MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR DE LA RECHERCHE
ET DE L'INNOVATION

UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

UFR SCIENCES ET TECHNOLOGIES

DÉPARTEMENT INFORMATIQUE

MÉMOIRE DE FIN D'ÉTUDES

POUR L'OBTENTION DU DIPLÔME DE MASTER

MENTION : INFORMATIQUE ; SPÉCIALITÉ : GÉNIE LOGICIEL

SUJET:

CONCEPT DE LA TECHNOLOGIE BLOCKCHAIN : LES DIFFÉRENTS PROTOCOLES ET LE CONCEPT DANS LA RÉVOLUTION IA/BIG DATA/IOT

PRÉSENTÉ PAR : MR DJIBY NDIAYE, SOUTENANCE LE 26 /11/2022.

SOUS LA DIRECTION DE DR MALICK NDOYE & MR MALAW NDIAYE

MEMBRE DU JURY

M. Youssou Faye	**Président Jury**	**Professeur assimilé (MC CAMES) UASZ**
M. Ibrahima Diop	**Rapporteur**	**Professeur assimilé (MC CAMES) UASZ**
M. Thierno Ahmad Diallo	**Examinateur**	**Maître de Conférences titulaire (MA CAMES) UASZ**
M. Malick Ndoye	**Encadrant**	**Maître Conférence titulaire (MA CAMES) UASZ**
M. Malaw Ndiaye	**Co-Encadrant**	**Assistant UASZ**

2021/2022

Remerciements

Je remercie **Dieu**, le tout puissant de m'avoir donné la santé et la volonté d'entamer et de terminer ce mémoire.

Tout d'abords ce travail ne serait pas aussi riche et n'aurait pas pu voir le jour sans l'aide et l'encadrement de **M. Elhadji Malick Ndoye** et **M. Malaw Ndiaye**. Je les remercie pour leurs encadrements exceptionnels et leurs disponibilités durant la rédaction de ce mémoire.

Mes remerciements s'adressent à Mr Youssou Faye pour avoir répondu à mes questions et s'être investi sur certaines parties du mémoire.

Je souhaite remercier les membres du jury, **M. Youssou Faye**, **M. Thierno Ahmad Diallo** ET **M. Ibrahima Diop,** Merci de m'avoir fait l'honneur d'être dans mon jury.

L'enseignement de qualité dispensé par le master « Génie Logiciel » a également su nourrir mes réflexions et a représenté une profonde satisfaction intellectuelle, Merci Donc aux enseignants-Chercheurs, Particulièrement à ma marraine **Mme Diop** (**MARIE NDIAYE**)

Je souhaite également remercier mes parents, mes frères et sœurs, ma famille, mes amis, mes camarades et toutes les personnes qui m'ont aidé dans mon cursus.

Dédicaces

Avec l'expression de ma reconnaissance, je dédie ce mémoire :

A mon très cher grand père **M. Baba Ndiaye** « King Baba », qui n'a pas cessé de me conseiller, encourager, et soutenir tout au long de mes études. Tous mes souhaits de santé et de longévité. Que Dieu te protège.

A l'homme, à qui je dois ma vie, ma réussite et tout mon respect : mon cher père **Elhadji Ndongo Ndiaye**.

A la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non à mes exigences et qui n'a épargné aucun effort pour me rendre heureux : mon adorable mère **Marianne Diop**.

A mon cousin, ami, frère, mon alter ego, qui m'a toujours soutenu et encouragé : **Mouhamadou Fallilou Ndiaye.**

A mon adorable petit frère, le juriste : **Pape Sarra Ndiaye.**

A mon papa et homonyme, le DG de l'ANER, **M. Djiby Sarra Ndiaye.**

A tous les membres de ma famille, mes amis d'enfance et ceux de l'université, mes camarades de classe la 2ème Promo MPI, je leur souhaite tous de réussir pleinement dans la vie.

Merci pour leurs amours et encouragements.

Sans oublier mes défunts camarades, M. Mamour Diouf et M. Alpha Sané, qui nous ont quitté très tôt, que firdawsi soit leurs demeures éternelles.

Résumé

L'intelligence artificielle, le Big Data et L'internet des objets sont tous des technologies novatrices, suscitant un énorme intérêt dans divers domaines scientifiques et techniques au cours des dernières années. Malgré leurs nombreux avantages et applications, elles sont confrontées à des défis de confidentialité et de sécurité. La blockchain avec sa nature décentralisée et immuable, a le potentiel d'améliorer les services et applications de ces différentes technologies. Dans ce mémoire nous allons d'abord étudier l'état de l'art de la blockchain (concept, domaines d'applications, avantages et inconvénients etc.,). Présenter de manière brève et explicite l'intelligence artificielle, le big data et l'internet des objets. Ensuite examiner les divers services de la blockchain pour les autres technologies, afin de proposer une architecture décentralisée et sécurisée, intégrant les 4 technologies à savoir IOT (pour la génération des données), Big data (pour le traitement et le stockage des données), L'intelligence artificielle (IA) (pour les modèles prédictifs) et enfin la blockchain (va se charger de sécuriser les données).

Abstract

Artificial Intelligence, Big Data and Internet of Things are all innovative technologies, attracting huge interest in various scientific and technical fields in recent years. Despite their many benefits and applications, they face privacy and security challenges. Blockchain, with its decentralized and immutable nature, has the potential to improve the services and applications of these different technologies. In this thesis we will first study the state of the art of the blockchain (concept, fields of application, advantages and disadvantages etc.,). Briefly and explicitly present artificial intelligence, big data and the Internet of Things. Then examine the various blockchain services for other technologies, in order to propose a decentralized and secure architecture, integrating the 4 technologies namely IOT (for data generation), Big data (for data processing and storage), Artificial intelligence (AI) (for predictive models) and finally the blockchain (will take care of securing the data).

Table des matières

Liste des figures :

Liste des tableaux :

INTRODUCTION GENERALE

Les années 2007-2008 sont terribles pour le monde de la finance. Aux États-Unis, le prix de l'immobilier a cessé subitement de croître, stagnant entre 8 et 15 % chaque année. Les emprunteurs ne parviennent pas à payer leurs crédits et entrent en défaut. Les institutions financières qui avaient transformées les crédits en produits financiers associés à un fort effet de levier se trouvent incapables de satisfaire leurs engagements. Les produits avaient été vendus pendant près d'une décennie et la crise est mondiale [1]. Cette crise financière et l'idée de contourner le système financier traditionnel, a motivé un inconnu utilisant le pseudonyme de « Satoshi Nakamoto » à créer la première blockchain (le Bitcoin). Le concept fondamental était de déposséder les États de leur droit à imprimer de la monnaie et ainsi spoiler les épargnants de la richesse qu'ils avaient pu amasser à la suite de leur travail. De la même manière, l'exploit technique avait pour mission de s'affranchir du système bancaire dans son état actuel [1].

La blockchain est une technologie de grande envergure, novatrice, permettant de stocker des données numériques de manière décentralisée et sécurisée. Ses données sont stockées sur les serveurs de ses utilisateurs et non à un unique endroit. Elle fonctionne sans organe central de contrôle et est basée sur un réseau pair à pair (peer-to-peer). Chaque objet du réseau (nœud) détient une copie de toutes les transactions afin d'éviter d'avoir un point unique de défaillance. Toutes les copies sont mises à jour et validées simultanément. Cette technologie peut être explorée dans de nombreux cas d'utilisation et utilisée comme un moyen sécurisé de gestion et de protection de toute sorte de données (monétaires ou pas) [2]. La nature décentralisée de la blockchain crée le nouveau concept d'une économie symbolique dans laquelle les revenus de la communauté peuvent être alloués aux producteurs de contenu et aux utilisateurs de services réels qui créent de la valeur. De surcroit presque toutes les blockchains ont leurs propres monnaies d'échanges, communément appelées cryptomonnaies [1]. Ces dernières sont des monnaies virtuelles, fabriquées par codage et leurs transactions sont stockées dans leurs blockchains respectives. Elles utilisent la cryptographie pour crypter et cacher les codes afin de protéger l'argent. La cryptomonnaie est la première et l'une des applications les plus importantes de la technologie blockchain.

De nos jours les applications de big data, d'internet des objets ou même de l'intelligence artificielle, ont gagné en popularité, mais sont confrontées à d'importants problèmes et défis de sécurité. Les sources suspectes de données et les liens de communications permettent à la collecte de données d'être exposée à diverses attaques et menaces malveillantes.

En effet nous pensons à combiner ces technologies avec la blockchain, afin de proposer une architecture décentralisée au service de la santé.

Ce mémoire sera structuré en quatre (4) parties. Nous présenterons en première partie le concept de la technologie blockchain. La deuxième partie proposera une étude détaillée des algorithmes de consensus qu'utilisent les différentes blockchains. La troisième partie nous permettra d'avoir une idée beaucoup plus claire sur les différentes relations entre la blockchain, le big data, l'intelligence artificielle et l'internet des objets, avant de terminer par une proposition d'architecture décentralisée reliant ces 4 technologies.

Chapitre 1 : Le concept de la blockchain

1.2 . Introduction

La blockchain ou chaine de blocs en français, est une nouvelle technologie qui permet de stocker et transmettre des informations de manière transparente, sécurisée, et sans organe central de contrôle[3]. Dans ce chapitre nous allons essayer de parler du concept de cette technologie en partant bien sûr de l'historique, ensuite son mode de fonction, avant de terminer sur ses avantages et limites.

1.3 . Historique

- En **1980**, y'a eu des rumeurs sur des protocoles pour les monnaies numériques décentralisées, reposant sur une primitive cryptographique.
- En **1990**, David Chaum met en place une monnaie électronique intitulée **Digicash**, cette dernière dépendait à un tiers centralisé, malheureusement en faillite en 1998.
- En **1996**, la naissance d'une monnaie électronique **E-Gold** qui a réussi à atteindre les 5 millions d'utilisateurs en 13ans, suspendu pour des raisons juridiques.
- Nous sommes en **2008**, un certain Satoshi Nakamoto, publie en ligne un article de 10 pages qui décrit le fonctionnement d'une nouvelle monnaie qu'il vient d'inventer : le **bitcoin**. Dans le réseau bitcoin les transactions sont enregistrées en blocs et chaque bloc est lié à un autre, ressemblant à une chaine, d'où le terme **Blockchain**.
  Cette dernière est un document permettant d'enregistrer toutes les transactions faites en son sein. Il faut noter aussi qu'il n'y a pas de pièces de monnaies palpables.

  L'auteur du premier article sur la blockchain reste anonyme, jusqu'à ce jour personne ne connait Satoshi Nakamoto. Quelques mois après le premier article, un programme open source mettant en œuvre le nouveau protocole a été publié. C'est un bloc genèse de 50 pièces, tout le monde pouvait l'installer et faire partir du réseau Bitcoin. Le Bitcoin a gagné en popularité depuis lors [4], [5].

1.4 . Concept et mécanisme de la blockchain

La blockchain est un **registre numérique distribué, immuable** qui est sécurisé à l'aide d'une **cryptographie** avancée, répliqué entre **les nœuds homologues du réseau** pair à pair, utilisant **un mécanisme de consensus** [4]. Cette définition nous permet d'identifier les concepts de base (mis en gras) de la technologie blockchain et de mieux comprendre ladite technologie. Ci-dessous nous allons essayer d'expliquer ces concepts afin d'avoir un aperçu sur le sens de la blockchain.

- **Un registre numérique distribué :** C'est un système numérique qui enregistre des transactions d'actifs et leurs détails dans plusieurs emplacements à la fois. Dans un registre distribué, chacun des nœuds traite et vérifie chaque élément des transactions. Un consensus sur la véracité de ces éléments est ensuite trouvé entre les différents nœuds [6].
- **Immuable :** Elle est immuable car son journal de transaction ne peut être modifié.
- **La cryptographie :** C'est une technique utilisée pour sécuriser une communication mais aussi permettre la protection des informations confidentielles. La blockchain utilise les concepts de crypto-systèmes à clé publique ou cryptographie asymétrique pour vérifier l'autorité de l'utilisateur à exécuter des transactions et des fonctions de hachages cryptographiques pour parvenir à un consensus entre les nœuds du réseau sur les données de la blockchain [4] :

  - **La cryptographie asymétrique**

    La blockchain fait recours à la cryptographie asymétrique pour la sécurité de ses échanges en ligne. Elle peut servir à chiffrer des informations mais aussi signer des messages.

    La cryptographie asymétrique comment ça marche ?

    Par exemple, imaginons que Bob souhaite envoyer des messages secrets à Alice.

    Alice génère d'abord une paire de clés. Une clé privée et une clé publique. Ces clés ont des propriétés propres aux algorithmes utilisés.

    En effet, un message chiffré avec une clé ne peut être déchiffré qu'avec l'autre. Ce sont des fonctions à sens unique. Alice va par la suite, partager sa clé publique en vert avec Bob ; permettant ce dernier de chiffrer le message et de l'envoyer [7].

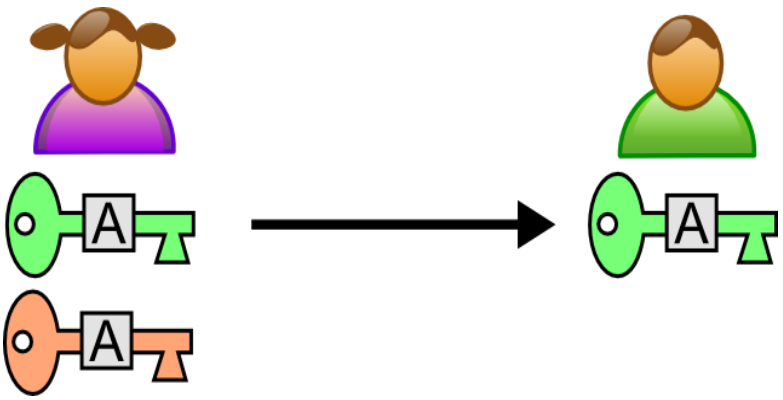


Figure 1:Génération et transmission des clés [7].

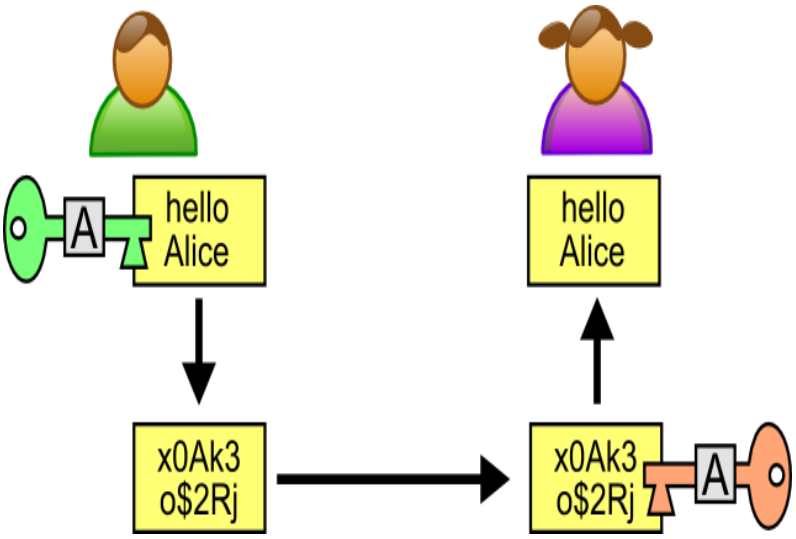


Figure 2:Chiffrement et déchiffrement des messages [7].

Avec l'usage de la clé publique d'Alice, Bob est sûr de deux choses :

- ✓ On ne peut pas lire son message, car il est crypté ;
- ✓ Seule Alice peut déchiffrer le message, puisqu'elle seule possède la clé privée.

❖ **Les fonctions de hachages**

Il s'agit d'une fonction mathématique qui convertit une chaine de caractère de n'importe quelle longueur en une autre chaine de longueur fixe. C'est un procédé à sens unique permettant d'obtenir une suite d'octets caractérisant un ensemble de données.

Un algorithme requis pour les fonctions de hachages de la blockchain, a 3 propriétés principales :

- La même entrée doit toujours donner le même hachage de sortie ;
- Impossible de partir du hash pour trouver l'original [8] ;
- Un petit changement dans l'entrée entraine un hachage de sortie complétement diffèrent.

On note plusieurs fonctions de hachages : Keccak, Sha-256, Sha-512, Ethash, md5, Sha-1…etc. Par exemple Bitcoin utilise la fonction de hachage SHA-256 (256bits) tandis que l'Ethereum utilise Ethash.

Exemple de hash avec SHA-256[8] **:**

b*itcoin.fr, site d'information et de nouvelles autour de Bitcoin.*

Hash SHA-256=

9578c1ea7cd3b3129efea270c64e0d1637f6184f325b58e1d02e95829d03ba6c

B*itcoin.fr, site d'information et de nouvelles autour de Bitcoin.*

Hash SHA-256=

ae7366010a2a5265344815b3ff98abd03283a1bf577f6f685fc31e74ff041d88

A quoi sert une fonction de hachage dans la blockchain ?

Avec les fonctions de hachage, il est pratiquement impossible de pirater le système de la blockchain. Elles garantissent la sécurité des données en comparant les signatures. Puisque chaque donnée à sa propre signature, on peut se dire que si les signatures sont identiques alors les données sont identiques. On a créé cette image pour essayer de montrer l'importance des hash dans les chaines de bloc.

Figure 3:Deux chaines de blocs.

Comme l'illustre la figure 3 ci-dessus, elle représente deux blockchains l'une valide et l'autre modifiée et invalide. La modification du contenu du deuxième bloc (le remplacement de « peuls » par « sérères »), change complétement le hachage de ce bloc qui est aussi l'entête du troisième bloc. Puisque les données sont liées, un petit changement invalide les blocs d'où la sécurité de la blockchain grâce notamment aux fonctions de hachages**.**

- **Le réseau blockchain**

  C'est un réseau pair à pair composé de nœuds. Ces derniers se sont les détenteurs du registre. Chaque ordinateur qui possède par exemple une copie de la blockchain est appelé « nœud » du réseau. Ces nœuds sont aussi appelés des pairs dans le réseau. Chaque pair est égal est une autre. Ainsi il n'y a donc pas de dispositif administrateur central au centre du réseau, ni de partie privilégiée. Parmi les nœuds, certains peuvent agir comme mineurs afin de participer à la vérification et à la validation de toutes

transactions effectuées au sein du réseau. Tous les mineurs sont des nœuds, mais tous les nœuds ne sont pas forcément des mineurs.

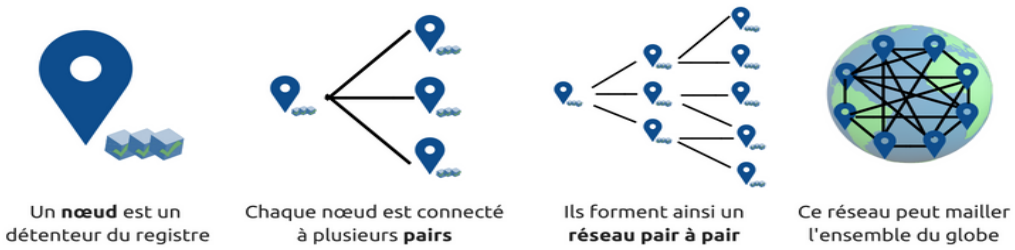


Figure 4:Le réseau pair à pair de la blockchain[5].

