Chapitre 2 : État de l'art sur la technologie Blockchain

2.1 Présentation et historique

La Blockchain est une invention indéniablement ingénieuse, née d'une personne ou d'un groupe de personne connu sous le nom de Satoshi Nakamoto. Mais depuis lors, il a évolué pour devenir quelque chose de plus grand, et la principale question que chaque personne se pose est la suivante : Qu'est-ce que la Blockchain ?

- En termes simples, une Blockchain est un grand livre distribué qui permet à une communauté d'enregistrer et de partager des informations.
- Dans cette communauté, chaque membre conserve sa propre copie des informations et tous les membres doivent valider les mises à jour collectivement.
- Les informations peuvent représenter des transactions, des contrats, des actifs, des identités ou pratiquement tout ce qui peut être décrit sous forme numérique.
- Les entrées sont permanentes, transparentes et interrogeables, ce qui permet aux membres de la communauté de visualiser l'historique des transactions dans son intégralité.
- Chaque mise à jour est un nouveau "bloc" ajouté à la fin d'une "chaîne".
- Un protocole gère la manière dont les nouvelles éditions ou entrées sont initiées, validées, enregistrées et distribuées. Avec Blockchain, la cryptologie remplace les intermédiaires tiers en tant que détenteur de la confiance, tous les participants à la Blockchain exécutent des algorithmes complexes pour certifier l'intégrité de l'ensemble.

La première chaîne de blocs connus était la chaîne de blocs Bitcoin, qui est également le nom de la première crypto-monnaie décentralisée et largement utilisée. « Bitcoin » fait également référence au protocole réseau sous-jacent à la crypto-monnaie.

En termes de langage populaire, la Blockchain Bitcoin est automatiquement associée à la 'Blockchain' alors qu'en pratique, il existe d'autres Blockchain d'une importance considérable, tels que la Blockchain Ethereum.

2.1.1 Crypto-monnaie Bitcoin

La monnaie virtuelle Bitcoin est la première monnaie libre et décentralisée capable de fonctionner à l'échelle du monde sans autorité centrale. Les Bitcoins sont non seulement impossibles à usurper ou à contrefaire, mais ils représentent aussi la première monnaie mondiale neutre et séparée de la politique. Tout cela grâce à un usage ingénieux de la mathématique et de la cryptographie.

Bitcoin a été introduit pour la première fois sur une liste de diffusion cryptographique le 31 octobre 2008 et a été publié en tant que logiciel à code source ouvert en 2009. L'idée de construire cette monnaie numérique ou virtuelle est de construire un système décentralisé qui permettrait à la monnaie de pouvoir être transférée électroniquement avec des frais de transaction négligeables ou nuls. Il s'agit du premier réseau peer-peer qui permet à ses utilisateurs de ne disposer d'aucune autorité centrale ni de banques. Ces Bitcoins sont construits à partir d'un protocole Bitcoin. Selon ce protocole, il y aurait un nombre défini de Bitcoins pouvant être produits (extraits), soit 21 millions. Cependant, chaque Bitcoin peut être divisé en parties plus petites pouvant aller jusqu'à un centième de Bitcoin. Cette plus petite division du Bitcoin est appelée "Satoshi". Bitcoin a des utilisateurs qui sont répandus à travers le monde et il n'est pas contrôlé par une seule personne. Du point de vue de l'utilisateur, Bitcoin est une application qui fournit un portefeuille et permet aux utilisateurs d'effectuer des transactions entre eux. Pour effectuer des transactions, les utilisateurs sont libres d'utiliser le logiciel de leur choix, à condition que le logiciel soit compatible et respecte les règles du protocole Bitcoin. Ce système de paiement électronique repose sur une preuve cryptographique plutôt que sur la confiance, raison pour laquelle le besoin d'un tiers est éliminé. Les transactions effectuées sont pratiquement impossibles à inverser ou à détruire. [1]

Le Bitcoin peut être comparé à un porte-monnaie d'argent liquide. Tout comme un porte-monnaie réel, il est possible de conserver de l'argent et le protéger soi-même (encrypter et sauvegarder son porte-monnaie). Ou alors, il est possible de stocker de l'argent dans une banque en ligne comme Coinbase.

Il s'agit du premier réseau peer-peer qui permet à ses utilisateurs de ne disposer d'aucune autorité centrale ni de banques. Ces Bitcoins sont construits à partir d'un protocole Bitcoin. Selon ce protocole, il y aurait un nombre défini de Bitcoins pouvant être produits (extraits), soit 21 millions. Cependant, chaque Bitcoin peut être divisé en parties plus petites pouvant aller jusqu'à un centième de Bitcoin. Cette plus petite division du Bitcoin est appelée "Satoshi".

Personne n'est propriétaire du réseau Bitcoin tout comme personne ne possède la technologie derrière l'e-mail ou Internet. Les transactions Bitcoin sont vérifiées par les mineurs Bitcoin. Alors que les développeurs améliorent le logiciel, ils ne peuvent pas forcer un changement dans le protocole Bitcoin car tous les utilisateurs sont libres de choisir quel logiciel et quelle version ils souhaitent utiliser.

2.1.2 Crypto-monnaie Ethereum

Ethereum est un protocole d'échanges décentralisés permettant la création par les utilisateurs de contrats intelligents. Ces contrats intelligents sont basés sur un protocole informatique permettant de vérifier ou de mettre en application un contrat mutuel. Ils sont déployés et consultables publiquement dans une Blockchain.

