatible avec l'IoT peut stocker les températures, la position, les heures d'arrivée et le statut des conteneurs d'expédition pendant leur déplacement. Les transactions blockchain immuables permettent de s'assurer que toutes les parties peuvent faire confiance aux données et prendre des mesures pour déplacer les produits rapidement et efficacement.

Le suivi des composants et de leur conformité : La capacité de suivre les composants qui entrent dans un avion, une automobile ou d'autres produits, est essentielle à la fois pour la sécurité et la conformité réglementaire. Les données IoT stockées dans des blockchains permettent à toutes les parties de voir la provenance des composants tout au long de leur vie. Le partage de ces informations avec les organismes de réglementation, les expéditeurs et les fabricants est sécurisé, facile et rentable.

L'enregistrement des données de maintenance opérationnelle : les dispositifs IoT suivent l'état de sécurité des machines critiques et de leur maintenance. La blockchain fournit un registre inviolable des données opérationnelles et de la maintenance qui en résulte. Les partenaires tiers peuvent surveiller la blockchain pour la maintenance préventive et enregistrer leur travail dessus. Les enregistrements opérationnels peuvent également être partagés avec des entités gouvernementales pour en vérifier la conformité.

Pour finir, nous pouvons prendre l'exemple d'application le plus connu en France : la blockchain utilisée par Carrefour pour tracer la vie de certains produits. Le groupe s'est associé à IBM en 2019 afin d'améliorer sa logistique et la traçabilité de ses produits : à partir d'un QR code apposé sur un produit, le consommateur peut visualiser toutes les informations relatives à un produit pour en connaître la provenance, le producteur, les différentes dates d'emballage et d'autres plus spécifiques à chaque produit.

## 2.2. Un système controversé

### 2.2.1. Des contreparties fortes : les désavantages de la blockchain

Les blockchains consomment trop d'énergie. Le minage avec preuve de travail est extrêmement énergivore et augmente considérablement avec le temps. Même si beaucoup de nouveaux systèmes commencent à prendre ce critère en compte en développant d'autres méthodes de minage, la preuve de travail reste la plus répandue à l'heure actuelle.

En raison de la nature des blockchains, elles peinent à se rapprocher de la vitesse des bases de données centralisées. Lorsqu'une transaction est traitée, une blockchain doit faire les mêmes choses qu'une base de données ordinaire, mais elle supporte également trois charges supplémentaires :

- La vérification des signatures est une action obligatoire à la validation d'une transaction. Dans les bases de données centralisées, une fois qu'une connexion a été établie il n'est pas nécessaire de vérifier individuellement chaque requête.
- Les mécanismes de consensus ralentissent également les processus. Dans une base de données distribuée telle qu'une blockchain, des efforts doivent être déployés pour s'assurer que les nœuds du réseau parviennent à un consensus. Lorsque la chaîne rencontre des cas de « fourches », quand différents blocs sont validés simultanément, le réseau doit attendre que l'une des branches se démarque pour la garder, au détriment de la seconde.

Cela entraîne des communications supplémentaires entre tous les nœuds du réseau, et les transactions faisant partie des branches non conservées devront attendre à nouveau d'être validées. S'il est vrai que les bases de données centralisées doivent également faire face à des transactions contradictoires et avortées, celles-ci sont beaucoup moins probables lorsque les transactions sont mises en file d'attente et traitées en un seul endroit.

- La redondance. Il ne s'agit pas de la performance d'un nœud individuel, mais de la quantité totale de calculs que nécessite une blockchain. Alors que les bases de données centralisées traitent les transactions une ou deux fois, dans une blockchain, elles doivent être traitées

indépendamment par chaque nœud du réseau. Il y a donc plus de travail pour le même résultat final.

Le bitcoin et les autres blockchains présentent un défaut de sécurité notable : si plus de la moitié des ordinateurs travaillant comme nœuds pour desservir le réseau disent un mensonge, celui-ci devient la vérité. Ce phénomène, appelé "attaque à 51 %", a été mis en évidence par Satoshi Nakamoto lorsqu'il a lancé le bitcoin. C'est pour cette raison que les fermes de minage sont surveillées de près par la communauté, afin de s'assurer que personne n'acquiert une telle influence sur le réseau, à l'insu des autres utilisateurs.

Protégés par pseudonymisation, les utilisateurs d'une blockchain s'exposent tout de même aux limites de ce principe. Si un individu publie quelque chose sur internet sous un pseudonyme, son anonymité n'est pas pour autant assurée.

En effet, un pseudo permet de dissocier une identité réelle de celle donnée par celui-ci, cependant cela ne fonctionne que s'il n'existe aucun lien entre celles-ci. Dans ce sens on peut donner l'exemple du créateur de Bitcoin encore inconnu à ce jour, se cachant sous l'identité de Satoshi Nakamoto.

À l'inverse, s'il existe un lien accessible à la communauté permettant d'associer ces deux identités réelle et virtuelle, alors l'individu n'est plus protégé. Représenté par une adresse, ses transactions pourront être tracées s'il l'associe publiquement à son identité réelle.