- **Les mécanismes de consensus**

Ce sont des mécanismes par lesquels les nœuds du réseau parviennent à trouver un accord sur la validité et l'authenticité des blocs de transactions ou des données. On note deux types d'algorithmes de consensus : les consensus par vote et les consensus par preuve. Ces derniers exigent que les nœuds rejoignant le réseau de vérification montrent qu'ils sont plus qualifiés que les autres pour effectuer le travail d'ajout tandis que les consensus par vote obligent que les nœuds échangent leurs résultats de vérification d'un nouveau bloc ou d'une nouvelle transaction avant de prendre une décision finale.

Exemples d'algorithmes de consensus y'a le proof of work (preuve de travail), le proof of stake (preuve d'enjeu), PBFT (tolérance aux pannes byzantines pratiques), Raft, etc. Les deux algorithmes les plus populaires sont le PoW et le PoS. Le premier cité est utilisé par la première blockchain à savoir le Bitcoin et le deuxième sera utilisé par Ethereum dans sa prochaine mise à jour.

1.4.1 . Structure d'un bloc

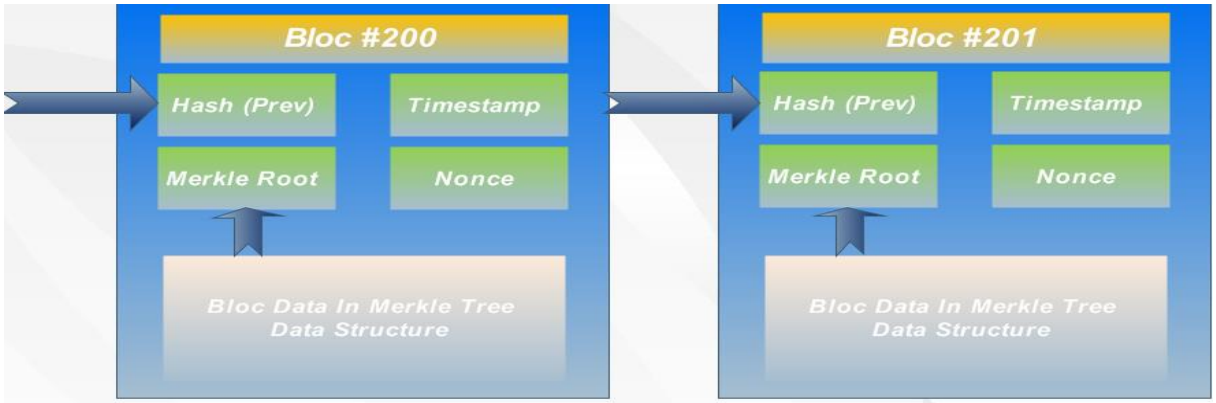


Figure 5: Structure d'un bloc

Le premier bloc a été créé par Satoshi Nakamoto le 09/01/2009 et depuis lors on a un bloc toutes les 10 minutes.

Comme le montre la figure 6 ci-dessus, un bloc contient un entête et des données de transactions.

L'entête contient 4 informations :

- Le hachage du bloc précédent :

  Le hachage permet de transformer une chaine de caractères de longueur indifférente à une autre de longueur fixe. Dans la Blockchain, les données de chaque bloc sont hachées et intégrées dans le bloc suivant, ce qui permet de les lier les uns des autres. Il garantit aussi la sécurité et l'intégrité de la chaine de blocs. Les hachages rendent la Blockchain presque infaillible.

- L'horodatage :

  L'horodatage est un petit élément de données stocké dans chaque bloc en tant que série unique et dont la fonction principale est de déterminer le moment exact où le bloc a été extrait et validé par le réseau blockchain. Il permet de construire un lien cryptographique entre l'empreinte numérique d'une donnée et un bloc de la blockchain qui est vérifiable en toute circonstance a posteriori[12].

- Le nonce :

  C'est un nombre arbitraire destiné à être utilisé une seule fois. Il s'agit souvent d'un nombre aléatoire ou pseudo-aléatoire émis dans un protocole d'authentification pour garantir que les anciennes communications ne peuvent pas être réutilisées dans des attaques par rejeu[13].

- La racine de l'arborescence de Merkle

  C'est un identifiant unique pour toutes les transactions combinées à l'intérieur du bloc. La modification des données de transaction dans un bloc, modifie le hachage de l'arborescence de Merkle stocké dans l'entête du bloc ; ainsi les données seront rejetées par les autres nœuds du réseau[14].

1.4.2 . Le fonctionnement d'une Blockchain

Pour mieux comprendre le fonctionnement de la blockchain, on va se référer de la figure ci-dessous.

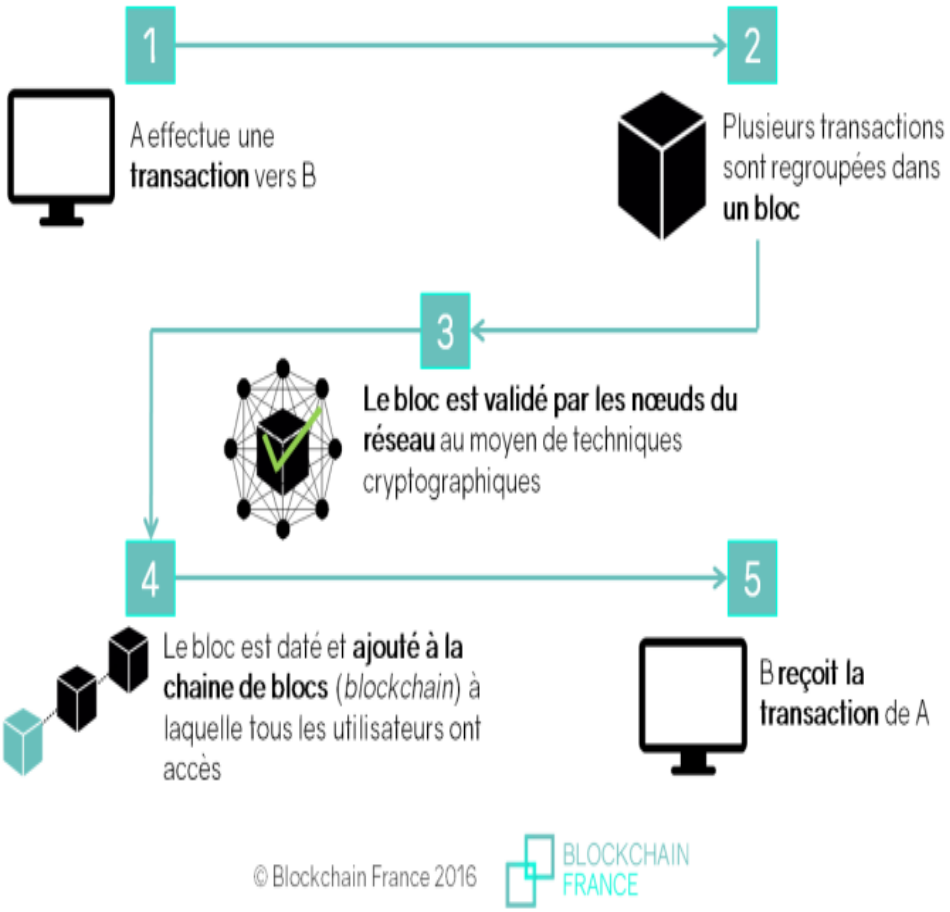


Figure 6:Fonctionnement d'une blockchain [15].

L'analyse de la figure 7 ci-dessus nous permet de savoir que l'ajout d'un bloc est déclenché par une demande de transaction par exemple A voulant envoyer de l'argent à B. Après cette demande, les données de la transaction seront regroupées dans un bloc et transmises dans le réseau. Les nœuds du réseau vont à leur tour procéder à la vérification et à la validation du bloc. Si ce dernier est valide, il sera daté et ajouté à la chaine de bloc. Le bloc sera consultable par tous les membres du réseau mais ne peut être modifié, et enfin B reçoit la transaction de A. Sinon (bloc invalide) le bloc sera rejeté, ce qui mettra fin à la transaction.

1.5 . L'architecture en couche de la blockchain

Comme le montre la figure 8 ci-dessous que nous avons créée, l'architecture en couche de la technologie blockchain est composée principalement de six (6) couches : une couche application, une couche modélisation, une couche de contrat, une couche système, une couche de données et une couche réseau. Ces dernières ont chacune un rôle spécifique dans l'évolution et le bon fonctionnement de ladite technologie.

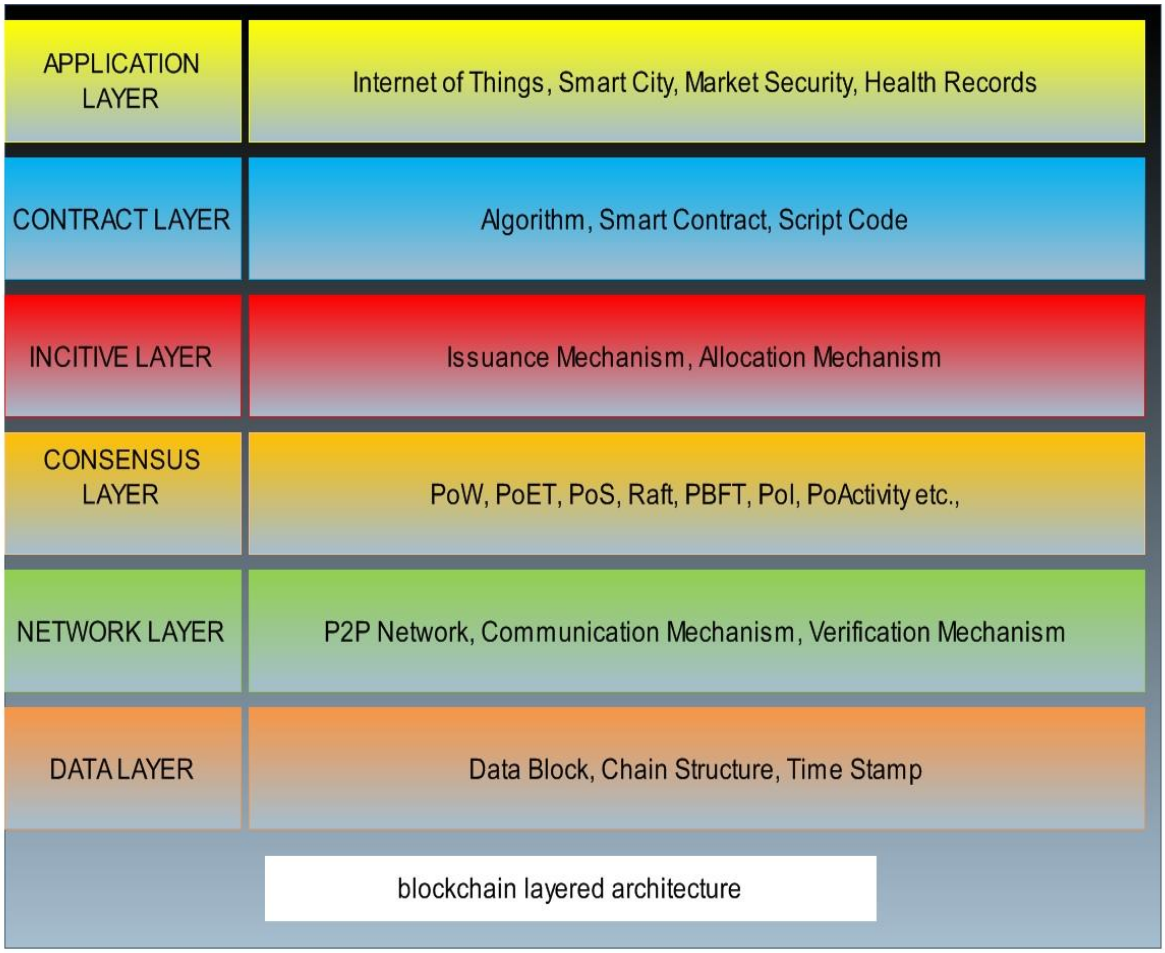


Figure 7:L'architecture en couche de la Blockchain.

Ci-dessous nous allons essayer d'expliquer brièvement mais aussi de manière précise, la fonctionnalité de chaque couche [16], [17], [18].

1.5.1 . La couche application

C'est la couche qui se concentre sur le développement de solutions blockchains à utiliser dans différentes applications et industries.

1.5.2 . La couche modélisation

Cette couche permet de faciliter les contrats intelligents, elle établit les flux de travail et définit comment l'utilisateur interagira avec le système.

1.5.3 . La couche de contrat

Cette couche concerne le contrat lui-même. Puisque y'a des répercussions financières sur un contrat mal défini ou exécuté, donc on doit s'assurer que le contrat soit correctement émis.

1.5.4 . La couche système

Elle est composée essentiellement d'éléments permettant de maintenir la Blockchain. C'est la couche qui fait intervenir les protocoles de consensus et sous-systèmes associés.

1.5.5 . La couche de données

C'est la couche de gestion des informations stockées sur la Blockchain.

1.5.6 . La couche réseau

La Blockchain fonctionne sur un réseau pair à pair. Les pairs partagent les informations sur l'état du réseau. La confidentialité et la sécurité sont incluses dans cette couche.

1.6 . Les types de Blockchain

Actuellement, on note l'existence de trois (3) types de blockchains :
Les blockchains publiques ou non autorisées, les blockchains privées ou autorisées et les blockchains de consortium.

1.6.1 . Les blockchains publiques ou non autorisé

La blockchain publique ne requiert aucune permission spécifique à l'entrée, ni au moment de réaliser une transaction. Les différents acteurs de la chaîne sont tous au même niveau, et tous les nœuds du réseau d'échange sont contrôlés par le réseau pair à pair. L'autre caractéristique essentielle de cette blockchain réside dans son caractère « open-source » : en effet, n'importe quelle personne disposant d'un bagage technique suffisant est en capacité de copier et de modifier le code du protocole selon son bon vouloir, ce qui donne lieu la plupart du temps à des protocoles alternatifs.
Cette blockchain est entièrement décentralisée et sécurisée mais aussi les transactions sont totalement irréversibles.
On retrouve ce mode de fonctionnement avec les monnaies virtuelles telles que **bitcoin** et **ether** [19].

Figure 8:Architecture d'une blockchain non autorisée [20].

1.6.2 . Les blockchains privées ou autorisées

Dans une blockchain privée, personne ne peut y participer sans être autorisé mais tout le monde peut la consulter. Vous trouverez ci-dessous quelques caractéristiques des blockchains privées :

- Restreignent l'accès en écriture pour un ensemble limité des participants.
- Un mécanisme de consensus est utilisé pour valider l'écriture des données parmi ses participants privilégiés.
- Utile pour les applications commerciales et sociales [21].

Figure 9:Architecture d'une blockchain autorisée [20].

Parmi les blockchains privées on peut citer Hyperledger Fabric et Corda.

1.6.3 . Les blockchains de consortium

La blockchain "de consortium" regroupe plusieurs acteurs qui possèdent des droits et les décisions sont prises par la majorité des acteurs. Par exemple, une dizaine d'institutions financières pourraient se mettre d'accord et organiser une blockchain dans laquelle un bloc devrait être approuvé par au moins 8 d'entre elles pour être valide. C'est donc très différent de la blockchain privée et de la

blockchain publique. Non seulement les participants au processus d'approbation sont limités et sélectionnés, mais ce n'est plus la règle de la majorité qui s'impose. Cette blockchain hybride est un véritable avantage pour les acteurs du secteur financier car ils opèrent dans des environnements réglementés et sont notamment obligés de connaître l'identité des participants (ce qui n'est pas le cas dans la blockchain publique). Le consortium de blockchain le plus connu est R3. Il compte environ 100 institutions financières dont BNP Paribas [22].

Figure 10:Architecture d'une blockchain de consortium [20].

1.7 . Les applications de la blockchain

La première et la plus excitante application de la blockchain est **la monnaie électronique** (les cryptomonnaies)**.** Mais les gens se sont vite rendu compte que la technologie blockchain pouvait être personnalisée et utilisée dans d'autres applications telles que **les smarts contracts** (contrat intelligent), **la DeFi** (la finance décentralisée), **les NFT**, **les registres des titres de propriétés** ou encore **Les votes numériques,** etc**.**

1.7.1 . Les cryptomonnaies

La cryptomonnaie est une monnaie émise de pair à pair, sans l'intervention d'un tiers de confiance, utilisable au moyen d'un réseau informatique décentralisé. Bien que de nombreux cryptomonnaies fonctionnent sur une infrastructure de blockchain similaire, elles représentent des différences majeures. De façon générale, les cryptomonnaies peuvent être regroupées en deux catégories distinctes : Les coins et les tokens (jetons) [23], [24].

- **Coins et altcoins**

- Un coin désigne toute cryptomonnaie qui utilise sa propre blockchain. Par exemple bitcoin est considéré comme un « coin » parce qu'il fonctionne sur sa propre infrastructure. De la même manière, l'ether fonctionne sur la blockchain Ethereum.

- Le terme « altcoin » désigne simplement tous les coins autre bitcoin. Beaucoup d'altcoin fonctionnent de la même manière que le bitcoin. Toutefois, certains comme dogecoin sont assez différents. Le Doge offre un nombre illimité de coins, alors que pour le Bitcoin, le nombre de bitcoin pouvant être crées a été plafonné à 21 millions [25].
    - **Les tokens**

Comme les coins, les tokens sont aussi des actifs numériques qui peuvent être achetés et vendus. Cependant, les tokens sont des actifs non-natifs, ce qui signifie qu'ils utilisent une infrastructure blockchain qui n'est pas la leur. Cela inclut tether, qui est hébergé sur la blockchain Ethereum et d'autres notamment Terra USD, Chainlink, Uniswap, et Polygon [26].

1.7.1.1 . Exemples de cryptomonnaies

De nos jours, on note l'existence de plus de huit milles (+8000) cryptomonnaies. Ces dernières n'ont pas la même valeur, ni la même ampleur. En effet, y'en a qui ont une forte capitalisation boursière comme le bitcoin, l'ether, l'ada, etc. Ci-dessous, nous allons essayer de dresser un tableau classifiant les dix (10) premières cryptomonnaies en termes de capitalisation boursière [30], [31].

Blockchain	**Symbole boursier**	**Capitalisation boursière en dollar**
Bitcoin	BTC	1067,74 Mds $
Ethereum	ETH	409,31 Mds $
Binance Coin	BNB	98,27 Mds $
Dogecoin	DOGE	78,35 Mds $
Ripple	XRP	75,96 Mds $
Tether	USDT	53,56 Mds $
Cardano	ADA	52,77 Mds $
Polkadot	DOT	37,98 Mds $
Bitcoin Cash	BCH	26,24 Mds $
Litecoin	LTC	23,05 Mds $

Tableau 1:Les cryptomonnaies qui ont les plus fortes capitalisations boursières.

Comme vous pouvez le constater, en analysant le tableau ci-dessus, y'a une énorme différence en termes de capitalisation boursière entre les deux premières cryptomonnaies (bitcoin, ethereum) et les autres. Le bitcoin est la crypto mère, avec l'ethereum, sont les deux projets les plus réussis dans le monde de la blockchain et des cryptomonnaies. Nous allons essayer par la suite d'avoir un petit aperçu sur ces deux blockchains.