Il utilise une unité de compte dénommée Ether comme moyen de paiement de ces contrats. Son sigle correspondant, utilisé par les plateformes d'échanges, est « ETH ».

Ethereum, pris dans son ensemble, peut être vu comme une machine à état basée sur des transactions : nous commençons avec un état originel et nous exécutons des transactions de manière incrémentale pour le transformer en un état final. C'est cet état final que nous acceptons comme la « version » canonique du monde d'Ethereum. L'état peut inclure des informations telles que les soldes de comptes, la réputation, des accords de confiance, des données portant sur l'information du monde physique ; en résumé, tout ce qui peut actuellement être représenté par un ordinateur est admissible. [1]

Le but d'Ethereum est de créer un protocole alternatif pour construire des applications décentralisées, fournissant un ensemble différent de compromis que nous pensons être très utile pour une vaste classe d'applications décentralisées, avec un accent particulier sur les situations où le développement rapide, la sécurité des petites applications rarement utilisées et la possibilité pour les différentes applications d'interagir ensemble de manière très efficace sont importants. Ethereum fait cela en construisant ce qui est essentiellement la couche fondamentale abstraite ultime : une Blockchain intégrant un langage de programmation Turing-complet, permettant à quiconque de rédiger des smart-contracts (contrats autonomes) et des applications décentralisées où l'on peut créer ses propres règles concernant la propriété, les formats de transaction et les fonctions de transition d'état.

2.1.3 Comparaison avec autres crypto-monnaie

Tableau 1: comparaison de Bitcoin, Ethereum, Bitcoin cash

EXTRAIT DE : HTTPS://FR.WIKIPEDIA.ORG/WIKI/CRYPTOMONNAIE

Code	Monnaie	Date création	Equivalent de la masse monétaire en USD	Algorithme	Quantité de monnaie émise	Qtité max pouvant être émise	**Note**
BTC, XBT	Bitcoin	2009	125 milliards USD au 04/09/2018	SHA-256 (preuve de travail)	17 millions au 16/05/2018	21 millions	La première monnaie décentralisée.
ETH	Ethereum	2015	29 milliards USD au 04/09/2018	Ethash	99,4 millions au 16/05/2018	Non limitée	La première monnaie basée sur une chaîne de blocs (Ethereum) permettant la création de contrats intelligents.
BCH, BCC	Bitcoin Cash	2017	10 milliards USD au 04/09/2018	SHA-256 (preuve de travail)	17 millions au 16/05/2018	21 millions	Fork de la chaîne de blocs Bitcoin avec augmentation de la taille maximale d'un bloc. Le but est de mieux faire face à la croissance du nombre d'utilisateurs.

2.2 Ledger (Grand livre)

Les grands livres sont des outils permettant de déterminer le propriétaire d'un actif à tout moment. Ils remplissent cette fonction en servant de liste centrale.
Dans un système ou une société qui a accepté d'utiliser un grand livre pour déterminer la propriété d'un actif particulier, tout ce qui est nécessaire pour transférer la propriété entre deux parties, est de faire une entrée dans le grand livre indiquant que cela est arrivé.
D'un point de vue technique, un grand livre est simplement une liste de transactions séquentielles horodatées, structurées comme suit :

Tableau 2 : Entrée typique du grand livre

Transaction	Date & times	Sender	Asset	Receiver
$	dd-mm-yy hh-mn	Person 1	Description de l'actif transféré d'une unité de monnaie, d'un acte de propriété à une propriété ou d'un certificat	Person 2
$	dd-mm-yy hh-mn	Person 1	Description de l'actif transféré d'une unité de monnaie, d'un acte de propriété à une propriété ou d'un certificat	Person 2

Ce concept simple consiste à conserver une liste de transfert d'actifs faisant autorité, permet le transfert et l'accumulation systématiques de capital et a été qualifié de technologie essentielle. La personne ou l'organisation qui possède ou contrôle physiquement un grand livre public (y compris le serveur sur lequel réside le grand livre, dans le cas d'un grand livre public en ligne) jouit d'un pouvoir et d'une influence significatifs. Plus précisément, le propriétaire du grand livre peut :

- Décider s'il faut enregistrer une transaction, ce qui donne à cette personne la possibilité d'imposer des conditions aux personnes pour que leurs transactions soient enregistrées ;
- Décider du système de contrôles à appliquer pour vérifier l'exactitude des transactions ;
- Modifier ou supprimer des transactions déjà dans le grand livre ;
- Détruire le grand livre entièrement, ou permettre sa destruction.

Comme dans un tel système, écrire, modifier ou supprimer une transaction dans le grand livre modifie également la propriété de l'objet, la personne ou l'organisation qui contrôle de tels grands exerce également une influence notable en contrôlant efficacement qui détient quoi simplement en étant le gardien de la liste des transactions.

La responsabilité de la tenue de grands livres de comptes a toujours été confiée à diverses institutions : les gouvernements contrôlent la propriété des terres en contrôlant les grands livres de biens ; les banques contrôlent le système monétaire mondial en tenant les grands livres pour la monnaie ; tandis que les bourses contrôlent une grande partie du monde des affaires en tenant des grands livres pour la propriété des entreprises. Puisque les sociétés capitalistes sont construites autour des concepts de vente et de propriété (transfert et accumulation de capital), la responsabilité de la conservation des grands livres implique de grandes responsabilités.
Plus précisément, on fait confiance à ces autorités centrales pour :

- Fournir un témoin : c'est à dire certifier l'identité et s'assurer que les personnes inscrites dans le grand livre sont bien ce qu'elles prétendent être et que les actifs transférés existent ;
- Être honnête et transparent dans toutes les transactions, c'est-à-dire ne pas céder les utilisateurs de leurs actifs en créant de fausses transactions ou en modifiant illégalement des transactions après leur création ;
- Être en sécurité : c'est à dire s'assurer que des tiers non autorisés ne peuvent ni lire ni écrire dans le grand livre (piratage) ;
- Ne pas abuser de leur monopole en imposant des coûts injustes / exceptionnels à leurs services ;
- Permettre aux personnes d'effectuer des transactions, c'est-à-dire de donner accès à toute personne ayant un intérêt légitime à effectuer des transactions en les inscrivant sur le grand livre.