### 2.2.2. Les impacts et risques d'un nouveau marché financier

De part ses avantages, la blockchain a joué, joue et jouera un rôle positif à de nombreux niveaux. Toutefois, le développement de la technologie se fait non sans mal. Nous allons voir certains des impacts directement liés à la technologie.

#### 2.2.2.1. *Une explosion de l'économie spéculative*

Un rapport de la bourse Crypto.com estime qu'il y avait 106 millions d'utilisateurs de cryptomonnaies dans le monde en janvier 2021, après un bond de 16 % dans le mois, suite à l'explosion de valeurs

qu'ont pris le Bitcoin et l'ensemble des actifs les plus populaires. Là où le sujet n'intéressait que certains enthousiastes des milieux informatiques et économique, aujourd'hui même les plus jeunes commencent à investir dans toutes sortes de cryptomonnaies.

Basé sur des cours très volatiles, le marché des cryptomonnaies participe largement à la popularisation de l'économie spéculative.

### 2.2.2.2. Un nouveau moyen de paiement pour les marchés illégaux

Par son caractère libertarien, la blockchain a souvent été décriée pour la facilité qu'elle offre aux commerces illicites.

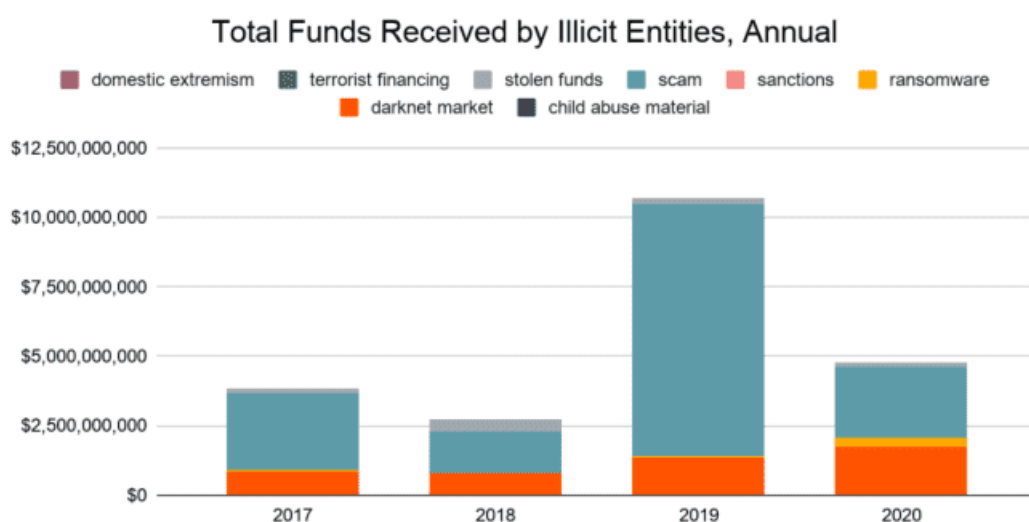


Figure 5 - Fonds reçus par des entités illicites entre 2017 et 2020, par Chainalysis

Comme on peut le voir sur ce graphique, la plupart des actions illicites traquées correspondent à des arnaques. Les arnaques en ligne existent depuis la création d'internet, se basant sur la crédulité et l'ignorance de leurs victimes. Étant accessible à tous, Internet n'est pas toujours sécurisé et ses utilisateurs doivent souvent agir à leurs risques et périls. Il en va de même pour l'utilisation des blockchains, dans le domaine des cryptomonnaies notamment.

Même si la technologie est bien souvent sécurisée, les moyens d'y accéder ne le sont pas toujours, comme les gestionnaires de « wallets » et les plateformes d'échanges par exemple. L'absence de gouvernance joue un rôle important sur cet aspect, mais il est aussi largement exploité par les marchés noirs qui y trouve un moyen d'échanger des fonds, matériels et services sans être inquiétés.

### *2.2.2.3. Un impact environnemental fort*

Selon l'université de Cambridge, une seule transaction de bitcoin a la même empreinte carbone que 680 000 transactions Visa ou 51 210 heures de visionnage de YouTube. Estimant quotidiennement la consommation électrique du Bitcoin, ils ont recensé le 14 mai 2021 un record qui, de manière annualisée, a atteint les 150 TWh. Si le bitcoin était un pays, il se placerait dans le top 30 des pays les plus consommateurs d'électricité au niveau mondial.

Une autre conséquence négative des cryptomonnaies concerne le matériel informatique. La courte durée de vie des plateformes de minage peut entraîner une quantité importante de déchets électroniques dans les années à venir. Les dispositifs de minage exacerbent également la pénurie mondiale actuelle de puces en se disputant les mêmes puces que les appareils électroniques personnels et les véhicules électriques.

### *2.2.2.4. Un nouvel enjeu économique pour certains pays*

Les pays où l'électricité est bon marché, comme l'Iran, peuvent créer de nouvelles sources de revenus grâce au minage de bitcoins. Cette évolution peut permettre à l'Iran d'atténuer les sanctions économiques imposées aux exportations de pétrole, qui empêchent le développement d'armes nucléaires et menacent la sécurité internationale. L'activité minière en Iran représente déjà 8 % de la puissance de calcul totale du réseau Bitcoin.