- Le bitcoin

Figure 11:Le bitcoin [32].

Le bitcoin c'est une preuve cryptographique, mécanisme permettant à deux parties disposées d'exécuter une transaction en ligne, protégée par une signature numérique.

Il est la plus importante cryptomonnaie décentralisée avec une capitalisation de plus de 1000 milliards de dollars en mars 2022, d'ailleurs ce qui n'est pas une surprise car étant la première blockchain réussie. Le bitcoin, pour le maintien et la bonne marche de son réseau, utilise l'algorithme de consensus « proof of work). Il existe plusieurs forks de bitcoin. Ce terme désigne la création d'une nouvelle « branche » du bitcoin, indépendante mais se basant sur une structure similaire. Parmi les forks bitcoin on peut citer le Bitcoin Cash, Namecoin, Litecoin, etc.

- **Les transactions sur Bitcoin :**

Dans Bitcoin, les utilisateurs sont identifiés par des adresses Bitcoin, qui sont des hachages générés à partir de leurs clés publiques correspondantes.

Un utilisateur peut posséder plusieurs adresses pour renforcer son anonymat.

Le modèle de transaction utilisé par Bitcoin est un modèle centré sur les transactions, où une transaction peut avoir plusieurs entrées et plusieurs sorties, étant associée à plusieurs adresses. Les entrées sont constituées d'un ensemble de sorties de transaction non dépensées dont la somme des montants n'est pas inférieure au montant qui doit être payé, et le receveur peut désigner une nouvelle adresse pour recevoir la monnaie. De plus, il n'y a aucune notion de solde de compte dans Bitcoin. Le solde d'un utilisateur Bitcoin peut être calculé par la somme de la valeur du montant des sorties de transaction non dépensées disponibles dans son portefeuille [33], [34].

- Ethereum

Figure 12:L'ethereum [35].

Initié par **Vitalik Buterin,** un jeune russo-canadien qui voulait généraliser l'aspect programmable de Bitcoin,

Ethereum est une plateforme basée sur la technologie blockchain qui permet aux développeurs de réaliser et déployer des applications décentralisées ou D'Apps (pour *decentralized applications*). Alors que le rôle principal de Bitcoin est de transférer de la monnaie virtuelle, celui d'Ethereum est de faire fonctionner le programme de n'importe quelle application décentralisée.

L'unité de compte, de la monnaie Ethereum est l'éther (ou *ether*), dont le sigle est ETH.

L'éther possède deux fonctions principales :

- Il rémunère les validateurs (mineurs) qui garantissent la validité de la chaîne de blocs ;
- Il sert à payer les frais pour utiliser les D'Apps.

La blockchain Ethereum est actuellement sécurisée par le proof of work (les mineurs utilisent de la puissance de calcul pour sécuriser le réseau) mais cette sécurisation devrait évoluer vers du proof of stake avec le passage à Ethereum2.0.De nombreux projets se construisent sur ce réseau décentralisé, dont notamment les projets liés à la finance décentralisée (DeFi) qui permettent à n'importe qui de prêter ou d'emprunter des crypto-monnaies. Le rôle principal de cette plateforme est d'exécuter ce que l'on appelle des smart contracts, aussi connus sous le nom de contrats intelligents ou encore de contrats autonomes. Comme on l'a dit, Ethereum a pour but d'être un ordinateur mondial décentralisé. Pour cela, il utilise une machine virtuelle (l'*Ethereum Virtual Machine* ou EVM) qui fonctionne simultanément sur chacun des nœuds du réseau. Cette machine virtuelle modifie l'état global système (constitué des comptes Ethereum**,** de leurs soldes, des données en stockage et du code) selon les actions

des utilisateurs et l'exécution des smart contracts. Les modifications sont répliquées sur chacun des ordinateurs du réseau en consensus, d'où le fait qu'on parle de machine « virtuelle » : celle-ci n'existe pas vraiment mais est une abstraction pratique pour représenter ce qu'est Ethereum [36], [37].

- **Les transactions sur Ethereum :**

Le modèle de transaction d'Ethereum est un modèle centré sur le compte, qui contient deux types de comptes, à savoir les comptes détenus en externe (EOA) et les comptes contractuels. Un compte détenu en externe est similaire à un compte bancaire, qui peut déposer/retirer de l'argent et enregistrer des informations d'état dynamiques comme le solde du compte. En particulier, un compte détenu en externe peut créer des comptes de contrat et invoquer des contrats intelligents. Chaque compte de contrat est associé à un morceau de bytecode exécutable et conserve des informations d'état comme la valeur de hachage du bytecode ainsi que le solde de son compte. Une transaction dans Ethereum est un paquet de données signé d'un compte à un autre et il ne contient qu'une seule entrée et une seule sortie, ce qui est différent du scénario de Bitcoin. Il existe trois principaux types de fonctions que les transactions dans Ethereum peuvent remplir, à savoir le transfert d'argent, la création de contrat et l'invocation de contrat. Selon le type d'émetteur de transaction, les transactions peuvent être divisées en transactions externes et transactions internes. Une transaction n'est externe que si elle est initiée par un compte détenu en externe, tandis qu'une transaction interne est déclenchée par l'invocation d'un contrat et le contrat est son émetteur de transaction. Il convient de noter qu'une transaction externe (c'est-à-dire un appel de fonction de contrat) peut entraîner de nombreuses transactions internes [38].

- **Comment créer un nœud sur Ethereum :**

Comme on l'a dit plus haut, un nœud est juste un détenteur du registre. Il existe trois types de nœuds :

- Un nœud complet : qui enregistre la totalité des transactions de la blockchain ;
- Un nœud léger : qui enregistre une partie des transactions de la blockchain ;
- Un nœud mineur qui est chargé de valider les différentes transactions du système.

Pour prendre part au réseau Ethereum et bénéficier de nombreuses fonctionnalités, il faut tout simplement installer Go Ethereum ou Geth sur sa machine. Cette dernière est l'une des trois implémentations majeures du protocole Ethereum. A l'aide de Geth, on peut miner de l'ether

(qui nécessite des moyens), et explorer l'historique de la blockchain. Devenir un nœud sur Ethereum nécessite tout simplement de la connexion et un disque dur [39], [40].

Ci-dessous nous allons essayer de créer un nœud ethereum léger sur Ubuntu :

Pour installer Geth il faut avoir un ordinateur qui a minimum les caractéristiques suivantes :

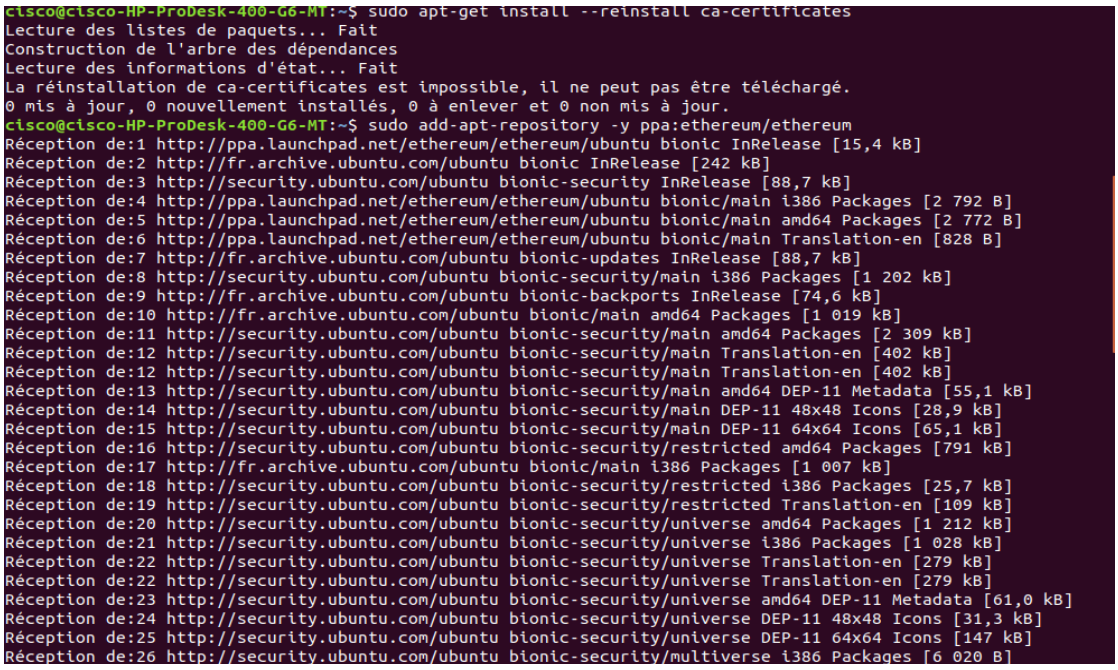
- CPU avec 2+ cores ;
- 4 GB RAM minimum ;
- 8Mbit/s de bande passante ;
- Un disque dur SSD ou 250GB minimum HDD.

Avant de commencer l'installation, assurez-vous d'avoir une connexion internet stable.

Les différentes étapes de l'installation :

La commande : ***sudo apt-get install –reinstall ca-certficates***, n'est pas obligatoire ça permet juste d'installer et de mettre à jour certains paquets, on l'exécute au cas où la deuxième commande ne marche pas.

La commande : ***sudo add-apt-repository -y ppa : ethereum/ethereum,*** permet d'ajouter le référentiel Ethereum dans notre machine Ubuntu.



La commande : ***sudo apt update***, permet de mettre à jour les paquets apts.

La commande : ***sudo apt - -upgradable***, permet d'afficher la liste de tous les paquets apts mis à jour, 721 dans notre cas.

```
cisco@cisco-HP-ProDesk-400-G6-MT:~$ sudo apt update
Atteint:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Atteint:2 http://ppa.launchpad.net/ethereum/ethereum/ubuntu bionic InRelease
Atteint:3 http://fr.archive.ubuntu.com/ubuntu bionic InRelease
Atteint:4 http://fr.archive.ubuntu.com/ubuntu bionic-updates InRelease
Atteint:5 http://fr.archive.ubuntu.com/ubuntu bionic-backports InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
721 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
cisco@cisco-HP-ProDesk-400-G6-MT:~$
```

La commande : ***sudo apt install geth***, permet d'installer geth.

```
cisco@cisco-HP-ProDesk-400-G6-MT:~$ sudo apt install geth
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  geth
0 mis à jour, 1 nouvellement installés, 0 à enlever et 721 non mis à jour.
Il est nécessaire de prendre 8 503 ko dans les archives.
Après cette opération, 31,4 Mo d'espace disque supplémentaires seront utilisés.
Réception de:1 http://ppa.launchpad.net/ethereum/ethereum/ubuntu bionic/main amd64 geth amd64 1.10.19+build27
919+bionic [8 503 kB]
8 503 ko réceptionnés en 25s (344 ko/s)
Sélection du paquet geth précédemment désélectionné.
(Lecture de la base de données... 128015 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../geth_1.10.19+build27919+bionic_amd64.deb ...
Dépaquetage de geth (1.10.19+build27919+bionic) ...
Paramétrage de geth (1.10.19+build27919+bionic) ...
cisco@cisco-HP-ProDesk-400-G6-MT:~$
```

La commande : ***useradd --no-create-home --shell /bin/false djiby***, permet de créer un nouvel utilisateur sur la machine pour exécuter geth.

La commande : ***cat /etc/passwd | grep djiby***, permet de vérifier si l'utilisateur a été bien crée.

La commande : ***pwd***, permet d'imprimer le répertoire courant.

La commande : ***mkdir -p chain/data***, permet de créer le répertoire où les données de la chaine seront réellement stockées.

La commande : ***cd chain/data***, permet de se placer dans le nouvel répertoire.

```
cisco@cisco-HP-ProDesk-400-G6-MT:~$ sudo useradd --no-create-home --shell /bin/false djiby
cisco@cisco-HP-ProDesk-400-G6-MT:~$ cat /etc/passwd | grep djiby
djiby:x:1001:1001::/home/djiby:/bin/false
cisco@cisco-HP-ProDesk-400-G6-MT:~$ pwd
/home/cisco
cisco@cisco-HP-ProDesk-400-G6-MT:~$ mkdir -p chain/data
cisco@cisco-HP-ProDesk-400-G6-MT:~$ cd chain/data
cisco@cisco-HP-ProDesk-400-G6-MT:~/chain/data$ pwd/home/cisco/chain/data
bash: pwd/home/cisco/chain/data: Aucun fichier ou dossier de ce type
cisco@cisco-HP-ProDesk-400-G6-MT:~/chain/data$ pwd /home/cisco/chain/data
/home/cisco/chain/data
```

La commande : ***sudo -R djiby:djiby /home/cisco/chain/data***, permet d'accorder à l'utilisateur que nous avons créé, l'autorisation d'écrire dans ce dossier.

La commande : ***ls -l /home/cisco/chain***, permet de vérifier, si les autorisations ont été bien modifiées.

```
cisco@cisco-HP-ProDesk-400-G6-MT:~/chain/data$ sudo chown -R djiby:djiby /home/cisco/chain/data/
[sudo] Mot de passe de cisco :
cisco@cisco-HP-ProDesk-400-G6-MT:~/chain/data$ ls -l /home/cisco/chain/
total 4
drwxr-xr-x 2 djiby djiby 4096 juin  27 19:41 data
```

La commande : ***sudo gedit /etc/systemd/system/geth.service***, permet d'ouvrir l'éditeur de texte d'Ubuntu « gedit » afin de créer un service geth dont le nom sera geth.service.

```
cisco@cisco-HP-ProDesk-400-G6-MT:/media/cisco/blob$ sudo gedit /etc/systemd/system/geth.service

** (gedit:5150): WARNING **: 17:55:36.698: Set document metadata failed: La définition de l'attribu
t metadata::gedit-spell-language n'est pas prise en charge

** (gedit:5150): WARNING **: 17:55:36.698: Set document metadata failed: La définition de l'attribu
t metadata::gedit-encoding n'est pas prise en charge

** (gedit:5150): WARNING **: 17:57:02.873: Set document metadata failed: La définition de l'attribu
t metadata::gedit-position n'est pas prise en charge
cisco@cisco-HP-ProDesk-400-G6-MT:/media/cisco/blob$
```

Le fichier ci-dessous permet de configurer le service geth.service. Dans ce fichier c'est la ligne commençant par Execstart qu'on doit impérativement modifier.

-- **datadir /media/cisco/blob/chain/data**, est le chemin du répertoire qu'on avait créé pour le stockage des données.

-- **port 41556**, ce port est ce que le client écoute pour communiquer avec d'autres nœuds ethereum. C'est le port qui est lié à l'adresse IP publique de notre fournisseur de service internet.

-- **syncmode « light »**, permet de spécifier le type de nœud qu'on veut créer (complet ou léger). Dans notre cas on a choisi le mode léger parce qu'on n'a pas le matériel pour prendre en charge un nœud complet.

-cache=4096, spécifie tout simplement la quantité de RAM que nous souhaitons utiliser sur le système.

-- **http**, exécute simplement le serveur web pour geth, cela permet d'interagir avec geth et de collecter des métriques.

-- **metrics**, cela permet d'avoir des rapports améliorés pour geth.

-- **maxpeers 10**, spécifie le nombre maximum de pairs que notre système peut prendre en charge.

Après avoir écrit le fichier on clique sur enregistrer, cela nous redirige directement vers l'invite de commande et nous affiche un message d'avertissement (voir la capture ci-dessus).

```
[Unit]
Description=Go Ethereum client
After=network.target
Wants=network.target

[Service]
User=djiby
Group=metapod
Type=simple
Restart=always
RestartSec=5
ExecStart=geth --datadir /media/cisco/blob/chain/data --port 41556 --syncmode "light" -cache=4096
--http --metrics --maxpeers 10

[Install]
WantedBy=default.target
```

La commande : ***sudo cat /etc/systemd/system/geth.service***, permet de vérifier que le fichier a été créé et enregistré correctement.

```
cisco@cisco-HP-ProDesk-400-G6-MT:/$ sudo cat /etc/systemd/system/geth.service
[Unit]
Description=Go Ethereum client
After=network.target
Wants=network.target

[Service]
User=djiby
Group=metapod
Type=simple
Restart=always
RestartSec=5
ExecStart=geth --datadir /media/cisco/blob/chain/data --port 41556 --syncmode "light" -cache=4096
--http --metrics --maxpeers 10

[Install]
WantedBy=default.target

cisco@cisco-HP-ProDesk-400-G6-MT:/$
```

La commande : ***sudo systemctl daemon-reload***, permet de recharger le démon de service, afin qu'il puisse relire le nouveau service.

La commande : ***sudo systemctl start geth,*** permet de démarrer le service geth.