2.2.1 Blockchain en tant que grands livres publics

L'application la plus connue d'une Blockchain est celle d'un grand livre public de transactions pour des crypto-monnaies, telles que Bitcoin et Ether. Comme dans le cas des autres registres publics, le registre Blockchain fournit l'enregistrement de la provenance et du transfert de propriété d'un actif. La structure transactionnelle des protocoles de chaîne de blocs facilite non seulement le transfert de crypto-monnaie, mais également d'autres ressources numériques.
Pratiquement tout ce qui a de la valeur peut être suivi et échangé sur un réseau de Blockchain, réduisant ainsi les risques et les coûts pour toutes les parties concernées. Dans la mesure où ils sont conçus pour enregistrer et préserver les transactions, toutes les chaînes de blocs sont traditionnellement associées à une monnaie numérique, ce qui en fait l'actif le plus fondamental sur l'ensemble du réseau. Cela a également incité à adopter le protocole de cette chaîne en payant les contributeurs au réseau dans sa propre crypto-monnaie.

Les Blockchains sont donc des ledgers qui enregistrent des groupes de transactions, autrement appelés blocs, qui sont reliés entre eux par cryptographie.

2.2.2 Concept de la Blockchain

Une Blockchain, ou chaîne de blocs, est définie comme une base de données distribuée (ledger) qui conserve un enregistrement permanent et immuable (infalsifiable) des données transactionnelles liées entre elles par une chaîne (par blocs).

Tableau 3 : Comparaison entre Blockchain et Base de données

Propriétés	Blockchain	Base de données traditionnelle
Opérations	Seulement des opérations d'insertion	Peut effectuer des opérations CRUD
Réplication	Réplication complète du bloc sur chaque pair	Maître esclave multi-maître
Consensus	La majorité des pairs s'accordent sur le résultat des transactions	Transactions distribuées (validation en 2 phases)
Invariants	Tout le monde peut valider les transactions sur le réseau	Contraintes d'intégrité

Une Blockchain est un système totalement décentralisé et basé sur un réseau pair à pair (peer-to-peer). Chaque objet du réseau conserve une copie du ledger afin d'éviter d'avoir un point unique de défaillance. Toutes les copies sont mises à jour et validées simultanément. Bien que l'objectif initial de la création de la Blockchain fût la résolution du problème de la dépense multiple en crypto-monnaie (monnaie virtuelle). Cette technologie peut être explorée dans de nombreux cas d'utilisation et utilisée comme un moyen sécurisé de gestion et protection de toute sorte de données (monétaire ou pas)

Le ledger est composé d'un ensemble de blocs. Chaque bloc contient deux parties. La première partie représenté le corps du bloc. Il contient les transactions, que la base de données doit enregistrer. Ces transactions peuvent être des transactions monétaires, des données médicales, des informations industrielles, des logs systèmes, etc. La deuxième partie est l'entête (header) du bloc. Ce dernier contient des informations concernant le bloc tel que l'horodatage (time-stamp), le hach des transactions, etc. Ainsi que le hachage du bloc précédent. De ce fait, l'ensemble des blocs existants forme une chaîne de blocs liés et ordonnés. Plus la chaîne est longue, plus il est difficile de la falsifier.

En effet, si un utilisateur malicieux veut modifier ou échanger une transaction sur un bloc, (1) il doit modifier tous les blocs suivants, puisqu'ils sont liés par leurs hash, (2) ensuite, il doit changer la version de la chaîne de blocs que chaque objet participant stocke.