La Chine est depuis longtemps le pays possédant le plus de mineurs sur le réseau Bitcoin. Sa position est partagée : d'un côté, l'apport économique de ce marché est très intéressant pour l'État. De l'autre, la Chine, connue pour sa gouvernance forte, a du mal à statuer sur l'avenir d'une monnaie sur laquelle elle ne contrôle pas toutes les transactions.

Au cours du mois de mai 2021, l'État a annoncé sanctionner les transactions Bitcoin pour ses ressortissants, entraînant une baisse drastique du prix de la monnaie. Toutefois, ce n'est pas la première fois qu'elle annonce ce genre de mesure, n'apportant pas pour l'instant de réels changements à long terme sur le réseau.

Cependant, l'État mène une deuxième bataille en parallèle, qui pourrait être fortement liée à la première.

La cryptomonnaie officielle de la Chine est connue sous le nom de e-Yuan, et son développement a attiré l'attention du monde entier. Les investisseurs sont impatients d'acquérir une part de la nouvelle monnaie, dans l'espoir qu'elle atteigne les niveaux atteints par le Bitcoin.

L'État chinois contrôlera la manière dont la cryptomonnaie circulera et seuls les banques et les courtiers agréés seront autorisés à vendre l'e-Yuan dans un premier temps.

Lancé par une telle puissance mondiale, l'e-Yuan devrait s'assurer d'éviter les risques de chutes de son prix trop prématurés, car soutenu par la Chine s'il commence à chuter de manière drastique.

### *2.2.2.5. L'arrivée des ordinateurs quantiques : une menace de taille*

L'informatique quantique aura un impact direct sur les blockchains.

La plupart des avantages des blockchains découlent de leur attrait pour la sécurité, car la blockchain est une technologie innovante qui a prouvé qu'elle apportait des avantages considérables dans de nombreux domaines en assurant de manière inhérente la sécurité, l'interopérabilité et la durabilité.

La blockchain est considérée comme une technologie décentralisée permettant de partager des informations et d'effectuer des transactions de manière sécurisée. L'une des caractéristiques les plus importantes est l'immuabilité. Les données, les hash et les signatures d'une blockchain sont censés être infailibles et doivent assurer la sécurité des transactions pour toute la durée de vie du réseau.

À l'heure actuelle, les algorithmes cryptographiques classiques sont toujours utilisés dans la technologie blockchain. Or, il a été prouvé que des algorithmes quantiques peuvent casser les algorithmes de hachage les plus sûrs comme le RSA, le DSA et l'ECDSA.

En conséquent, comme la technologie blockchain est basée sur ces algorithmes, sa sécurité est affectée par l'avènement de l'informatique quantique.

En raison de l'explosion que vont créer les ordinateurs quantiques, des algorithmes sont en cours de conception et d'évaluation afin de remplacer ceux qui deviendront faillibles dans les années à venir.

## Conclusion

La blockchain est un système fascinant, de ses principes techniques jusqu'aux utilisations qu'on en fait, et qui ne cessent de se développer au cours du temps.

Créée en 2008 à partir de recherches datant pour les premières du 20<sup>ème</sup> siècle, la technologie s'est développée jusqu'à atteindre le niveau de popularité qu'elle connaît aujourd'hui.

Cultivant divers avantages permettant à une multitude de secteurs d'activité de se développer, la blockchain a su jusqu'à maintenant s'adapter au monde dans lequel elle évolue.

Toutefois, une technologie aux nombreux avantages ne peut exister sans son lot d'inconvénients, qui impactent plus ou moins fortement différents secteurs.

Basée sur des principes cryptographiques qui se sont montrés jusqu'à lors comme très résistants, il se pourrait qu'ils commencent à trembler dès les premières utilisations publiques d'ordinateurs quantiques.

De ces différents enseignements découlent une multitude de questions, qui seront représentées par une seule et même problématique.

## Problématique

Comment la technologie blockchain peut-elle s'imposer comme une solution novatrice pour différents secteurs d'activité alors qu'elle est confrontée à des risques qui remettent en question ses principes fondamentaux ?



## Perspectives d'évolution envisagées

Nous avons vu jusqu'ici le fonctionnement de la technologie blockchain ainsi que ses différents enjeux, s'installant depuis plusieurs années. À partir des points observés dans cet état de l'art, le but sera de tirer des conclusions afin d'anticiper quelles seront les réponses de ce système novateur, face aux problématiques auxquelles il sera confronté dans les années à venir.

Afin de réaliser ce mémoire de recherche nous aurons besoin d'établir une stratégie qui nous permettra de formuler des hypothèses qui tenteront de répondre à la problématique soulevée.

Pour ce faire, nous devons procéder à une enquête auprès de professionnels qui font de la blockchain leur quotidien, tout en obtenant l'avis de ceux qui travaillent sur l'avancée de la technologie qui se présente comme une épée de Damoclès pour la blockchain, à savoir l'informatique quantique.

Il faudra enfin analyser les résultats obtenus, pour les confronter aux informations remontées dans l'état de l'art.