La commande : ***sudo systemctl status geth***, permet de voir le statut du service. Le grand cercle en vert nous permet de dire que le service s'est correctement démarré.

```
mom@mom-VirtualBox:~$ sudo systemctl daemon-reload
[sudo] Mot de passe de mom :
mom@mom-VirtualBox:~$ sudo systemctl start geth
mom@mom-VirtualBox:~$ sudo systemctl status geth
● geth.service - Go Ethereum Client
     Loaded: loaded (/etc/systemd/system/geth.service; disabled; vendor preset>
     Active: active (running) since Tue 2022-06-28 20:20:41 GMT; 1min 0s ago
   Main PID: 3719 (geth)
      Tasks: 12 (limit: 1689)
     Memory: 396.5M
     CGroup: /system.slice/geth.service
             └─3719 /usr/bin/geth --datadir /home/mom/chain/data/ --port 51372>

suw 28 20:21:09 mom-VirtualBox geth[3719]: INFO [06-28|20:21:09.855] New local>
suw 28 20:21:09 mom-VirtualBox geth[3719]: INFO [06-28|20:21:09.879] Started P>
suw 28 20:21:10 mom-VirtualBox geth[3719]: INFO [06-28|20:21:10.347] IPC endpo>
suw 28 20:21:10 mom-VirtualBox geth[3719]: INFO [06-28|20:21:10.347] HTTP serv>
suw 28 20:21:10 mom-VirtualBox geth[3719]: WARN [06-28|20:21:10.348] Light cli>
suw 28 20:21:20 mom-VirtualBox geth[3719]: INFO [06-28|20:21:20.305] Looking f>
suw 28 20:21:23 mom-VirtualBox geth[3719]: INFO [06-28|20:21:23.311] Block syn>
suw 28 20:21:30 mom-VirtualBox geth[3719]: INFO [06-28|20:21:30.530] Looking f>
suw 28 20:21:41 mom-VirtualBox geth[3719]: INFO [06-28|20:21:41.003] Looking f>
suw 28 20:21:51 mom-VirtualBox geth[3719]: INFO [06-28|20:21:51.495] Looking f>
suw 28 20:22:02 mom-VirtualBox geth[3719]: INFO [06-28|20:22:02.151] Looking f>
```

La commande : ***la commande sudo journalctl -fu geth.service***, permet de visualiser la sortie de geth, il s'attache au service invité et imprime les données de geth (les blocs, leur âge, leur hash, etc.,).

```
mom@mom-VirtualBox:~$ sudo journalctl -fu geth.service
-- Logs begin at Sun 2021-11-07 18:32:11 GMT. --
suw 28 20:24:38 mom-VirtualBox geth[3719]: INFO [06-28|20:24:38.975] Imported n
ew block headers               count=2048 elapsed=12.394s  number=13,847,103 ha
sh=25e646..492356 age=6mo1w2d
suw 28 20:24:48 mom-VirtualBox geth[3719]: INFO [06-28|20:24:48.888] Looking fo
r peers                        peercount=2 tried=5  static=0
suw 28 20:24:50 mom-VirtualBox geth[3719]: INFO [06-28|20:24:50.215] Imported n
ew block headers               count=2048 elapsed=11.238s  number=13,849,151 ha
sh=f9a85e..3b4711 age=6mo1w2d
suw 28 20:24:59 mom-VirtualBox geth[3719]: INFO [06-28|20:24:59.257] Looking fo
r peers                        peercount=2 tried=4  static=0
suw 28 20:25:01 mom-VirtualBox geth[3719]: INFO [06-28|20:25:01.392] Imported n
ew block headers               count=2048 elapsed=11.175s  number=13,851,199 ha
sh=97a015..8fbe6b age=6mo1w1d
suw 28 20:25:11 mom-VirtualBox geth[3719]: INFO [06-28|20:25:11.019] Looking fo
r peers                        peercount=2 tried=9  static=0
suw 28 20:25:12 mom-VirtualBox geth[3719]: INFO [06-28|20:25:12.431] Imported n
ew block headers               count=2048 elapsed=11.038s  number=13,853,247 ha
sh=33f07f..16d22f age=6mo1w1d
suw 28 20:25:23 mom-VirtualBox geth[3719]: INFO [06-28|20:25:23.594] Imported n
ew block headers               count=2048 elapsed=11.161s  number=13,855,295 ha
sh=834ef7..44a14c age=6mo1w1d
suw 28 20:25:34 mom-VirtualBox geth[3719]: INFO [06-28|20:25:34.458] Imported n
ew block headers               count=2048 elapsed=10.862s  number=13,857,343 ha
sh=fbfae5..b95c29 age=6mo1w23h
suw 28 20:25:45 mom-VirtualBox geth[3719]: INFO [06-28|20:25:45.367] Imported n
ew block headers               count=2048 elapsed=10.905s  number=13,859,391 ha
sh=dfd7a7..8b13b9 age=6mo1w15h
```

La capure ci-dessus nous permet de voir l'importation des nouveaux blocs, leurs hashs, leurs ages, ici on peut clairement voir que le systéme a chargé des blocs de 6 mois parce qu'on a choisi le mode leger lors de la configuration. Apres le lancement de la sysnchronisation des blocs le systéme a trouvé deux pairs. On peut clairement voir sur la capture le temps écoulé pour chaque bloc (ça varie entre 10 et 13 seconde) et sa place dans la chaine (on a le bloc 13857343, le bloc 13859391, etc.,)

La commande : ***sudo systemctl enable geth***, permet au service geth de démarrer lorsque l'ordinateur est démarré.

La commande : ***sudo systemctl disable geth***, pour désactiver le démarrage automatique.

```
mom@mom-VirtualBox:~$ sudo systemctl enable geth
[sudo] Mot de passe de mom :
Created symlink /etc/systemd/system/default.target.wants/geth.service → /etc/sy
stemd/system/geth.service.
mom@mom-VirtualBox:~$ sudo systemctl disable geth
Removed /etc/systemd/system/default.target.wants/geth.service.
mom@mom-VirtualBox:~$
```

La commande : ***sudo geth attach --datadir /home/mom/chain/data***, permet de se connecter au service client et d'interagir avec la blockchain. Après exécution de cette commande, si tout se passe bien, on va rentrer sur l'accueil de la console javascript geth, ce qui montre en quelque sorte, on peut interagir avec la blockchain.

La commande ***: eth.syncing***, avec comme resultat « false » montre que notre client geth est entièrement synchronisé avec la blockchain.

```
mom@mom-VirtualBox:~$ sudo geth attach --datadir /home/mom/chain/data
Welcome to the Geth JavaScript console!

instance: Geth/v1.10.13-stable-7a0c19f8/linux-amd64/go1.17.2
at block: 15048380 (Thu Jun 30 2022 03:36:02 GMT+0000 (GMT))
 datadir: /home/mom/chain/data
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 les:1.0 net:1.0 personal:1.0 r
pc:1.0 txpool:1.0 vflux:1.0 web3:1.0

To exit, press ctrl-d or type exit
> eth.syncing
false
>
```

NB : On pouvait aller plus loin, en testant d'autres commandes mais pour l'instant on préfère en rester là.

1.7.2 . Les smarts contracts

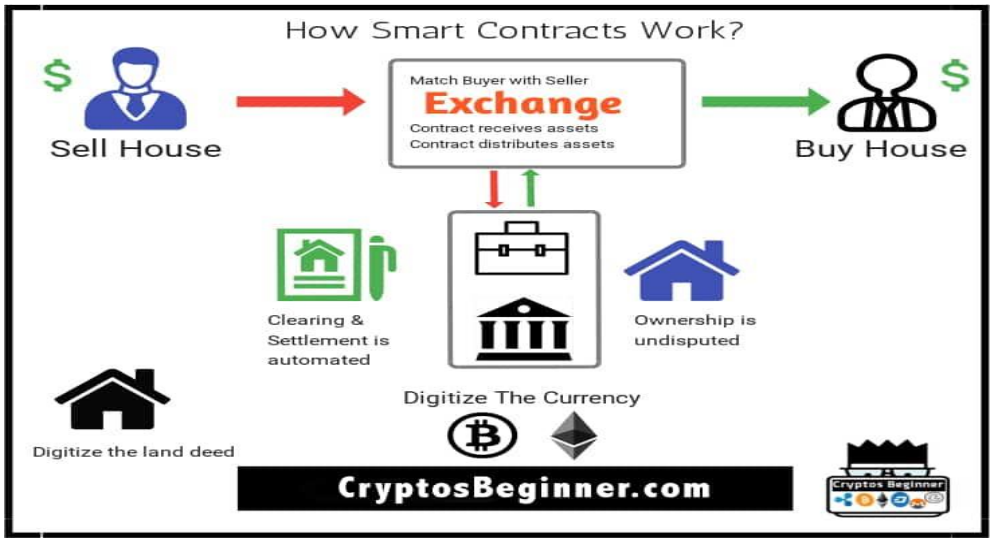


Figure 13:Les Smarts Contracts [43].

Le concept a été discuté depuis la fin des années 90, mais les plateformes pour exécuter des contrats intelligents sans implication des tiers n'ont été possible qu'avec l'avènement de la blockchain. Les parties qui se méfient mutuellement peuvent utiliser des systèmes de contrats intelligents sur des monnaies décentralisées. Un contrat intelligent est un petit programme informatique développé en utilisant un langage de haut niveau (Solidity, Vipper, etc.). Le programme est ensuite compilé en byte code et s'exécute sur une machine virtuelle. Les contrats intelligents sont sécurisés, rapides, rentables et autonomes.

- Comment fonctionne les smarts contracts ?

Les participants transfèrent des unités de devise dans le contrat, une fois que les conditions contractuelles ont été négociées et programmées. Apres négociation des termes du contrat, le contrat intelligent est automatiquement validé et exécuté dans la blockchain. La validation du contrat dans la blockchain peut entrainer la libération des fonds si les conditions contractuelles ont été remplies sinon c'est-à-dire lorsque les conditions ne sont pas remplies, les fonds seront retournés aux utilisateurs initiaux.

- Quelles blockchains les utilisent ?

Les blockchain Bitcoin et Ethereum offrent la capacité d'exécuter des contrats intelligents, même si bitcoin a un support moins programmable pour les contrats intelligents, ce qui rend leurs rédactions très difficiles.

Par contre Ethereum est la première plate-forme de blockchain, conçue pour les smarts contracts et les applications décentralisées. Même si Ethereum fournit un support programmable

indispensable pour les contrats intelligents, le nombre de transactions pouvant être traitées par seconde est limité.

Y'a aussi **Zilliqa** qui est une plateforme de blockchain conçue pour évoluer dans les taux de transactions, qui propose également un langage de contrat intelligent et un environnement d'exécution spécial.

EOS est encore une autre plateforme de contrat intelligent puissante qui fournit une version décentralisée d'un système d'exploitation pouvant atteindre des millions de transactions par seconde [44], [45].

Exemple de smart contract avec solidity :

```
41
42      //Approval
43      function approve(address spender, uint256 tokens) public returns (bool){
44          _allowances[msg.sender][spender] = tokens;
45          emit Approval(msg.sender, spender, tokens);
46          return true;
47      }
48
49      //Permet au priopiétaire du contrat de transférer un nombre de tokens à une autre addresse
50      function transfer(address to, uint256 tokens) public returns (bool){
51          _balances[msg.sender] = _balances[msg.sender] - tokens;
52          _balances[to] = _balances[to] + tokens;
53          emit Transfer(msg.sender, to, tokens);
54          return true;
55      }
56
57      //Permet au priopiétaire du contrat de transférer un nombre de tokens d'une addresse donnée à une autre add
58      function transferFrom (address from, address to, uint256 tokens) public returns (bool){
59          _balances[from] = _balances[from] - tokens;
60          _allowances[from][msg.sender] = _allowances[from][msg.sender] - tokens;
61          _balances[to] = _balances[to] + tokens;
62          emit Transfer(from, to, tokens);
63          return true;
64      }
65  }
66
```

Figure 14:exemple de smart contract [43].

La figure ci-dessus montre l'exemple d'un smart contract (écrit en Solidity). Ce contrat possède une méthode *transfer* qui permet de transférer des fonds à une autre adresse, une méthode *transferFrom* qui permet de transférer un montant donné d'une adresse à une autre adresse, et une méthode *approve* qui permet d'approuver une transaction.

1.7.3 . Les NFTs

Les NFT (Not Fongible Tokens), initiés en 2015, ce sont des biens numériques uniques, dont les transactions se font en cryptomonnaie.

Ils sont utilisés pour désigner le plus souvent une œuvre d'art numérique, ça peut aussi être des tweets, des gifs, des chansons, des noms de domaines, etc. Le NFT (jeton non fongible) est un jeton qui appartient à la même catégorie que les XRP ou en encore les bitcoins. Néanmoins, il diffère des autres crypto monnaies par sa caractéristique « non fongible ». Chaque jeton

initialement créé sur une plateforme de contrats intelligents est unique, c'est-à-dire que tout le monde est libre d'en créer, d'en acheter ou d'en vendre sans avoir à demander une quelconque autorisation. La plupart des NFT sont basés sur Ethereum donc pour en acheter sur cette plateforme, il est indispensable d'installer l'application Metamask.

Ci-dessous quelques exemples de projets NFT [46], [47]:

- **Les cryptopunk** : Ce sont des jetons représentant chacun un « crypto art » unique : un être humain au look punk. En janvier 2021 un cryptopunk a été vendu à 605 ether, soit 750000 $;
- **Enjin :** C'est un réseau de jeux fondé en 2009. Il a commencé a utilisé les NFT en 2017 avec le lancement de Enjin Coin. Ce dernier peut être utilisé pour symboliser des éléments de jeux sur Ethereum ;
- **Nba Top Shot :** Récemment, la Nba (National Association Basketball) a lancé une application Blockchain, pour commercialiser des objets de collection. L'application permet essentiellement d'acheter des clips vidéo contenant les meilleurs moments forts des jeux les plus mémorables de la série. Chaque semaine, des packs limités de NFT sont émis, avec des prix qui varient en fonction de leur authenticité.

  Ci-dessous une image montrant des exemples de cryptopunks :

Figure 15:Exemples de cryptopunks [48].

1.7.4 . Les finances décentralisées (Defi)

La finance décentralisée représente un écosystème où chacun pourrait profiter de différents services et produits financiers, sans organe de contrôle. Cela veut dire que n'importe quel utilisateur pourrait par exemple accéder à des prêts, sans aucune discrimination.

La DeFi regroupe de nombreuses applications décentralisées reposant sur la Blockchain, ayant pour but de rénover l'accès, l'utilisation d'outils, les services bancaires et financiers traditionnels.

On note différents types d'applications DeFi :

- **Les plateformes d'emprunts et de prêts** : Ces plateformes utilisent les contrats intelligents pour gérer automatiquement et sans intermédiaire les transactions ;
- **Decentralised Exchange (DEX)** : Les échanges décentralisés agissent comme une bourse en ligne mettant en relation des acheteurs et des vendeurs de devises numériques ;
- **Le Staking** : Il s'agit de l'action d'immobiliser certaine quantité de jetons pour obtenir des revenus passifs, un peu comme un compte épargne ;
- **Les stables coins** : Ce sont des crypto monnaies ayant une valeur stable liée à un autre actif, généralement une monnaie fiduciaire populaire comme le dollar américain.

  Voici quelques exemples de plateformes DeFi : Cred, Celsuis, Crypto.com, BlockFi, PolyNetwork, etc.

  Cependant l'investissement dans la finance décentralisée n'est pas sans risque car il y'a beaucoup de piratages ces derniers temps dans cet écosystème. L'exemple le plus récent est le piratage du Poly Network où l'hackeur avait réussi à dérober 611 millions de dollars dans le réseau mais l'a finalement rendu trois (3) jours après [49], [50].

1.7.5 . Les registres de titres de propriétés :

Elles peuvent être répertoriées comme une application très importante de la technologie blockchain.

Les registres écrits des droits de propriété se sont révélés assez vulnérable :

- La confiscation de terres via la falsification ou la destruction de documents publics ;
- La reconstruction à partir d'enregistrement informels est également couteuse, sujette aux erreurs et risque de fraude ;
- La transcription directe des documents écrits dans un référentiel en ligne centralisé peut aggraver les problèmes avec une possible perte de données et une falsification.

  Pour remédier à toutes ces problèmes énumérés, la **Blockchain** aide à fournir à la plateforme un registre distribué ouvertement auditable pour stocker les titres de propriétés sur la blockchain avec un cout minimum.

L'élimination de la fraude, la transparence, la rentabilité, le transfert des droits sans l'intervention d'un notaire tiers, sont les principaux avantages d'un registre des titres de propriétés basé sur la Blockchain [4].

1.7.6 . Le vote numérique :

Une application importante qui pourrait fonctionner sur une Blockchain ouverte et autorisée.
Les élections sont menacées d'actions malveillantes telles que :

- Le gonflage des machines à vote ;
- La modification de la base de données d'inscriptions des électeurs ;
- La coordination des campagnes de désinformation ;
- Compromettre les systèmes de rapport électoraux.

La Blockchain face à tous ces problèmes énumérés ci-dessus :

- **Pendant la pré-élection** : La Blockchain sous-jacente pourrait aider à garantir que le contenu numérique provient d'une source fiable et responsable, cela pourra réduire la propagande affectant les faux jugements des élections ;
- **Pendant l'élection** : La Blockchain aide à stocker les données d'identité des électeurs pour l'authentification mais aussi enregistrer en toute sécurité les votes numériques tout en éliminant les risques de piratages de la base de données des électeurs ;
- **Apres l'élection** : Les auditeurs indépendants peuvent auditer les résultats des élections enregistrées sur une Blockchain ouverte autorisée, tout en gardant l'identité confidentielle.

Par titre d'illustration : En 2018 lors des élections de mi-mandat aux USA, La Virginie Occidentale a mené avec succès un projet pilote de vote mobile soutenu par un réseau distribué et redondant de serveurs blockchain pour le personnel militaire et leurs familles travaillant à l'étranger.

Toutefois ça à manquer de transparence suffisante car le vote s'est déroulé sur une blockchain autorisée fermée [4], [51].

1.8 . Les acteurs de la blockchain

Etant une technologie bien structurée et prometteuse, la blockchain nécessite que de nombreux acteurs jouant des rôles spécifiques soient pleinement fonctionnels. Parmi ces acteurs, on peut citer [2] :

- **Un architecte blockchain**, qui est le designer de la solution blockchain. Pour qu'une solution blockchain soit fonctionnelle, elle doit d'abord exister. L'architecte blockchain est la personne ou le groupe qui a conçu la blockchain ;
- **Un operateur blockchain**, qui stocke et met à jour le livre de la blockchain. Une fois que la solution blockchain est conçue et réalisée, un opérateur peut s'associer pour créer le réseau homologue pair à pair. Le rôle de l'opérateur est de configurer et de maintenir des pairs au sein du réseau ;
- **Les développeurs blockchains**, qui créent des contrats intelligents à exécuter sur la blockchain. La fonctionnalité de la blockchain a été considérablement étendue par l'introduction de blockchains prenant en charge des contrats intelligents. Les développeurs conçoivent et téléchargent des contrats intelligents dans la blockchain pour étendre ses capacités. Outre la mise en œuvre des contrats intelligents, des développeurs frontend peuvent également implémenter des applications qui accèdent à la blockchain (c'est-à-dire que les applications initient les transactions sur la blockchain) ;
- **Le régulateur blockchain**, de nombreuses entreprises sont soumises à des réglementations concernant la manière dont leurs données doivent être stockées et traitées. Pour les solutions de type blockchain, un régulateur peut avoir une plus grande visibilité dans le grand livre historique en raison de son rôle au sein de l'organisation ;
- **L'utilisateur final**, qui est le consommateur de services construits autour de la blockchain. En règle générale, cela implique l'utilisation d'un logiciel qui utilise la blockchain comme solution de stockage principale. Les utilisateurs interagissent rarement directement avec la blockchain ;
- **Le stockage des données**, qui est représenté par les bases de données traditionnelles pour stocker les données hors chaîne. La blockchain fournit un stockage distribué immuable avec un contrôle d'intégrité intégré ; Cependant, sa capacité maximale est basée sur la taille et le taux de blocs standard. Pour permettre la vérification de l'intégrité de grandes quantités de données, il est courant de stocker les données hors chaîne et de stocker un hachage des données en chaîne. Cela garantit que les données ne sont pas modifiées tout en protégeant la blockchain contre le gonflement ;
- **Le traitement des données**, qui est représenté par un système externe utilisé pour un traitement supplémentaire. Les contrats intelligents s'exécutent sur la blockchain, ce qui signifie que chaque membre du réseau homologue doit exécuter le code pour rester synchronisé avec l'état actuel du réseau. Si les contrats intelligents nécessitent

généralement une grande quantité de puissance de traitement, des périphériques externes au réseau homologue peuvent être utilisés pour augmenter la puissance de traitement du réseau.

1.9 . Les avantages et limites de la blockchain

Malgré qu'elle soit une technologie bien conçue et présentant de nombreux avantages, la blockchain a certains aspects que les gens considèrent aussi comme des limites. Nous allons essayer d'énumérer quelques avantages et limites de la blockchain [52], [53].