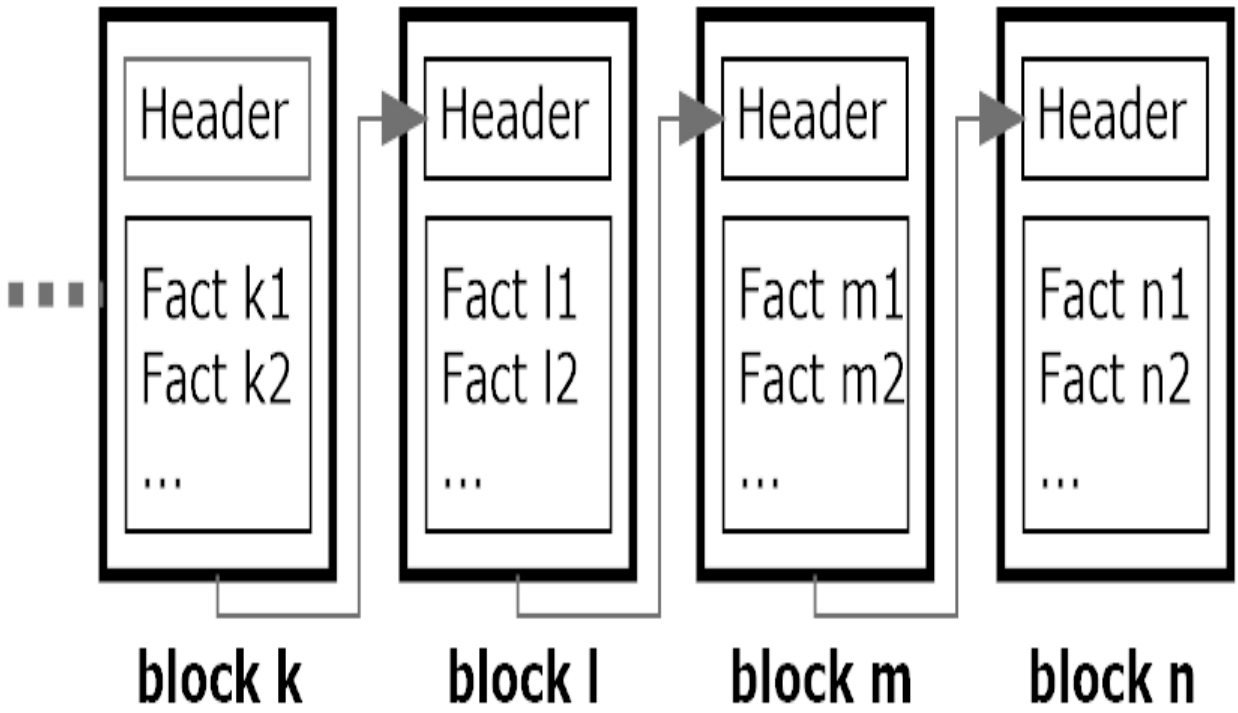


Figure 1 : Exemple simplifie d'une Blockchain **[I1]**

Une Blockchain suit un réseau P2P. il s'agit essentiellement d'un cadre de réseau multi-réseaux intégré entre pairs, composé de cryptographie, d'algorithmes et d'expressions mathématiques visant à résoudre les limitations classiques de la synchronisation de bases de données distribuées à l'aide d'algorithmes de consensus distribués.

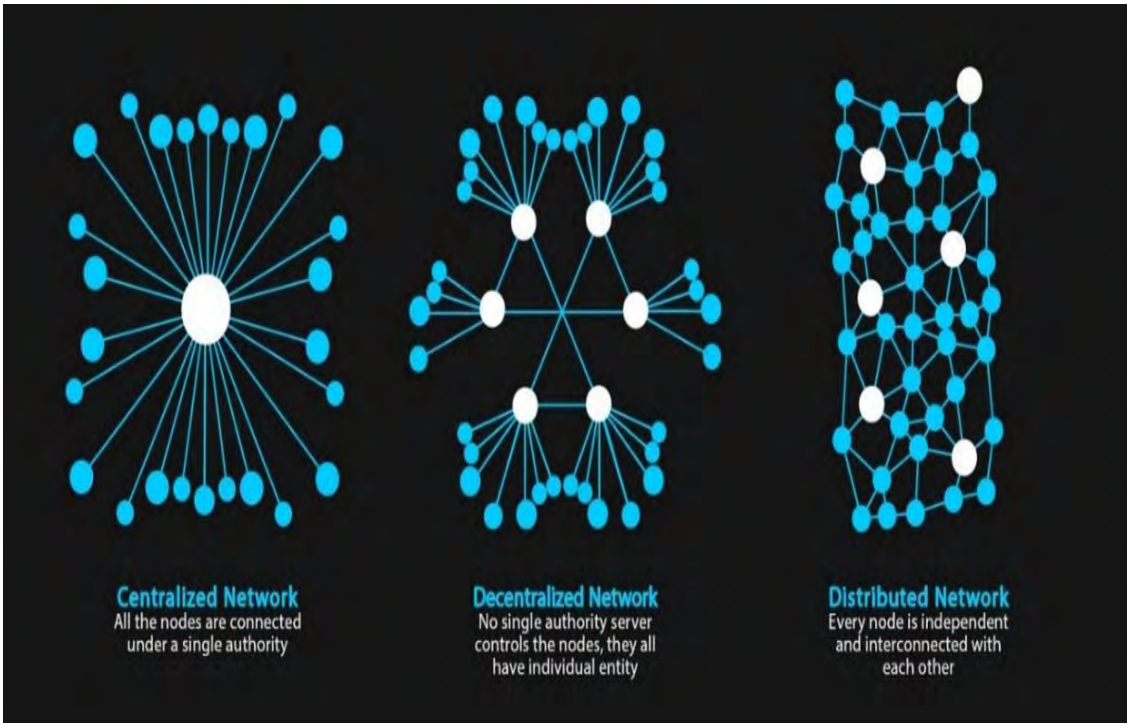


Figure 2 : De gauche à droite, réseaux centralisés, décentralisé et distribué **[I2]**

La figure 2 montre les différentes topologies de réseau ; centralise, décentralisé et distribue, qui sont les types de réseau de la technologie Blockchain.

La technologie Blockchain se caractérise principalement de six éléments majeurs : décentralisé, transparente, sécurisé et immuable, autonome, open source et anonyme. Comme décrit ci-dessus :

- **Elle est décentralisé** : La Blockchain contient un système de bases de données décentralisé avec un contrôle en libre accès pour tous ceux qui sont connectés au réseau. Les données peuvent être consultées, surveillées, stockées et mises à jour sur plusieurs systèmes.