1.9.1 . Les avantages de la blockchain :

- **La décentralisation**

  La décentralisation provient de l'absence d'intermédiaire de confiance lors des transactions, mais aussi du fait que chaque nœud du réseau dispose d'une copie de l'intégralité des données de la chaine. Les transactions de pair à pair et la décentralisation des données protègent donc les utilisateurs d'un certains nombres de maux tels que : La fragilisation du système, les conflits d'intérêts, etc. ;

- **La sécurité et la stabilité du système**

  Les blockchains sont réputées parfaitement inviolables. La sécurité d'une blockchain est assurée par ses utilisateurs eux même, notamment à travers le processus de minage. Ce dernier nécessite des calculs mathématiques complexes, impliquant des fonctions de hachages, qui demandent une grande puissance de calcul ;

- **La rapidité des transactions**

  La technologie blockchain permet d'effectuer des transactions monétaires entre deux parties de manière bien plus rapide que dans le cadre classique des monnaies fiat. En effet, du fait de l'absence de passage par un tiers, la validation ainsi que l'exécution d'une transaction ne prennent pas plus de quelques minutes. Les temps de transactions très faibles font donc partie des avantages majeures de la blockchain ;

- **La fiabilité des données**

  L'immuabilité fait partie des caractéristiques de la technologie blockchain, ce qui fait que son journal de transaction soit infalsifiable. Une fois une transaction validée et ajouté dans le réseau, on ne peut ni la modifier, ni la supprimer. Les informations contenues dans une blockchain sont ainsi d'une haute fiabilité, en plus d'être parfaitement traçables.

1.9.2 . Les limites de la blockchain :

- **La taille de la blockchain**

  Par exemple Bitcoin a une taille de 220Go en Aout 2019.

  Même si Ethereum a introduit un concept appelé « élagage » pour contre-attaquer la taille de stockage croissante de la blockchain, ce qui n'empêche pas Ethereum de compter actuellement plus de 120 Go en taille. La taille très importante des blockchains réduit considérablement le nombre d'individu pouvant participer au réseau blockchain en tant que nœuds complets ;

- **L'anonymat**

  L'anonymat relatif des transactions a fait de la blockchain un refuge privilégié par les activités illicites tel le blanchiment d'argent, le trafic d'armes ou de drogue. De ce fait, les cryptomonnaies adossées aux blockchains sont un peu l'argent liquide du net. La lutte contre les transactions frauduleuses est un enjeu central, elle n'est pas impossible grâce à la traçabilité permise par la blockchain ;

- **La forte consommation d'énergie**

  Le système de validation par proof of work, utilisé par de nombreuses blockchains notamment bitcoin, assurant la sécurité du registre consomme énormément d'énergie. Bien que cela soit difficile à estimer, le fonctionnement du Bitcoin aurait une consommation électrique équivalente à celle de l'Irlande.

1.10 . Conclusion

En somme, ce chapitre nous a permis de nous familiariser avec cette technologie novatrice qu'est la blockchain. Il a nous a permis aussi d'avoir une idée sur ses domaines d'applications, ses avantages et limites mais aussi sur les différents protocoles qu'elle utilise pour l'intégrité et le bon fonctionnement de son réseau. Ces protocoles sont d'une importance capitale. Le chapitre suivant sera dédié en intégralité aux protocoles (les algorithmes de consensus) de la blockchain.

Chapitre 2 : Les algorithmes de consensus de la Blockchain

2 . Introduction et définition

Un algorithme de consensus est un mécanisme par lequel un réseau Blockchain parvient à trouver un accord afin d'ajouter un nouveau bloc. Les algorithmes de consensus peuvent être classés en deux (2) groupes principaux : les consensus basés sur la preuve et les consensus basés sur le vote. Dans ce chapitre nous allons essayer en premier temps, de lister, mais aussi d'expliquer le mode de fonctionnement des différents algorithmes de consensus (preuve comme vote). Ensuite faire une étude comparative de ces algorithmes en donnant aussi les plateformes blockchains qui les utilisent.

2.1 . Classification des algorithmes de consensus de la Blockchain

La figure 17 ci-dessous montre une classification des algorithmes de consensus.

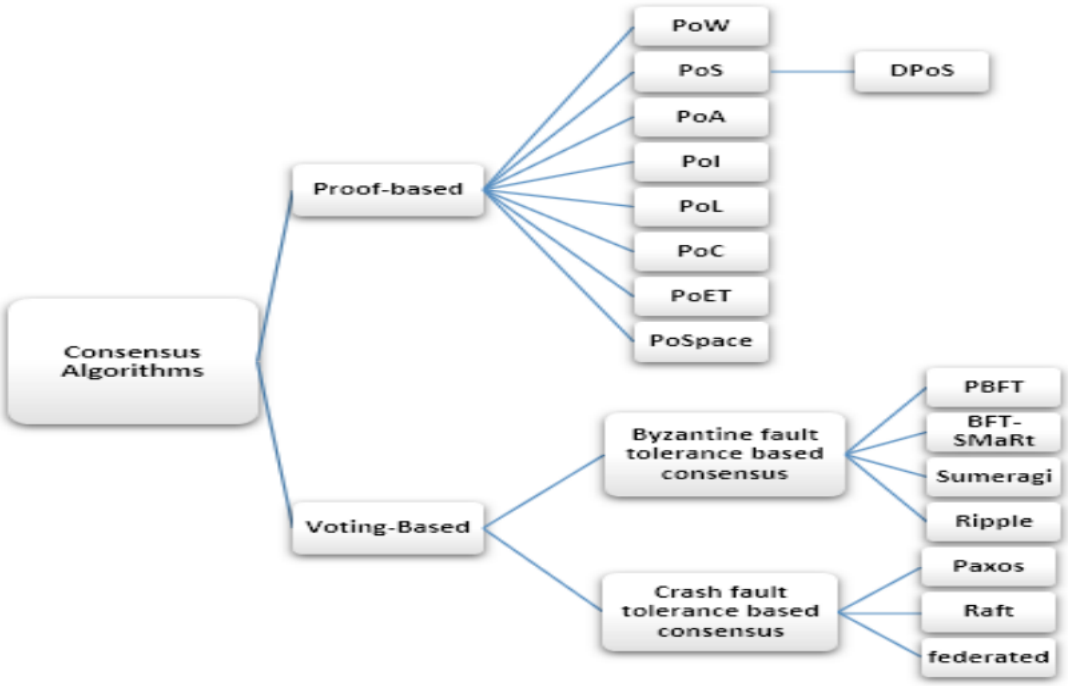


Figure 16:Classification des algorithmes de consensus [54].

2.2 . Les algorithmes de consensus basés sur la preuve

Ce consensus exige que les nœuds rejoignant le réseau de vérification montrent qu'ils sont plus qualifiés que les autres pour effectuer le travail d'ajout. On note l'existence de plusieurs algorithmes de consensus basés sur la preuve :

2.2.1 . La preuve de travail ou proof of work (PoW)

Afin d'obtenir un accord entre tous les mineurs sur le bloc nouvellement ajouté, le PoW exige que chaque mineur résolve un puzzle avec une difficulté ajustée, pour obtenir le droit d'ajouter un nouveau bloc à la chaine actuelle. Le premier qui réussit à le résoudre, aura ce droit. Avant de résoudre le puzzle par exemple deviner la valeur secrète du champs nonce, les nœuds de vérification devront au préalable mettre leurs transactions vérifiées, le Prev_Hash et le Timestamp dans un bloc.

Toutes les informations contenues dans l'entête de bloc seront combinées et entrées dans une fonction de hachage SHA-256. Si la sortie de cette fonction est inférieure à un seuil T donné, la valeur est acceptée, sinon le mineur doit faire une autre estimation de la valeur secrète jusqu'à ce qu'il obtienne la réponse. Plus l'énigme est difficile, plus le seuil est petit.

Lorsqu'un mineur trouve la valeur secrète, il diffuse son bloc avec cette valeur à d'autres nœuds pour les notifier que la réponse a été trouvée, les autres nœuds vérifient la validité du bloc diffusé, si tout est ok le bloc sera ajouté dans la chaine et le mineur récompensé [55], [56].

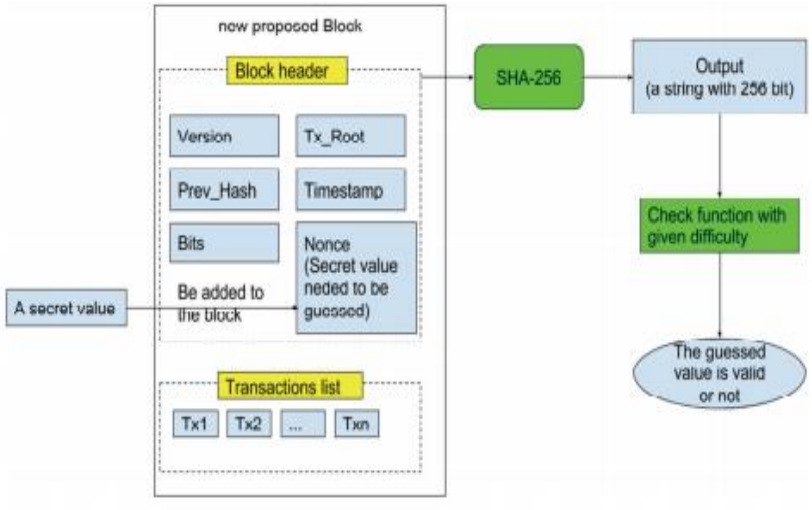


Figure 17:PoW fonctionnement [57].

Cependant il y'a un cas rare où plus d'un mineur trouve les réponses au puzzle. Dans ce cas les mineurs diffuseront toujours leur bloc avec le nonce trouvé. Par la suite les autres mineurs qui reçoivent le premier bloc à venir ignorent les autres qui arriveront, ce qui conduit aux problèmes de la fourche.

Solution à la fourche

Satoshi a proposé que ces mineurs continuent à extraire un nouveau bloc sur leurs fourches, jusqu'à ce qu'une fourche soit plus longue que les autres. En ce moment tous les nœuds doivent suivre cette longue fourche.

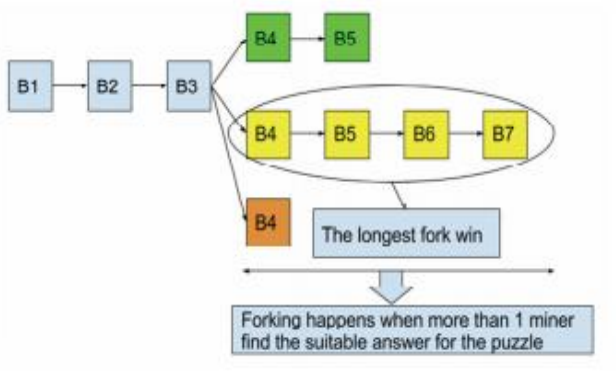


Figure 18:La solution à la fourche [57].

2.2.2 . La preuve d'enjeu ou proof of stake (PoS)

Pour cet algorithme celui qui a misé le plus, a plus de la chance d'exploiter un nouveau bloc. Par exemple s'il y'a une totale de b pièce de tous les mineurs, et un mineur M possède une pièce (a<b), la chance pour ce mineur d'obtenir le droit d'exploiter un nouveau bloc est a/b. Le travail de cueillette des mineurs chanceux est exécuté toutes les 60 minutes, et ce travail est effectué au hasard en fonction de l'enjeu de chaque mineur.

Si un mineur est sélectionné, il vérifiera les transactions, les rassemblera dans un bloc puis les diffusera aux autres mineurs, si ces derniers le valident, il recevra les frais gratifiants.

Il y'a aussi la procédure de suivi du Satoshi, où on considère une valeur Satoshi comme étant la plus petite unité monétaire.

Cette procédure obtiendra une entrée en tant qu'indice Satoshi, qui est compris entre 0 et le nombre total de Satoshi, puis il trouvera le bloc qui l'a créé. Ensuite toutes les transactions incluant ce Satoshi seront découvertes pour identifier le dernier propriétaire, qui deviendra celui qui ajoutera le bloc suivant.

Le travail du choix de Satoshi est basé sur une fonction de hachage qui a trois (3) paramètres d'entrées :

- La première est une valeur obtenue à partir d'une fonction dite de peigne possédant des entrées sous forme de bits ;
- La deuxième est tirée du nombre de blocs actuels dans la chaine ;
- La troisième est un entier aléatoire [58], [2].

2.2.3 . La preuve d'enjeu délégué ou Delegated proof of stake (DPoS)

Cet algorithme a été introduit par Daniel Larimer (Larimer, 2014). Cette méthode est une amélioration de la méthode Proof of Stake afin que les nœuds sélectionnent des représentants par le biais d'un vote pour la validation des blocs. Le nombre de représentants est limité et cela permettra d'organiser plus efficacement le réseau et chaque représentant pourra déterminer le temps adéquat pour publier chaque bloc. Cette méthode a été utilisée dans les Bitshares. Cependant, cette limitation du nombre de représentants rendrait le réseau plus centralisé. Les caractéristiques les plus importantes de ce mécanisme peuvent être mentionnées comme l'évolutivité, l'efficacité énergétique et les transactions à faible coût. Malgré tous ces avantages, il s'agit d'un mécanisme semi-centralisé et il est préférable de l'utiliser dans les blockchains privées. Cependant, si un représentant sélectionné retarde ou commet une erreur dans la présentation des rapports requis, les nœuds du réseau peuvent voter pour déterminer son remplacement [59].

2.2.4 . La preuve d'activité ou proof of activity (PoActivity)

Les auteurs de cet algorithme ont déclaré avoir proposé un algorithme de consensus basé sur la combinaison de PoW et PoS. Cet algorithme est présenté comme une protection contre les problèmes potentiels de Bitcoin comme la "tragédie des biens communs", où les mineurs commencent à agir uniquement dans leur propre intérêt, et les attaques de réseau telles que le déni de service et l'isolement du réseau. Pour le bitcoin, la tragédie des biens communs peut se produire après que les 21 millions de pièces de récompense minière ont été extraites et que les mineurs ne reçoivent que des récompenses transactionnelles. De plus, dans Bitcoin, un attaquant peut essayer de manipuler le réseau sur les bourses dans lesquelles le Bitcoin est échangé, pour causer une perte de confiance. Cependant, avec les protocoles basés sur la preuve de participation, les parties prenantes sont moins susceptibles de subir des spirales de prix à la baisse, car les pièces qu'ils détiennent génèrent des revenus proportionnels au commerce réel en cours. En termes de sécurité, la probabilité d'attaque de 51% dans le PoActivity tombe à près de zéro, car une telle attaque nécessiterait à l'attaquant d'avoir 51% de toutes les pièces et aussi 51% de la puissance minière en même temps et, par conséquent, le PoActivity est plus sûr en comparaison à PoW et PoS. Deux crypto-monnaies populaires, Decred et Espers ont adopté le PoActivity dans leur blockchain[60], [61] .

2.2.5 . La preuve d'importance ou proof of importance (PoI)

Introduit pour la première fois dans le projet NEM, afin de répondre aux critiques de PoS.

Dans NEM, chaque nœud se voit attribuer un score d'importance qui influence ses chances d'obtenir une petite récompense financière en échange de l'ajout d'un bloc. Pour être éligible, un nœud doit avoir au moins 10000 XEM.

Y'a trois (3) facteurs qui déterminent le score global d'un nœud :

- **Acquisition** : plus le nombre de pièces acquises est élevée, plus le score est élevé. Seules comptent les pièces qui sont sur un compte depuis un certain nombre de jours ;
- **Partenariat transactionnel** : Celui qui effectue plus de transactions avec d'autres comptent NEM sur le réseau obtiendrait un meilleur score ;
- **Nombre et taille des transactions au cours des 30 derniers jours** : Chaque transaction au-dessus d'une taille minimale augmenterait le score du compte, les transactions les plus importantes et fréquentes ont un impact plus important. Cet algorithme résiste aux attaques de type Sybil (identités multiples afin de prendre le contrôle du système). Elle est rapide, économe en énergie et nécessite pas de matériel spécifique pour le minage [62].

2.2.6 . La preuve du temps écoulé ou proof of Elapsed Time (PoET)

La preuve du temps écoulé est présentée par Intel comme l'une des méthodes de consensus des blockchains similaires à la PoW, où chaque mineur est tenu de résoudre un problème de hachage. Chaque approbateur de bloc (mineur) est sélectionné dans les plus brefs délais, en respectant une fonction fiable grâce à la production en bloc. Cette élection sélectionne le mineur au hasard sur le réseau et utilise le Trusted Environnement d'exécution (TEE) qui est l'environnement d'exécution de confiance pour assurer la sécurité de son processus électoral. TEE est présenté par du matériel Intel spécifique (SGX, Secure Extension de garde). Le principal problème de cette méthode est sa dépendance vis-à-vis d'Intel qui entre en conflit avec la philosophie de base de la blockchain sur la décentralisation. En fait, on peut classer cette méthode comme un algorithme de consensus semi-centralisé [63].

2.2.7 . La preuve de poids ou proof of weight (PoWeight)

Utilisé dans Algorand, développé par des chercheurs du MIT, le Proof of Weight est un mécanisme de consensus qui donne aux utilisateurs un « poids » basé sur la quantité de crypto monnaie qu'ils détiennent. Elle est sécurisée tant que la majorité (2/3) des utilisateurs pondérés sont honnêtes et protège le réseau contre les attaques à double dépense. Elle a des ressemblances avec la PoS. Filecoin et Chia sont des exemples de crypto-monnaies utilisant actuellement

PoWeight. Filecoin calcule le facteur pondéré en tenant compte de la quantité de données IPFS qu'un utilisateur possède et appelle cet algorithme « Proof of Spacetime ». Chia dépend de la preuve de l'espace et de la preuve du temps pour parvenir à un consensus. La preuve de réputation est également un autre facteur pondéré utilisé dans les systèmes PoWeight. D'une part l'algorithme PoWeight apporte une personnalisation et une évolutivité considérables, confirme les transactions très rapidement et utilise efficacement une alimentation électrique. D'autre part, comme les participants ne reçoivent pas de récompenses dans ce réseau, il est difficile d'inciter les utilisateurs à participer [64].

2.2.8 . La preuve de brulure ou proof of burn (PoB)

Utilisé par Slimcoin, ici les mineurs ne doivent pas perdre d'énergie ou de temps pour prouver qu'ils ont fait quelque chose de difficile. Dans cet algorithme les mineurs doivent bruler certaines des crypto-monnaies qu'ils possèdent déjà pour obtenir des récompenses. Bruler signifie ici qu'un utilisateur doit envoyer des crypto-monnaies à « une adresse de mangeur » pour recevoir des pièces, jetons ou privilèges de minage sur le réseau (bitcoin-wiki). L'argent envoyé à cette adresse est irrécupérable et personne ne peut le dépenser à nouveau. Brûler des pièces est une activité couteuse mais ne consomme aucune ressource ni d'énergie.

La seule ressource utilisée dans le PoB est la volonté de l'utilisateur d'accepter une perte à court terme pour recevoir une récompense à long terme. Plus l'utilisateur brûle de pièces plus il a de la chance de trouver le prochain bloc [65].

2.2.9 . La preuve de capacité ou proof of capacity (PoC)

Le concept de preuve de capacité (PoC), également connu sous le nom de preuve d'espace (PoSpace) a été introduit par Dziembowski en 2015. Ici les mineurs utilisent les espaces libres sur leur disque dur pour miner des pièces gratuites. La première crypto-monnaie utilisant cet algorithme est Burstcoin fondée en 2014. L'algorithme PoC consiste à tracer le disque dur ce qui signifie calculer et stocker des solutions sur votre disque dur avant que le minage ne commence. Certaines solutions sont plus rapides que d'autres. Si un disque dur se trouve avoir stocké la solution la plus proche au puzzle du dernier bloc, il gagne le bloc. La mise en œuvre de l'algorithme de PoC consiste deux (2) étapes :

- La première étape est nommée traçage dans laquelle les mineurs créent quelque chose qui s'appelle "Nonce". Les nonces sont créés par hachage répété de données, y compris l'identifiant du mineur, à l'aide d'une fonction de hachage très lente connue sous le nom de Shabal. Comme les hachages Shabal sont difficiles à calculer, ils sont calculés à l'avance et sont stockés sur le disque dur sous forme de

nonces. Plus un mineur alloue d'espace libre au traçage, plus le nombre de nonces créés deviennent important. Les nonces contiennent 8192 hachages, formés deux à deux sur un scoop, donc un nonce contient 4096 scoops étiquetés de 0 à 4095 ;

- Avant de commencer à miner, un mineur doit remplir tout l'espace libre de son disque dur avec des nonces. Ces nonces agissent comme un billet de loterie qui contient une série de chiffres et de lettres. Si l'un des hachages dans un nonce est le plus proche du puzzle récent du réseau, cela signifie qu'il a gagné la bataille du minage.

  Ce réseau reste décentralisé, accessible, plus économe en énergie car nécessitant tout simplement un disque dur [66], [67].

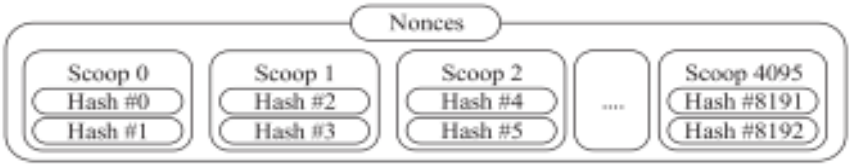


Figure 19:PoC, structure des nonces [67].

2.2.10. La preuve d'autorité ou proof of autority (PoAutority)

Dans les réseaux basés sur PoAutority, les transactions et les blocages sont validés par des comptes approuvés, appelés validateurs. Les validateurs exécutent des logiciels leur permettant de mettre les transactions en blocs. Le processus est automatisé et ne nécessite pas que les validateurs surveillent constamment leurs ordinateurs. Cependant, cela nécessite de maintenir l'ordinateur (le nœud d' autorité) sans compromis.

Les trois principales conditions qui doivent être remplies pour qu'un validateur soit établi sont :

- L'identité doit être formellement vérifiée en chaîne , avec la possibilité de recouper les informations dans un domaine accessible au public ;
- L'éligibilité doit être difficile à obtenir, pour avoir le droit de valider les blocs gagnés et valorisés. (Exemple : les validateurs potentiels sont tenus d'obtenir une licence de notaire public) ;
- Il doit y avoir une uniformité complète dans les contrôles et les procédures d'établissement d'une autorité.

Avec le PoAutority, les individus gagnent le droit de devenir validateurs, il y a donc une incitation à conserver le poste qu'ils ont acquis. En attachant une réputation à l'identité, les

validateurs sont incités à maintenir le processus de transaction, car ils ne souhaitent pas que leur identité soit attachée à une réputation négative, perdant ainsi le rôle de validateur durement gagné.

Utilisé par POA. Network, Vechain, cet algorithme est rapide et consomme pas beaucoup d'énergie. Elle est aussi un peu centralisée [68].

2.3 . Les algorithmes de consensus basés sur le vote

Dans ce consensus, les nœuds doivent être connu et flexible, afin qu'ils puissent échanger des messages plus facilement. Pour participer à ce consensus, les nœuds doivent respecter certains critères [69], [70]:

- Tous les nœuds du réseau devront participer au maintien du registre ;
- Doivent aussi vérifier l'ensemble des transactions dans les blocs ;
- Ils communiqueront entre eux avant décider d'ajouter ou non leurs blocs proposés à leur chaine ;

Le consensus basé sur le vote devrait être conçu pour résister à certains cas graves :

- Le plantage des nœuds ;
- L'écrasement ou la subversion des nœuds.

2.3.1 . Le consensus byzantin basé sur la tolérance aux pannes

En cas de plantage les nœuds attendront les messages des autres. Cependant certains nœuds ne s'exécuteront pas, alors les nœuds normaux ne reçoivent pas suffisamment de preuve pour pouvoir prendre des décisions. Il devrait y'avoir t= 2N/3 + 1 nœuds fonctionnant normalement afin d'éviter les cas de crashs et de nœuds subvertis. Voici quelques exemples d'algorithmes de consensus basés sur la tolérance aux pannes [57]:

2.3.1.1 . Tolérance aux pannes byzantines pratiques ou Pratical Byzantin Fault Tolerance (PBFT)

IBM avec HyperLedge Fabric utilise une sorte de tolérance aux pannes appelé PBFT. Dans ce consensus il existe deux (2) types de nœuds :

- Un nœud leader ;
- Certains pairs de validateurs qui exécuteront quelques tours afin d'ajouter un bloc à la chaine.

Les clients envoient leurs demandent de transactions à leurs homologues de validateurs correspondants ; le pair récepteur les diffusera à d'autres pairs y compris le leader. Si le nombre

de transactions atteint un seuil appelé taille de lot, le nœud principal les ordonne en fonction de leurs heures de création puis les met dans un bloc ce qui entraine l'exécution de trois (3) phases : Premièrement le leader diffuse son bloc proposé à d'autres pairs après réception ces derniers le stockent localement. Cette phase est appelée la pré-préparation. Ensuite ils procèdent à une double vérification en le diffusant dans la phase de préparation et de validation afin d'assurer que le bloc est fiable. Après la phase de préparation si 2/3 des nœuds reçoivent les mêmes blocs que ceux stockés localement alors ils exécuteront la phase de validation. Après cette dernière chaque nœud doit obligatoirement exécuter les transactions dans le bloc, puis l'ajouter à leur chaine. Y'a aussi Symbiont et R3 Corda qui sont des plateformes de Blockchain populaire utilisant un consensus byzantin basé sur la tolérance aux pannes appelé le BFTSMaRt qui est similaire au PBFT [71], [68].

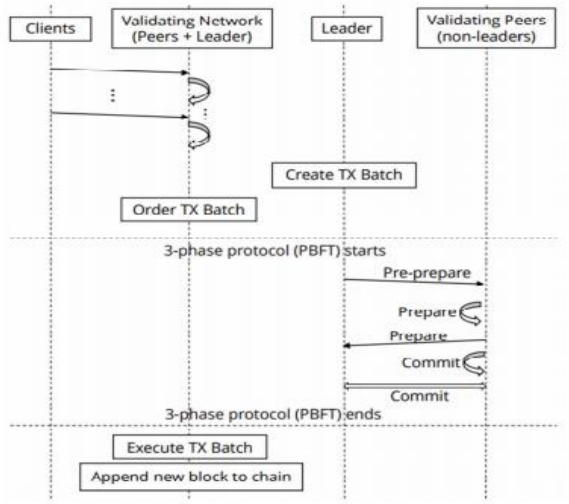


Figure 20: le PBFT [57].

2.3.1.2 . La tolérance aux pannes byzantines déléguées ou byzantine delegated fault tolerance (DBFT)

La tolérance aux pannes byzantine déléguée, un mécanisme de consensus byzantin tolérant aux pannes qui permet une participation à grande échelle au consensus par le biais du vote par procuration. Le détenteur du jeton NEO peut, en votant, choisir le comptable qu'il prend en charge. Le groupe de comptables sélectionnés, grâce à l'algorithme DBFT, parvient à un consensus et génère de nouveaux blocs. Le vote dans le réseau NEO se poursuit en temps réel plutôt que selon une durée déterminée.

Le DBFT fournit une tolérance aux pannes de f = [(n- 1) / 3] pour un système de consensus composé de n nœuds. Cette tolérance aux pannes inclut également la sécurité et la disponibilité, résiste aux pannes générales et byzantines, et convient à tout environnement réseau. DBFT a

une bonne finalité, ce qui signifie qu'une fois les confirmations définitives, le bloc ne peut pas être bifurqué et la transaction ne sera ni révoquée ni annulée. Utilisé par NEO cet algorithme est rapide et évolutif. L'inconvénients ici tout le monde se bat pour être la chaine racine. Il peut y'avoir plusieurs chaines racines [72].

2.3.1.3 . Sumeragi

Iroha est une plateforme Blockchain utilisant un algorithme de consensus appelé Sumeragi. Ici tous les nœuds sont disposés linéairement de sorte qu'un nœud donné ne recevra que le message de son nœud précédant et enverra de message qu'à son suivant dans la chaine. Ce qui permet d'éviter le travail de diffusion et d'équilibrer la charge entre les nœuds. Mais le coût du temps d'exécution et de reconfiguration en cas de panne est élevé. Il est aussi similaire aux PBFT et PBFTSMaRT [73].

2.3.1.4 . Le Quorum Slice ou Stellar

Stellar est une plateforme Blockchain utilisant un algorithme de consensus appelé Quorum Slice. Ici les nœuds de validation peuvent appartenir à une ou plusieurs tranches de quorum différentes. Pour une transaction donnée, si un nœud veut confirmer qu'elle est valide, il devra demander l'avis des autres nœuds de sa tranche de quorum, si la transaction est vérifiée avec succès par tous les nœuds de sa tranche alors il la considérera comme valide. Voir l'exemple figure 22 :

Par exemple (1,2,3,5) et (1,2,4,6) deux tranches de quorum créées par le nœud 1 ; le groupe1 et groupe2 sont les niveaux supérieurs (les transactions doivent d'abord être vérifiées à partir de ces deux niveaux). Pour que le nœud 10 vérifie une transaction donnée, il devra demander aux autres membres de sa tranche de quorum par exemple (1,2,7,10) si tous sont d'accords avec cette transaction, le nœud 10 la considère comme valide [74].

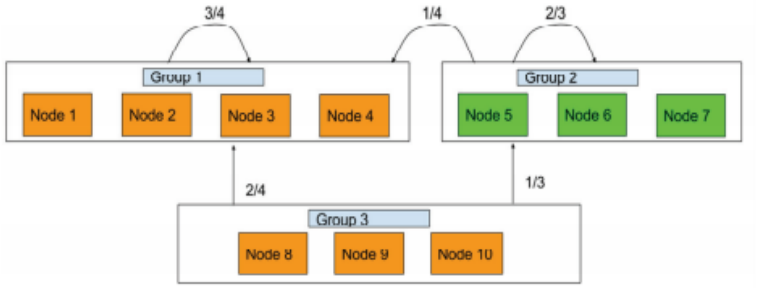


Figure 21:L'algorithme quorum slice [57].

2.3.1.5 . Ripple

Ripple est algorithme de consensus qui est censé amélioré les faiblesses de Bitcoin. Dans Ripple, la chaîne de blocs n'est pas utilisée, mais plutôt un grand livre brut ; et après quelques vérifications rondes, les transactions seront ajoutées directement au grand livre. Ici on ajoute de nouvelles transactions au grand livre si elles sont vérifiées avec succès par au moins 80 % de tous les serveurs. Pour gérer la vérification des transactions demandées, Ripple a deux formes principales : le dernier registre fermé, qui indique que toutes les transactions qu'il contient sont vérifiées avec succès par suffisamment de serveurs (80 %) ; et le grand livre ouvert, dont les transactions sont vérifiées par des serveurs insuffisants. Pour effectuer la vérification, au lieu de diffuser les transactions aux autres, chaque serveur a sa propre liste, appelée liste de nœuds uniques (UNL), qui comprend d'autres serveurs. Ces serveurs ne communiqueront avec les autres que dans leur UNL. Ils agrègent toutes les transactions correctes dans un soi-disant ensemble candidat. À ce stade, il y aurait quelques tours à faire pour un grand livre ouvert de devenir un dernier grand livre fermé.

Au premier tour, chaque serveur agrégerait tous les ensembles candidats des autres serveurs de son UNL dans son ensemble candidat, puis vérifierait les transactions à l'intérieur de cet ensemble. Un vote « oui » sera appliqué à chacune des transactions si elles sont vérifiées avec succès. Par la suite, lors des tours suivants, toutes les transactions qui ne reçoivent pas suffisamment de votes « oui » seront éliminées de l'ensemble des candidats (les derniers tours nécessitent au moins 80 % de votes pour chaque transaction). Afin de maintenir l'exactitude, il ne devrait y avoir au maximum (n–1) /5 nœuds subvertis parmi n nœuds dans le réseau [75], [76].

2.3.2 . Le consensus byzantin basé sur la tolérance aux pannes en cas de nœuds écrasés ou subvertis

C’est une sorte de consensus qui ne peut que prévenir les cas de crash de nœuds. Dans ce consensus il devrait y’avoir au moins T nœuds (T<N) fonctionnant normalement avec T= N/2 +1.

2.3.2.1 . Raft

Raft est un algorithme de consensus utilisé pour tolérer les plantages et il doit y’avoir à chaque fois N/2 +1 des nœuds fonctionnants normalement.

Dans cet algorithme les nœuds sont repartis en suiveur, candidat et leader. La communication entre ces nœuds se fait à travers deux principaux types de messages :

- Request Vote : pour voter le nœud leader ;
- AppendEntries : pour transférer les requêtes vers d'autres nœuds.

Au départ tous les nœuds sont des suiveurs. Le leader reçoit les transactions demandées par les clients, il les écrit dans une liste appelée entrée de journal, ensuite il envoie aux suiveurs le message AppendEntries contenant chaque transaction enregistrée (R)et l'index de la transaction précédente (pi) dans la liste. Lorsqu'un suiveur reçoit le message AppendEntries, si pi est l'indice de la dernière transaction qu'il a reçu, il écrira R dans sa liste d'entrée de journal. Sinon le leader devra trouver la dernière transaction que lui et le suiveur ont en commun, puis le suiveur va recommencer à synchroniser la liste des entrées du journal avec le leader. Ce processus permet de vérifier que les transactions sont ordonnées de la même manière dans tous les nœuds de vérification. Apres vérification le nœud leader choisi un index puis valide toutes les transactions et les mettent dans un bloc qu'il ajoutera dans sa chaine. Par la suite il diffusera le résultat aux autres nœuds, qui à leurs tours ajouteront le bloc dans leurs chaines [73].

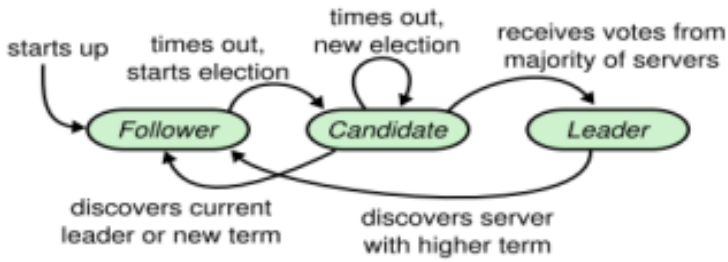


Figure 22:Raft [73].

2.3.2.2 . Fédéré

Fédéré est un algorithme de consensus utilisé par Chain.

Dans cet algorithme parmi n nœuds du réseau, il y'a un appelé générateur de bloc et d'autres nœuds appelés signataires de bloc. Le générateur de bloc reçoit les transactions des clients, les vérifient et stockent celles valides dans une liste temporaire, puis il les envoie aux signataires de bloc. Si un bloc est signé par plus de M (M < N) signataires de bloc différents, le générateur de bloc ajoutera le bloc à sa chaine actuelle et proposera ce bloc aux autres nœuds. Chain pourrait résister à l'erreur de plantage si un signataire de bloc ne fonctionne pas. Cependant si ce cas se produit avec le générateur de bloc, le réseau sera interrompu.

2.4 . Etude comparative des algorithmes de consensus

Le tableau 1 ci-dessous nous permet de faire une comparaison entre la preuve de travail (PoW) et la preuve d'enjeu ou de participation (PoS), les deux algorithmes de consensus les plus populaires et les plus utilisés dans la technologie Blockchain. On va essayer de mettre en exergue quelques critères comme la forte consommation d'énergie, le problème de fourche, les moyens nécessaires pour pouvoir miner, le problème de l'attaque à double dépense et quelques exemples de blockchains utilisant ces algorithmes [77], [78], [79], [80].

Critères	**PoW**	**PoS**
Efficacité énergétique	**Non**	**Oui**
Matériel moderne	**Très important**	**Pas nécessaire**
Problème de Fourche	**Lorsque deux nœuds trouvent le nonce approprié en même temps**	**Très difficile**
Attaque à double dépense	**Oui**	**Difficile**
Exemples	**Bitcoin, Ethereum, Litecoin, Dogecoin…**	**Ethereum (dans sa prochaine mise à jour), Peercoin, Nxt…**

Tableau 2: comparaison entre PoW et PoS.

L'analyse du tableau 2 montre que les deux algorithmes de consensus à savoir le PoW et le PoS fonctionnent différemment, le premier cité consomme énormément d'énergie et nécessite des matériels spécifiques pour le minage alors que dans l'autre (le PoS), il suffit juste d'avoir des fonds car celui qui mise le plus a plus de la chance d'être sélectionné. Il est très difficile aussi de rencontrer des problèmes de fourches (expliquer en haut) ou d'attaque à double dépense dans le PoS.

Dans le tableau2 ci-dessous nous allons faire une comparaison entre les consensus basés sur le vote et ceux basés sur la preuve, en s'accentuant sur des critères comme la décentralisation, les protocoles d'accord, l'anonymat, la sécurité des algorithmes et les récompenses, etc.

Critères	Consensus basé sur le vote	Consensus basé sur la preuve
Protocoles d'accord	**Sur décision de la majorité des nœuds**	**Par concurrence, les nœuds font leur preuve**
Liberté des nœuds à joindre le réseau de vérification.	**Non on choisit les vérificateurs**	**Pour la plupart**
Nombre de nœuds qui s'exécute dans le réseau	**Limité**	**Illimité**
Décentralisation	**Un peu faible**	**Généralement élevé**
Anonymat	**Oui**	**Non**
Menace pour la sécurité	**Moins sérieux**	**Plus sérieux**
Récompense	**Pas de récompense**	**Oui**

Tableau 3:comparaison entre le consensus basé sur le vote et le consensus basé sur la preuve.

L'analyse du tableau 3 ci-dessus, montre pourquoi les mineurs sont plus intéressés par les consensus par preuve plutôt que ceux par vote parce que tout simplement l'un les récompense et l'autre non. Mais les consensus par vote respectent plus que l'autre (par preuve) l'anonymat des nœuds, et ont un niveau de sécurité supérieur aux consensus par preuve. Ces derniers sont beaucoup plus décentralisés, de surcroit y'a un nombre illimité de nœuds pouvant s'exécutant dans son réseau et sont libres aussi de participer au minage.

Nous allons dresser un tableau récapitulatif de plusieurs algorithmes de consensus, on va se focaliser principalement sur leurs avantages, limites et les blockchains qui les utilisent.

Consensus	Avantages	Limites	Blockchains
PoW	Sécurise le réseau efficacement en rendant les tentatives de piratage difficile.	Lent et consomme beaucoup d'énergie.	Bitcoin, Ethereum, Litecoin, Dogecoin, etc.
PoS	Faible consommation d'énergie et forte résistance aux attaques des 51%.	Le problème du rien en jeu	Peercoin, Nxt, Ethereum (bientôt)
PBFT	Rapide et évolutif.	Centralisé et autorisé.	Hyperleger Fabric.