  Ces données ne sont pas toutes regroupées dans le serveur d'un intermédiaire central, mais au contraire « distribuées », c'est à dire hébergées chez chaque participant ; il n'y a donc pas d'autorité unique pouvant approuver les transactions ou définir des règles spécifiques pour que les transactions soient acceptées. Cela signifie que la confiance est énorme, car tous les participants du réseau doivent parvenir à un consensus pour accepter les transactions.

- **Elle est transparente** : C'est l'avantage le plus important. Tous les participants peuvent voir les blocs et les transactions qui y sont stockés dedans. Les données enregistrées et stockées dans la Blockchain sont transparentes pour les utilisateurs potentiels et peuvent être mises à jour facilement. Cela ne signifie toutefois pas que tout le monde peut voir le contenu réel des transactions, qui sont protégés par une clé privée.

Comme dans le réseau Bitcoin, toutes les transactions sont publiques et vérifiables par tous en effectuant un mécanisme consensus, ce qui va permettre à chacun de s'assurer que chaque participant possède bien les Bitcoins qu'il dépense et qu'il ne les dépense qu'une seule fois. La nature transparente des Blockchains pourrait certainement empêcher la modification ou le vol de ces données.

- **Le consensus** : la Blockchain correspond à un historique de transactions sur lequel tout le monde s'accorde, ce consensus sur le séquencement des transactions permet de résoudre le problème dit de la "double dépense" : un Bitcoin dépensé dans une transaction ne peut pas être dépensé une deuxième fois dans une transaction qui serait diffusée ultérieurement sur le réseau. La deuxième transaction serait rejetée par le réseau.
- **Elle est sécurisé** : La base de données peut uniquement être étendue et les enregistrements précédents ne peuvent pas être modifiés (au moins, le coût est très élevé si quelqu'un souhaite modifier les enregistrements précédents).

Ces enregistrements sont dits Immuables, une fois stockés, deviennent réservés pour toujours et ne peuvent pas être modifiés facilement sans le contrôle simultané de plus de 51% des nœuds du réseau.

Le système cryptographique de validation garantit qu'il est quasiment impossible de réécrire une transaction une fois son bloc validé (personne n'a réussi à le faire depuis la création du Bitcoin).

- **Autonome :** Le système Blockchain est indépendant et autonome, ce qui signifie que chaque nœud du système Blockchain peut accéder aux données, les transférer, les stocker et les mettre à jour en toute sécurité, ce qui les rend fiables et exemptes de toute intervention externe.

- **Open source :** La technologie de la Blockchain est formulée de manière à fournir un accès open source à toutes les personnes connectées au réseau. Cette polyvalence inimitable permet à quiconque non seulement de vérifier publiquement les enregistrements, mais également de développer diverses applications imminentes.

- **Anonyme :** Lorsque le transfert de données à lieu entre nœuds, l'identité de l'individu reste anonyme, ce qui en fait un système plus sécurisé et fiable.

Une personne faisant partie de ce réseau doit vérifier chaque nouvelle transaction effectuée. Une transaction de recherche dans un bloc d'une Blockchain est vérifiée par tous les nœuds du réseau, elle devient de plus en plus immuable.

La figure 3 ci-dessous illustre le flux de travail du processus de la chaîne de blocs.