Tableau 4:Tableau récapitulatif de quelques algorithmes de consensus.

Consensus	Avantages	Limites	Blockchains
DBFT	Rapide et évolutif.	Il peut y avoir plusieurs chaines racines.	NEO
DPoS	Faible consommation d'énergie et Rapide.	Un peu centralisé.	BitShares, EOS Steemit, etc.
PoActivity	Sécurise efficacement le réseau.	Consomme beaucoup d'énergies.	Decred, Espers.
PoAutority	Faible consommation Rapide.	Un peu centralisé.	POA.Network, VeChain.
PoC	Utilise de l'espace. Détection de logiciels malveillants.	L'incitation peut être un problème	Burstcoin, Chia SpaceMint.
PoB	Ne consomme ni de ressources ni d'énergies.	Fort investissement	Slimcoin, TGCoin.
Raft	Implémentation disponible dans de nombreuses langues.	Utilisé que dans les réseaux privés et autorisés.	Quorum.
PoWeight	Faible consommation mais aussi personnalisable et évolutif.	L'incitation peut être difficile.	Algorand.
Quorum Slice	Contrôle, décentralisé Faible latence Flexible	Parfois mauvais comportement des nœuds arrêtant la progression du réseau	Stellar.
PoET	Faible coût de participation. Il est simple pour tous les participants de vérifier que le leader a été légitimement sélectionné.	Nécessite un matériel spécialisé. Ne convient pas aux Blockchains publiques.	Hyperledger Sawtooth.
PoI	Rapide et économe en énergie.	Tout le monde n'est pas éligible au minage.	NEM.

Tableau 5:Tableau récapitulatif de quelques algorithmes de consensus suite.

Consensus	Avantages	Limites	Blockchains
Fédéré	Faible coût de transaction Très rapide Réseau évolutif.	Si le générateur de bloc ne fonctionne pas, le réseau est interrompu.	Chian.
Ripple	Peu coûteux Rapide.	Centralisé mais aussi pas de récompense.	Ripple.

Tableau 6:Tableau récapitulatif de quelques algorithmes de consensus fin.

L'analyse du tableau3 nous permet de voir clairement que les avantages et limites de la majorité des algorithmes de consensus dépendent généralement de leurs fortes ou faibles consommations d'énergies, ou de leurs natures décentralisées ou centralisées. Cependant y'en ont qui ont des avantages et limites qui leurs sont spécifiques. Parmi ces avantages y'a la rapidité des algorithmes et leurs natures évolutives.

2.5 . Conclusion

En somme cette étude nous a permis de savoir l'importance des algorithmes de consensus dans le maintien et le bon fonctionnement des réseaux blockchains. On a pu constater aussi leurs diversités, leurs niveaux de sécurité, leurs temps et vitesses d'exécution, y'a aussi beaucoup de limites dues principalement à la forte consommation d'énergie de certains consensus. Ces limites montrent que la technologie blockchain n'est pas infaillible, de ce fait nous allons dans le prochain chapitre essayer de combiner la blockchain avec d'autres technologies innovatrices comme L'intelligence artificielle (IA), l'internet des objets (IdO) et les mégadonnées (Big Data), pour remédier à certaines limites.

Chapitre 3 : La Blockchain dans la révolution IOT/Big data /IA

3 . Introduction

Bien qu'elle soit une technologie novatrice et très prometteuse, La blockchain n'est pas infaillible comme énumérer précédemment. Sur ce les experts ont pensé à le combiner à d'autres technologies pionnières comme l'intelligence artificielle, le big data, l'internet of thing (IOT) ou internet des objets en français etc., afin d'obtenir la quintessence de ces différentes technologies. En effet de meilleures applications plus sécurisées, ont été conçu à travers leurs combinaisons. Dans ce chapitre nous allons en premier temps parler des notions de l'internet des objets, de l'intelligence artificielle et du big data. Ensuite parler des relations entre la blockchain et ces technologies, les projets existants. Pour finir nous allons essayer en guise de contribution, proposer une architecture décentralisée, reliant ces quatre (4) technologies au service de la santé.

3.1 . La notion d'internet of thing (IOT)

L'évolution de l'internet peut être classée en cinq époques [81] [82]:

- L'internet des documents : bibliothèque électronique, pages web basées sur les documents, etc. ;
- L'internet du commerce : sites web de commerce électronique, de banques en ligne et de négociation d'actions, etc. ;
- L'internet des applications : le web 2.0 ;
- L'internet des personnes : les réseaux sociaux ;
- L'internet des objets : appareils et machines connectés.

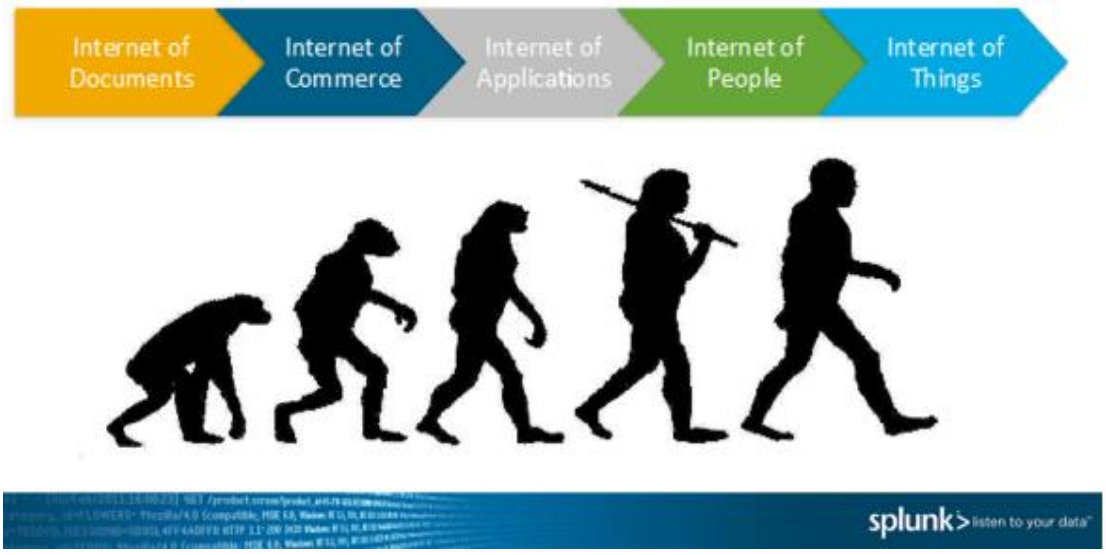


Figure 23: L'évolution de l'internet [81].

L'expression Internet des Objets, fait référence à la connexion de divers appareils et objets physiques à travers le monde via internet. Elle a été initialement utilisée par Kevin Ashton en 1999, et s'est largement répandue grâce aux travaux d'un groupe de chercheurs, travaillant dans le domaine de l'identification par radiofréquence en réseau et la détection d'autres technologies émergentes. L'idée de base de l'internet des objets est de permettre l'échange autonome d'informations utiles entre différents dispositifs du monde réel, identifiable de manière invisible, alimentés par des technologies de pointes, détectés par des dispositifs de détection et traités ultérieurement par la prise de décision, sur la base duquel une action automatisée est effectuée. La détection et le contrôle des objets à travers des infrastructures de réseau, permet de créer des opportunités pour une intégration plus directe du monde physique dans le système informatique, et résultant en une efficacité et une précision améliorée.

L'IOT peut être divisé en six couches :

- La couche codage : dans cette couche, chaque objet se voit attribuer un id unique qui permet de discerner facilement les objets ;
- La couche de perception : cette couche rassemble les informations utiles des objets à partir des dispositifs de détection qui leurs sont liés et convertit les informations en signaux numériques ;
- La couche réseau : le but de cette couche est de recevoir les informations utiles de la couche de perception et de les transmettre aux systèmes de traitement dans la couche intermédiaire via Wifi, Bluetooth, etc., avec des protocoles tels que IPV6, IPV4 etc. ;
- La couche intermédiaire : cette couche est chargée de traiter les informations reçues des dispositifs de détection (capteurs) ;
- La couche application : elle permet de réaliser les applications de l'IOT pour tous les types d'industries, sur la base des données traitées. Les applications liées à l'IOT sont généralement des maisons intelligentes, des transports intelligents, une planète intelligente, etc. ;
- La couche métier : cette couche gère les applications et les services de l'IOT. Elle génère différents modèles commerciaux pour des stratégies commerciales efficaces.

L'intégration de différentes technologies peut permettre d'identifier et de faire communiquer les objets entre eux. Cela peut aider aussi au développement à grande échelle de l'IOT. Parmi ces technologies on peut citer :

- L'identification radiofréquence (RFID) :

  La RFID est la technologie clé pour rendre les objets identifiables de manière unique. Il s'agit d'une micro puce émettrice-réceptrice similaire à un autocollant adhésif qui peut être à la fois active et passive selon le type d'application. Le système RFID est composé de lecteurs et d'étiquette RFID associées qui émettent l'identification, la localisation ou toute autre spécificité de l'objet, les quelles sont déclenchés par la génération de tout signal approprié. Les fréquences RFID sont divisées en quatre gammes de fréquences différentes :

  - ✓ Basse fréquence (135 KHz ou moins).
  - ✓ Haute fréquence (13,56 MHz).
  - ✓ Ultra haute fréquence (862 MHz – 928 MHz).
  - ✓ Fréquence micro-onde (2.4 GHz – 5,80 GHz).

- Le réseau de capteurs sans fil :

  C'est un réseau bidirectionnel de capteurs connectés sans fil dans un mode multi-sauts construit à partir de plusieurs nœuds dispersés dans un champ de capteurs où chacun est connecté à un ou plusieurs capteurs, pouvant collecter des données spécifiques à l'objet telles que la température, l'humidité, la vitesse, etc., puis les transmettre à l'équipement de traitement. Les nœuds de détections communiquent en plusieurs sauts, chaque capteur est un émetteur-récepteur ayant une antenne, un microcontrôleur et un circuit d'interface pour les capteurs en tant qu'unité de communication, d'actionnement et de détection, respectivement avec une source d'alimentation qui peut être à la fois une batterie ou tout autre technologie de récupération d'énergie.

- Le cloud computing :

  Avec des millions d'appareils connectés, le cloud semble être la seule technologie capable d'analyser et de stocker toutes les données efficacement. Le cloud computing est la partie la plus importante de l'IOT, qui non seulement fait converger les serveurs mais traite également sur une puissance de traitement accrue et analyse les informations utiles obtenues à partir des capteurs et fournit une bonne capacité de stockage. Le cloud associé avec des objets intelligents peut aider l'IOT pour un développement à très grande échelle.

- La technologie de mise en réseau :

Cette technologie joue un rôle très important dans le succès de l'IOT puisqu'elle est responsable de la connexion entre les objets, donc on doit avoir un réseau simple et efficace pour gérer un grand nombre d'appareils potentiels. Suivant la portée de la transmission on peut utiliser la 3G, la 4G, un système sans fil ultra rapide et ultra efficace, Wifi, Bluetooth, etc.

- Les nanotechnologies :

  Cette technologie réalise une version plus petite et améliorée des choses qui sont interconnectées. Ça peut permettre de diminuer à l'échelle du nanomètre, la consommation d'un système en développant des appareils.

- Les technologies microsystèmes électromécaniques :

  Les microsystèmes électromécaniques sont une combinaison de composants électriques et mécaniques travaillant ensemble pour fournir plusieurs applications, y compris la détection et l'actionnement qui sont déjà utilisés commercialement dans de nombreux domaines sous la forme de transmetteur et d'accélérateurs, etc. Les microsystèmes électroniques combinés aux nanotechnologies, peuvent donner une solution rentable pour improviser sur le système de communication de l'IOT, mais aussi réduire la taille des capteurs et actionneurs.

- Les technologies optiques :

  Le développement rapide des technologies optiques sous la forme de technologies comme Li-Fi et la technologie optique BiDi de Cisco pourrait être une percée majeure dans le développement de l'IOT. Li-Fi est une technologie révolutionnaire de communication par la lumière visible. Elle fournit une grande connectivité sur une bande passante plus élevée pour les objets interconnectés sur le concept de l'IOT. De même la technologie optique bidirectionnelle (BiDi) donne un Ethernet de 40G pour un big data à partir de plusieurs appareils de l'IOT [83], [84], [85].

3.2 . La notion d'intelligence artificielle (IA)

Le terme IA a été défini pour la première fois en 1956 lors de la conférence de Dartmouth, par un groupe d'informaticiens. C'est eux qui ont fourni la genèse du domaine. Cependant depuis 2010, la discipline connait toute fois un nouvel essor, grâce notamment à l'émergence du cloud computing et du big data, par leur puissance de calcul peu coûteuse et de l'accessibilité à un grand nombre de données. De ce fait les machines ne sont plus programmées ; elles apprennent. Avec une large variété d'application d'IA, nous sommes définitivement à l'aube d'un monde automatisé, alimenté par l'interconnexion machine-machine ou machine-économie [86].

3.3 . Les domaines d'applications de l'IA

Les principaux objectifs de la recherche en IA sont axés sur le raisonnement, l'apprentissage, la capacité de déplacer et de manipuler des objets, etc. Nous allons ci-dessous énumérer quelques domaines d'application de l'IA :

- Les systèmes experts : Ce sont des logiciels capables de simuler le comportement d'un humain effectuant une tache très précise. C'est un domaine où l'intelligence artificielle est incontestablement un succès ;
- Le calcul formel : C'est un domaine permettant de traiter les expressions symboliques ;
- La représentation des connaissances : C'est l'un des secteurs de recherche en intelligence artificielle qui est le plus important ;
- Simulation du raisonnement : Tenter de mettre au point des logiques qui formalisent le mode de raisonnement ;
- Traitement du langage naturel : C'est la compréhension qui reste le problème majeur à la traduction ou au résumé d'un texte dans une autre langue. De grands progrès ont été fait pour obtenir une représentation sous une langue indépendante dans laquelle l'original est écrit ;
- L'apprentissage : Un logiciel devrait avoir des capacités d'apprentissages autonomes pour pouvoir être véritablement qualifié d'intelligent ;
- Réseaux neuronaux : Un réseau de neurones formels est un modèle rudimentaire du cerveau humain. Une cellule neuronale possède une sorte et des entrées reliées à d'autres neurones ;
- La robotique : C'est un domaine qui est fortement répandu dans les usines. La première génération est capable d'exécuter une série de mouvements préenregistrés, la deuxième génération est dotée de capteurs de perceptions permettant de prendre certaines décisions et la troisième possède une plus grande autonomie, elle peut se déplacer dans un environnement ;
- Reconnaissance des visages : Elle est considérée comme l'un des problèmes de l'intelligence artificielle le plus difficile mais les résultats récents deviennent intéressants avec les réseaux neuronaux ;
- Reconnaissance de la parole : Beaucoup de progrès ont été effectués. Y'a un logiciel comme Naturaly Speaking permettant la dictée. Cependant, la compréhension d'un mot ou d'une phrase requiert une grande quantité d'information extra langagières [87], [88].

3.4 . La notion de Big Data

Bien que le concept de Big Data soit relativement nouveau, les grands ensembles de données remontent aux années 60 et 70, lorsque le monde des données commençait à peine à démarrer avec les premiers datacenters et le développement de la base de données relationnelle. En 2005, on assista à une prise de conscience de la quantité de données que les utilisateurs généraient sur

Facebook, YouTube et autres services en ligne. Hadoop (une infrastructure open source créée spécifiquement pour stocker et analyser les jeux de Big Data) fut développé cette même année. Littéralement ces termes (big data) signifient mégadonnées, grosses données ou encore données massives. Ils désignent un ensemble très volumineux de données qu'aucun outil classique de gestion de base de données ou de gestion de l'information ne peut vraiment travailler [89], [90].

Les mégadonnées sont généralement caractérisées par les « 5 V » c'est-à-dire le volume, la vitesse ou vélocité, la variété, la véracité et la valeur comme l'illustre la figure ci-dessous.

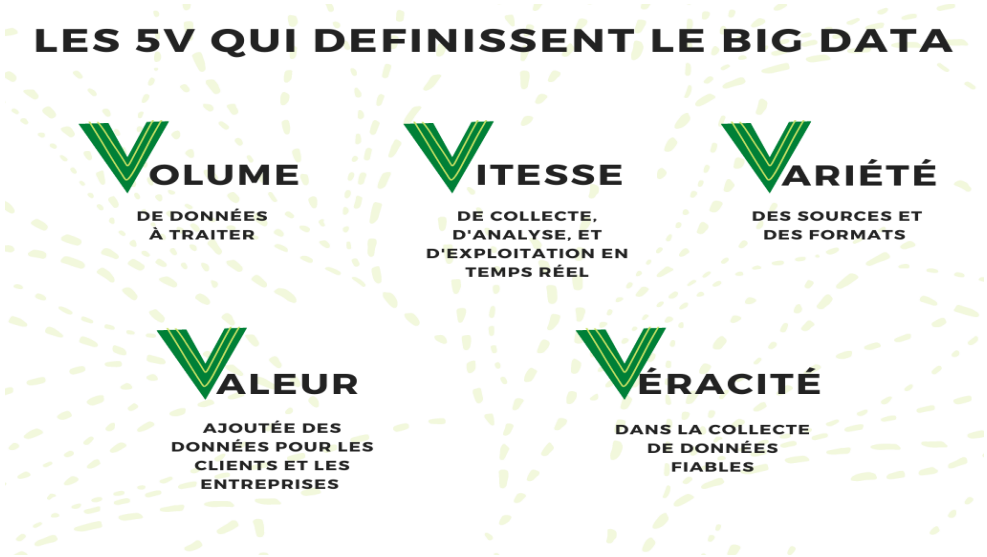


Figure 24:Les 5 V du big data [91].

3.4.1 . Le volume

Le volume définit tout simplement la quantité de données considérée comme du big data. Le traitement des mégadonnées est généralement confronté à plusieurs défis comme la malédiction de la modularité (indisponibilité de stocker/charger les données complètes dans une mémoire ou un disque), la malédiction du déséquilibre des classes (l'existence de différentes distributions de données), la malédiction de la dimensionnalité (les données diversifiées par leurs caractéristiques et attributs).

3.4.2 . La vélocité

Elle fait référence à la vitesse de génération des données suite à une demande. Cette caractéristique peut également être considéré comme une variabilité, c'est-à-dire que différentes applications peuvent avoir différents débits de flux de données. Par exemple, un système détection de foule pour véhicules, peut générer plus de données aux heures de pointes en raison de la participation d'un grand nombre de véhicules sur la route.

3.4.3 . La variété

Elle représente divers types de données telles que les vidéos, les textes et les audios. Ces données sont caractérisées de structurées, semi-structurées et non structurées. Les défis de la variété sont généralement, la localité des données (la répartition des données dans plusieurs emplacements physiques), l'hétérogénéité des données (la diversité des sources de données hétérogènes, ayant différents types de formats, modèles, et sémantiques), les données sales et bruyantes (la contenance de bruits et de la saleté, causé par les méthodes de collectes de données).