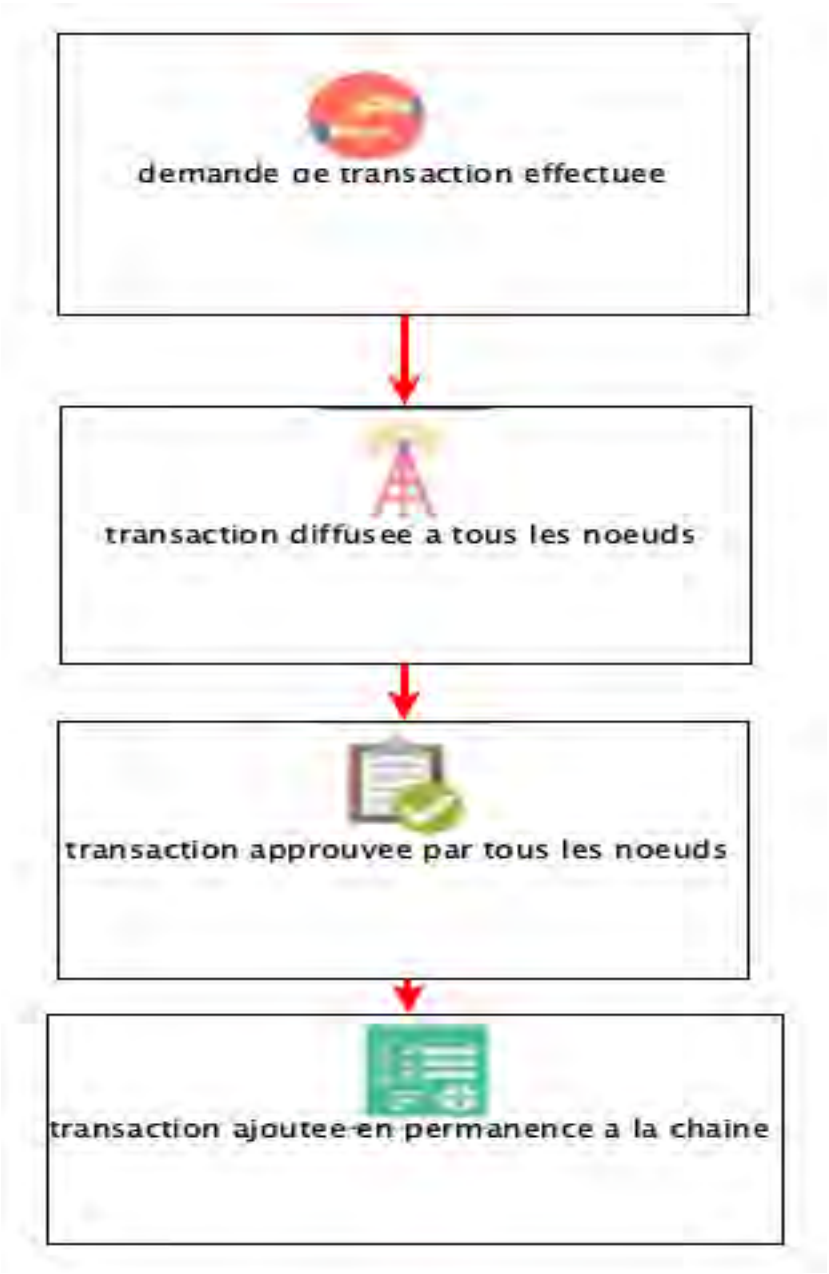


Figure 3 : Un flux de travail généralisé du processus de Blockchain [I3]

Il existe deux types d'objets participants dans la Blockchain : (1) des objets qui peuvent uniquement lire les transactions (mode passif), et (2) des objets qui peuvent lire et écrire des transactions (mode actif) appelés mineurs. Afin de rajouter un nouveau bloc à la Blockchain, il faut suivre les étapes suivantes :

- Une transaction est regroupée avec d'autres transactions dans un bloc ;
- Les mineurs vérifient quel est transactions du bloc respectent les règles définies ;
- Les mineurs exécutent un mécanisme de consensus pour valider le bloc ajouté.
- Une récompense est donnée aux mineur/mineurs qui valident le bloc ;

- Les transactions vérifiées sont stockées dans la Blockchain.

Afin de prouver la validation honnête d'un bloc, il existe de nombreux mécanismes de validation. Les plus utilisés sont le mécanisme de Proof of Work (PoW) et le mécanisme de Proof of Stake (PoS).

2.3 Mécanismes de validation de blocs

2.3.1 Proof of work(PoW)

Dans ce mécanisme, un mineur doit effectuer une quantité de travail, qui est souvent un puzzle ou un défi mathématique, difficile à calculer mais facile à vérifier. La difficulté du défi est adaptée, par la Blockchain, en fonction du temps nécessaire à la validation d'un bloc.

Une PoW est exigée pour la validation de chaque bloc. Elle a l'avantage de protéger l'intégrité des transactions et des blocs, car afin qu'un attaquant puisse modifier un bloc, il doit modifier tous les blocs qui le succèdent et fournir une nouvelle PoW pour chacun de ces blocs, ainsi que la mise à jour de tous les objets par la nouvelle version de la chaîne (falsifiée). Ce qui nécessité une énorme puissance de calcul et d'énergie. La PoW représente la méthode de validation de bloc la plus adoptée par les systèmes Blockchain.

Le concept de l'algorithme le plus utilisé dans la Blockchain existait bien avant sa naissance. Dans le cas de Bitcoin, la preuve de travail suppose que tous les membres du réseau votent en utilisant leur puissance de calcul en résolvant le PoW et la construction et la validation du bloc. La preuve de travail peut être considérée comme le principal composant afin de définir un calcul informatique couteux, également appelé extraction qui doit être effectuée afin de générer un nouveau bloc.

Les mineurs servent à deux fins : vérifier la légitimité d'une transaction et éviter les doubles dépenses.

2.3.2 Proof of Stake

Afin de résoudre les lacunes de la PoW (Preuve de Travail), la PoS (Preuve d'Enjeu) a été proposée.

Dans ce mécanisme il n'y a pas de minage où on consomme beaucoup de ressources. Les mineurs sont appelés forgeurs. Un forgeur peut valider des blocs en fonction de la quantité d'argent qu'il possède. Ce qui signifie que plus il possède de monnaies, plus il augmente sa chance de validation.

Si on compare la PoS à un jeu de pari, où chaque forgeur parie sur un bloc. On peut dire qu'une fois que les blocs honnêtes (ne contiennent aucune transaction frauduleuse) sont ajoutés à la chaîne, chaque forgeur touche une récompense relative à son pari.

Et contrairement à la PoW où les mineurs malicieux sont pardonnés, dans la PoS un forgeur dont le bloc s'avère malhonnête est pénalisé et le montant du pari qu'il a mis est débité de son solde. Le point faible de la PoS est que les forgeurs qui possèdent beaucoup de monnaies sont ceux qui bénéficient le plus. Il existe plusieurs systèmes Blockchain qui utilisent la PoS, et d'autres qui replacent la PoW par la PoS.

Il existe d'autres mécanismes de validation de blocs tel que la Delegated Proof-of-Stake (DPoS), la Proof of Stake/Time (PoST), la Proof of Existence (PoE), etc.

2.3.3 Delegated Proof of Stake (DPoS)

La principale différence entre les PoS et les DPoS réside dans le fait que les PoS sont un processus démocratique direct, tandis que le DPoS est démocratiquement représentatif. Les parties prenantes élisent des délégués pour générer et valider un bloc. Avec beaucoup moins de nœuds pour valider le bloc, le bloc peut être confirmé rapidement.

2.3.4 Practical Byzantine Fault Tolerance (PBFT)

Cet algorithme de consensus a été développé pour le comportement arbitraire du nœud, qui rejoint et quitte le réseau à tout moment qui se produit généralement dans un système distribué.

Cet algorithme présente une technique de réplication de machine à états permettant de gérer les erreurs.

Théoriquement, il utilise un algorithme de réplication de la machine d'état avec un seul aller-retour de message pour exécuter des opérations en lecture seule et deux pour exécuter des opérations de lecture-écriture.

2.4 Architecture de la Blockchain

L'architecture réseau d'un réseau distribué Blockchain est Peer to Peer. Le réseau d'égal à égal, également appelé P2P, fait référence à un groupe d'ordinateurs agissant en tant que nœuds pour partager des fichiers entre eux-mêmes.

La Blockchain fonctionne donc sur un réseau distribué de serveurs, également appelé nœuds. Ces nœuds du réseau ont pour objectif de fournir un consensus sur l'état de la Blockchain à tout moment, et contiennent une copie de la Blockchain.

L'application fondamentale de la Blockchain est un grand livre de transactions, un peu comme un grand livre public sécurisé, qui stocke toutes les transactions qui ont lieu dans le réseau. Cela en fait un système décentralisé très sécurisé et transparent.

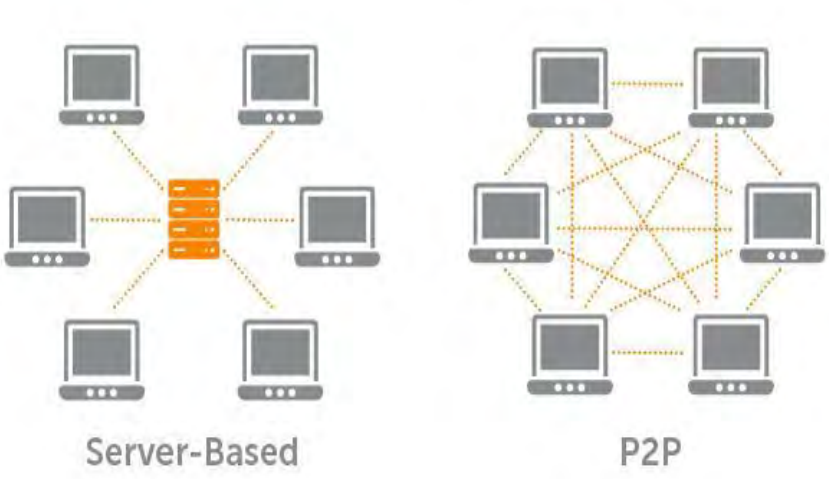
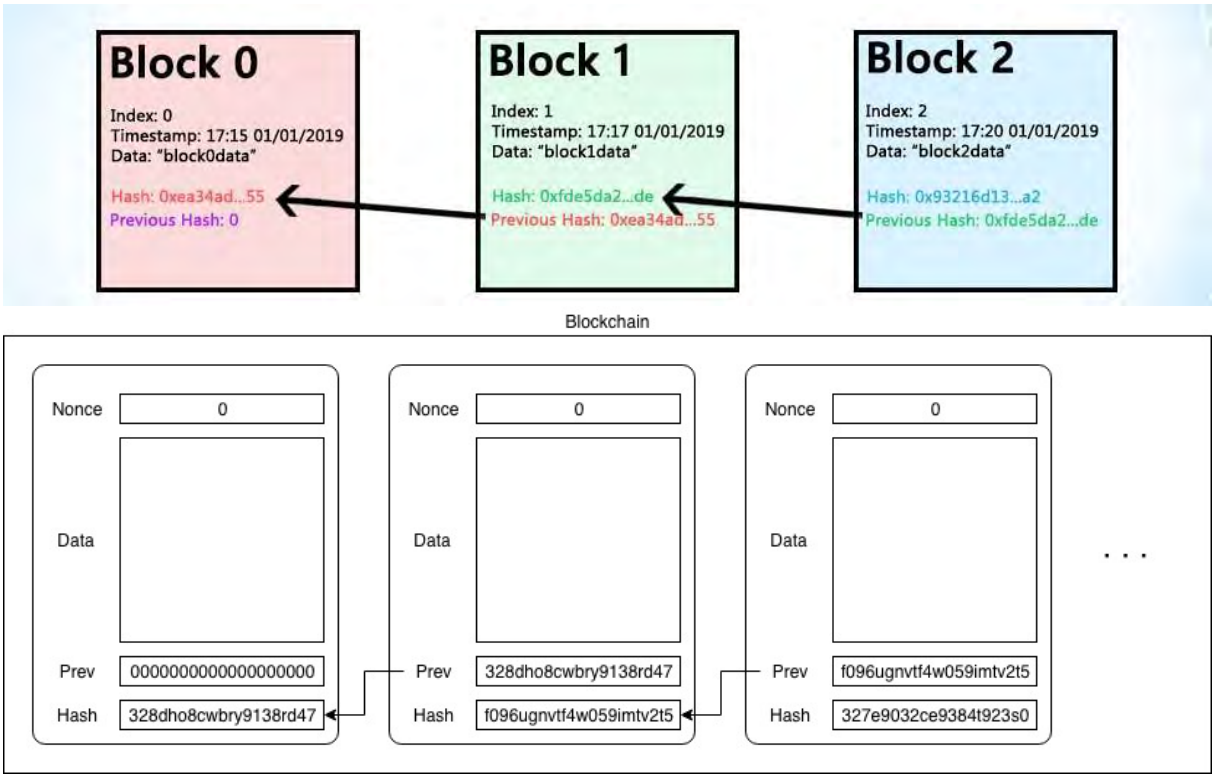


Figure 4 : Réseau basé sur les Serveurs vs Réseau P2P [I4]



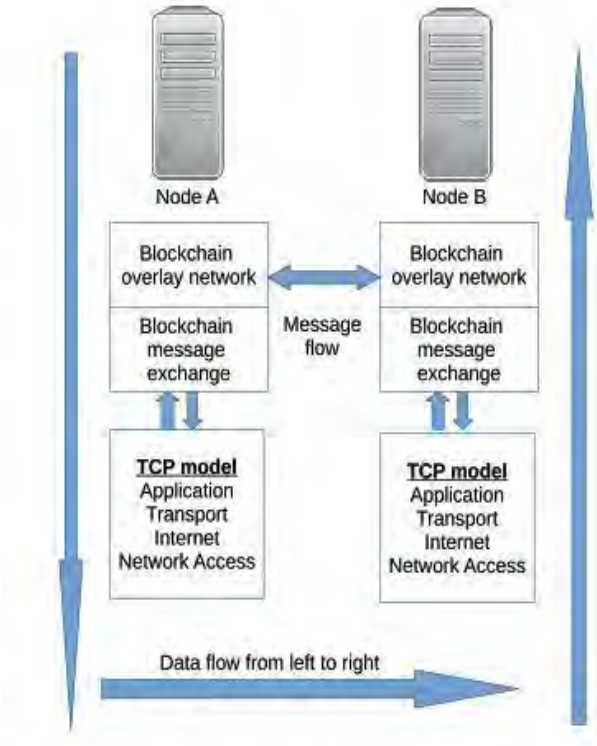


Figure 5 : Architecture de la Blockchain [I5]

2.5 Fonctionnement de la Blockchain

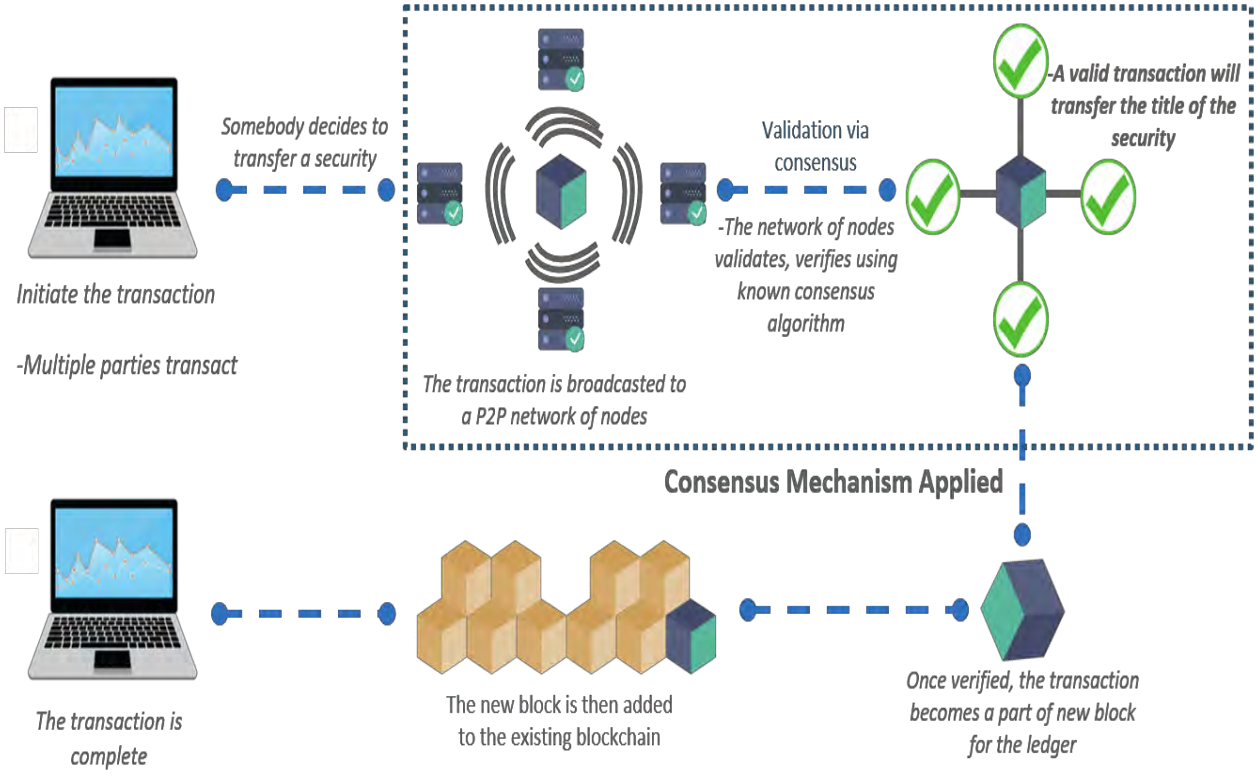


Figure 6 : Les étapes sur un réseau Blockchain [I6]

La figure 6 illustre le mécanisme de fonctionnement des transactions dans le réseau Blockchain

Les étapes de ce mécanisme sont les suivantes :

- Quelqu'un demande une transaction.
- La transaction est diffusée sur un réseau P2P public (réseau Blockchain) composé de plusieurs nœuds.
- Le réseau de nœuds valide la transaction en utilisant les algorithmes de hachage.
- Une fois vérifiée, la transaction est combinée avec d'autres transactions pour créer un nouveau bloc de données pour le grand livre.
- Le nouveau bloc est ajouté à la chaîne de blocs existants, sous une forme qui est permanente et inaltérable.
- Enfin la transaction sera effectuée avec succès.