3.4.4 . La véracité

Elle fait référence à la qualité des données, puisque ces dernières peuvent être collectées à travers diverses sources, qui peuvent inclure des échantillons de mauvaises qualités et bruyants. Pour améliorer la qualité et la précision analytique des mégadonnées, les défis de la provenance des données, de l'incertitude des données sales et bruyantes doivent être efficacement relevés.

3.4.5 . La valeur

Sûrement le point le plus important des 5 V ! Les technologies de stockage et d'analyse des Big Data n'ont de sens que si elles apportent de la valeur ajoutée. Exploiter les données, c'est avant tout répondre des objectifs commerciaux ou Marketing. La définition des objectifs orientera l'utilisation des Big Data [92], [93].

3.5 . La relation Blockchain-Internet des objets

Le manque de confiance au niveau de l'internet des objets, la non transparence des données, des participants qui n'ont pas une vision claire de l'endroit et de la manière dont les informations qu'ils fournissent seront utilisées, poussent les experts à penser à le combiner avec la technologie blockchain pour que cette dernière puisse offrir un service de partage de confiance fiable et traçable.

3.5.1 . L'architecture en couches basée sur la blockchain pour l'IOT :

Cette architecture est composée de trois (3) couches : une couche de données, une couche blockchain et couche une couche application.

- **La couche de données**

  Cette couche est composée d'une variété d'appareils IOT, y compris des capteurs, des étiquettes d'identification par radiofréquence (RFID), des appareils de communication en

champs proche (NFC) et des téléphones mobiles. Ces appareils permettent de collecter des données d'observations, qui sont hachées et peuvent être stockées hors chaine.

- **La couche blockchain**

  Cette couche reçoit les transactions de la couche de données et gère le maintien du réseau blockchain tout en ayant des interactions bidirectionnelles avec la couche application.

- **La couche application**

  Elle est responsable du traitement des données et de la fourniture de services aux utilisateurs finaux. Cette couche communique aussi avec celle de la blockchain pour s'adapter aux mécanismes de consensus de la blockchain [94], [95].

3.5.2 . Les services de la blockchain pour l'IOT

- La blockchain peut résoudre les problèmes de confidentialité et de fiabilité de l'internet des objets. Elle peut être utilisée pour suivre des milliards d'appareils connectés, permettant le traitement des transactions et la coordination entre les appareils. Cette approche décentralisée éliminerait les points de défaillances uniques, créant ainsi un écosystème plus résilient sur lequel les appareils peuvent fonctionner.
- Dans un réseau IOT, la blockchain peut conserver un enregistrement immuable de l'historique des appareils intelligents. En effet ces derniers peuvent fonctionner de manière autonome, sans avoir besoin d'une autorité centralisée.
- La blockchain peut traiter les échanges de messages entre les appareils d'un réseau IOT, comme les transactions financières. Pour permettre les échanges de messages, les appareils s'appuieront sur des contrats intelligents, qui modéliseront ensuite l'accords entre les deux parties.
- La blockchain a la capacité de maintenir un registre dûment décentralisé et fiable de toutes les transactions effectuées dans un réseau. Cette capacité est essentielle pour les nombreuses conformités et exigences réglementaires des appareils IOT industrielles sans avoir besoin de s'appuyer sur un modèle centralisé [96].

3.5.3 . Les applications IOT basées sur la blockchain

La combinaison IOT-Blockchain, a permis la mise en place de nombreuses applications dans différents domaines (santé, finance, vie sociale, etc.). Ci-dessous nous allons essayer d'énumérer et expliquer quelques applications IOT basées sur la blockchain :

- **Les soins de santé intelligents**

  Grace à l'IOT et ses capteurs, on peut collecter des données à partir du corps des patients avant de le transmettre aux médecins pour des diagnostics. Les prestataires de soins de santé sont susceptibles d'utiliser la blockchain pour stocker en toute sécurité les dossiers médicaux de leurs patients. Ces données médicales sensibles peuvent être encodés et conservés dans la blockchain avec un mot de passe ;

- **Les réseaux et services publics intelligents**

  C'est un réseau interconnecté de centrales électriques et de consommateurs : produire de l'électricité en fonction de la demande des utilisateurs. La blockchain offre avec son système décentralisé une confiance accrue, la transparence, l'efficacité, etc., grâce à la cryptographie, au processus de consensus, garanti aussi l'immuabilité des données. Ce qui permet d'avoir une clarté sur les prix en termes de production et consommation d'énergie électrique ;

- **Les villes intelligentes**

  C'est un réseau urbain intelligent, interconnecté pour la production des données à partir des capteurs. Ces données seront toutes dans la blockchain afin d'apporter une protection sur la vie privée des gens. L'utilisation de la blockchain pour un nouveau système de vote dans les villes intelligentes, éradiquant la fraude électorale ;

- **Les finances intelligentes**

  L'interconnexion étendue des réseaux IOT, introduisent des niveaux de serveurs financiers avec des mesures de performances. La blockchain peut faire gagner du temps et des ressources, en simplifiant le monde dynamique de la finance. L'utilisation des contrats intelligents peut conduire à de nouveaux types de services financiers [97] [98].

3.6 . La relation Blockchain-IA

Malgré qu'elle soit puissante, la blockchain souffre des faiblesses telles que la sécurité, l'évolutivité, et l'efficacité ; Et l'intelligence artificielle à sa juste part des problèmes de fiabilité, d'explicabilité et de confidentialité. Puisque toutes les données sur la blockchain sont publiquement disponibles, l'intelligence artificielle est la clé pour fournir aux utilisateurs la confidentialité et la vie privée. En effet l'union de ces deux technologies semble inévitable ; ils pourront se compléter pour révolutionner la prochaine génération de technologie.

3.6.1 . L'apport de l'IA pour la blockchain

L'utilisation de l'intelligence artificielle peut permettre de remédier à certaines limites de la blockchain. Ci-dessous nous allons essayer d'en énumérer quelques-unes :

- **La forte consommation d'énergie**

  Dans certaines blockchains, l'exploitation minière nécessite beaucoup d'énergie et de ressources, et l'intelligence artificielle s'est avérée très efficace dans l'optimisation de la consommation d'énergie. En effet la combinaison IA-Blockchain peut entrainer une baisse des investissements dans le matériel minier ;

- **L'évolutivité**

  La blockchain croît à un rythme constant (un bloc tous les 10 minutes), par exemple bitcoin a une taille de plus de 220 Go. Même Ethereum a introduit un concept appelé « l'élagage » permettant de supprimer les données inutile, la taille reste toujours importante. L'autre solution c'est de faire appel à l'intelligence artificielle car cette dernière peut introduire de nouveaux systèmes d'apprentissage fédéré ou nouvelles techniques de partage de données pour rendre le système plus efficace ;

- **La sécurité :**

  Bien vrai que le réseau blockchain est presque infaillible, ses applications comme la finance décentralisée, sont trop sensibles aux attaques des hackeurs. Les progrès incroyables de la machine learning au cours des deux dernières années font de l'intelligence artificielle une alliée fantastique de la blockchain pour garantir un déploiement sécurisé des applications ;

- **L'efficacité :**

  Deloitte (2016) a estimé les coûts de fonctionnement totaux associés à la validation et au partage des transactions sur la blockchain à 600 millions de dollars par an. Un système intelligent pourrait éventuellement être en mesure de calculer à la volée la probabilité que des nœuds spécifiques soient les premiers à effectuer une certaine tâche, en donnant la possibilité à d'autres mineurs d'arrêter leurs efforts pour cette transaction spécifique et de réduire les coûts totaux. De plus, même si certaines contraintes structurelles sont présentes, une meilleure efficacité et une consommation énergétique moindre peuvent réduire la latence du réseau permettant ainsi des transactions plus rapides ;

- **Les matériels spécifiques**

  Les mineurs (et pas nécessairement les entreprises mais aussi les particuliers) ont investi une somme incroyable dans des composants matériels spécialisés. Puisque la consommation d'énergie a toujours été un problème clé, de nombreuses solutions ont été proposées et bien d'autres seront introduites à l'avenir. Dès que le système devient plus efficace, certains éléments matériels peuvent être convertis (parfois partiellement) pour l'utilisation de réseaux neuronaux (le colosse minier Bitmain fait exactement cela) ;

- **Le manque de talent**

  C'est un acte de foi, mais de la même manière, on peut essayer d'automatiser la science des données elle-même (sans succès actuellement), pourquoi ne pas créer des agents virtuels capables de créer eux-mêmes de nouveaux registres (et même d'interagir dessus et de les maintenir) ;

- **Le portail des données**

  Dans un futur où toutes nos données seront disponibles sur une blockchain et les entreprises pourront les acheter directement, on aura besoin d'aide pour accorder l'accès, suivre l'utilisation des données et, en général, comprendre ce qu'il advient des informations personnelles à la vitesse d'un ordinateur. C'est un travail pour les machines (intelligentes) [99], [100].

3.6.2 . L'apport de la Blockchain pour l'IA

La blockchain peut alimenter des marchés décentralisés et des plateformes de coordination pour divers composants de l'intelligence artificielle, y compris les données, les algorithmes et la puissance de calcul. Elle aidera également les décisions de l'intelligence artificielle à être plus transparentes, explicables et digne de confiance. Ci-dessous nous allons énumérer quelques points qui peuvent permettre à l'évolution de l'intelligence artificielle à travers la blockchain :

- **Aider l'IA à s'expliquer**

La boite noire de l'intelligence artificielle n'est pas assez explicite, avoir une piste d'audit claire peut non seulement améliorer la fiabilité des données ainsi que des modèles, mais aussi un itinéraire clair pour retracer le processus de décision de la machine ;

- **Augmenter l'efficacité de l'IA**

Si le partage des données est sécurisé, non seulement il y'aura plus de données, mais aussi de meilleurs modèles, de meilleures actions, de meilleurs résultats et cela impactera positivement les données futures. L'effet du réseau est tout ce qui compte en fin de compte ;

❖ **La réduction des risques catastrophiques**

Une intelligence artificielle codée dans une DAO (Organisation Autonome Décentralisée) avec des contrats intelligents spécifiques, aura l'obligation de respecter les termes du contrat, de ce fait son espace d'action sera limité ;

❖ **Abaisser les barrières du marché à l'entrée**

Premièrement la blockchain peut favoriser la création de données personnelles plus propres et mieux organisées. Deuxièmement, il permettra l'émergence de nouvelles places de marché : une place de marché de la donnée (fruit à portée de main) ; une place de marché de modèles (beaucoup plus intéressante) ; et enfin même un marché de l'IA (voir ce que Ben Goertzel essaie de faire avec SingularityNET). Par conséquent, un partage facile des données et de nouveaux marchés, conjointement avec la vérification des données de la blockchain, offriront une intégration plus fluide qui abaissera la barrière à l'entrée pour les petits acteurs et rétrécira l'avantage concurrentiel des géants de la technologie. Dans l'effort d'abaisser les barrières à l'entrée, nous résolvons alors en fait deux problèmes, à savoir fournir un accès aux données plus large et un mécanisme de monétisation des données plus efficace ;

❖ **Augmenter la confiance artificielle**

Dès qu'une partie de nos tâches sera gérée par des agents virtuels autonomes, avoir une piste d'audit claire aidera les robots à se faire confiance (et à nous à leur faire confiance). Il augmentera également à terme chaque interaction machine à machine et chaque transaction, offrant un moyen sécurisé de partager des données et de coordonner des décisions, ainsi qu'un mécanisme robuste pour atteindre un quorum (extrêmement pertinent pour la robotique en essaim et les scénarios à agents multiples). Rob May a exprimé un concept similaire dans l'une de ses dernières newsletters [101], [102].

3.6.3 . Les exemples de projets Blockchain-IA

Ils ne sont pas si nombreux que ça mais on peut les catégoriser comme suit :

- **L'intelligence décentralisée** : Dans cette catégorie on note l'existence de différents projets comme la **TraneAi** qui est une formation de l'IA de manière décentralisée, y'a aussi **Neureal** qui est un supercalculateur d'IA pair à pair, **AI Blockchain** qui est une intelligence multi-applications, **AtMatrix** qui sont des robots décentralisés et Effect.ai qui un marché décentralisé de la main d'œuvre et des services de l'IA, etc. ;
- **Les plateformes de conversation :** Ici on peut noter le **Green Running** qui est assistant virtuel d'énergie domestique et le **doc.ai** qui sont des analyses quantifiées de la biologie et des soins de santé, etc. ;

- **Les plateformes de prédictions :** Y'a Augur qui une plateforme d'intelligence collective et Sharp Capital qui est une plateforme de prédictions de sentiments crowdsource, etc. ;
- **La propriété intellectuelle :** Y'a Loci.io qui permet de faire des découvertes et d'exploitation d'IP. ;
- **La provenance des données :** Y'a **KapeIQ** qui permet de détecter des fraudes sur les entités de santé, **Data Quarka** qui est un vérificateur des faits et **Priops** qui permet de vérifier la conformité des données, etc. ;
- **Trading :** Dans le domaine de la trading y'a l'application **Eukild** qui permet de faire des investissements en bitcoin et **EthVentures** qui permet des investissements en tokens numériques ;
- **Assurance :** On note l'existence de **Mutual.life** qui est une assurance paire à paire ;
- **Autres :** Dans cette catégorie on a le **Social Coin** qui sont des systèmes de récompenses des citoyens, **HealthyTail** qui est un projet permettant d'analyser les animaux de compagnie, y'a aussi **Crowdz** pour le commerce électronique, **Deepsee** qui est une plateforme multimédia et **ChainMind** pour la cybersécurité [103]**,** [104]**.**

3.7 . La relation Blockchain-Big Data

Les gouvernements et les organisations privées investissent massivement dans la technologie big data et la blockchain en raison de leur grand potentiel pour résoudre de nombreux problèmes du monde réel. De nos jours les clients sont plus enclins à effectuer les transactions en ligne et une quantité croissante de données est générée. Cependant, la croissance phénoménale des mégadonnées a présenté ses propres défis. Certains des principaux défis des mégadonnées sont les problèmes de sécurité, de confidentialité et de partage des données, etc. Ces défis auxquels sont confrontés, le big data peuvent être résolu par les propriétés uniques de la blockchain comme la décentralisation, l'immuabilité, la transparence et les mécanismes de consensus.

3.7.1 . L'apport de la Blockchain pour le Big Data

La blockchain peut aider la technologie des big data, à s'améliorer sur différents points, et ainsi participer à son évolution. Ci-dessous, on va essayer de lister mais aussi d'expliquer l'apport de la blockchain sur les mégadonnées.

❖ **L'amélioration de la sécurité et de la confidentialité des mégadonnées**

La fréquence élevée d'appareils connectés à internet, fait augmenter la quantité de données stockée dans les emplacements tiers comme le cloud. Ainsi cela peut amener de nouveaux défis comme la violation de données ou les menaces causés par les tiers curieux. Cependant

l'usage de la blockchain pour stocker les mégadonnées, a le potentiel de résoudre ce problème. Le stockage crypté et décentralisé des données dans le réseau blockchain rend très difficile tout accès non autorisé aux données.

- **L'amélioration de l'intégrité des données**

  Il se peut que des personnes malintentionnées falsifient les enregistrements des big data pour influencer la prédiction de l'analyse des mégadonnées en leur faveur. La propriété d'immuabilité de la blockchain garantit pratiquement l'impossibilité de falsifier les données stockées dans le réseau blockchain. Pour modifier les données dans un réseau blockchain, l'attaquant doit modifier les données dans au moins 50% des nœuds du réseau ce qui est quasi impossible. De surcroit l'immuabilité de la blockchain garantit la fiabilité des données stockées sur le réseau blockchain.

- **La prévention aux fraudes**

  Les solutions big data existantes reposent sur l'analyse de modèles dans les données historiques pour détecter les transactions frauduleuses. Par conséquent les mégadonnées ne peuvent pas résoudre le problème des transactions illicites dans le secteur financier. Ainsi le stockage des big data dans la blockchain permet aux institutions financières de surveiller chaque transaction en temps réel, leur permettant ainsi de détecter les transactions potentiellement malhonnêtes.

- **L'amélioration du partage des données**

  L'intégration de la blockchain avec les mégadonnées aide les fournisseurs de services à partager les données avec d'autres parties prenantes avec un risque minimal de fuite de données.

- **L'amélioration de la qualité des mégadonnées**

  Les scientifiques des données passent la plupart de leur temps sur l'intégration des données car différentes sources suivent des formats différents dans la collecte de données. En utilisant la blockchain pour le stockage des données, la qualité de celles-ci peut être amélioré car elles sont structurées et complète [105], [106], [107].

3.7.2 . L'apport du Big Data sur la blockchain

Les blockchains et les contrats intelligents ne peuvent pas accéder aux données situées en dehors du réseau. Cependant pour de nombreux accords contractuels, il est vital de disposer d'informations pertinentes provenant du monde extérieur afin d'exécuter l'accord. Les mégadonnées servent de ponts entre les blockchains et le monde extérieur. Ci-dessous nous

allons énumérer quelques solutions que les différents types de données peuvent apporter à la blockchain :

- **Les données logicielles**

  Elles entrent en contact avec des sources d'informations en ligne et les transmettent à la blockchain. Ces informations peuvent provenir des bases de données en ligne, des serveurs, des sites web…etc. Le fait qu'elles soient connectées à internet leurs permettent non seulement de fournir des informations aux smart contracts, mais aussi de transmettre ces informations à temps réel.

- **Les données matérielles**

  Certains contrats intelligents ont besoins d'une interface avec le monde réel. Les données matérielles sont conçues pour obtenir des informations du monde physique et les mettre à la disposition des smart contracts. Ces informations peuvent être relayées par des capteurs électroniques, des scanners de code-barres / QR, des étiquettes RFID, des robots et d'autres dispositifs de lecture d'informations. Une donnée matérielle traduit essentiellement des évènements du monde réel en valeurs numériques qui peuvent être comprise par des contrats intelligents.

- **Les données humaines**

  Parfois des personnes ayant des connaissances /connaissances spécialisées dans un domaine particulier peuvent également servir de source de données. Ils peuvent rechercher et vérifier l'authenticité des informations provenant de diverses sources et traduire ces informations en contrats intelligents. Les données humaines sont non seulement capables de transmettre des données déterministes, mais aussi de répondre à des demandes arbitraires, ce qui pourrait être difficile à faire par une machine.

- **Les données de calculs**

  Elles peuvent être utilisées pour effectuer une solution de calcul arbitraire « hors chaine », une fonction qui peut être particulièrement utile étant donné la limite de gaz de bloc inhérente à Ethereum et le coût de calcul comparativement élevé. Plutôt que de relayer simplement les résultats d'une requête, les données de calculs peuvent être utilisées pour effectuer des calculs sur un ensemble d'entées et de renvoyer un résultat qu'il n'aurait été impossible de calculer sur la chaine.

❖ **Les données entrantes/sortantes**

Les données entrantes transmettent des informations de sources externes aux contrats intelligents, tandis que les données sortantes envoient des informations des contrats intelligents aux mondes extérieurs. Un exemple de donnée entrante est celui qui dit à un contrat intelligent, quelle est la température mesurée par un capteur. Tandis que qu'un exemple de donnée sortante peut être considéré comme une serrure intelligente ; Si des fonds sont déposés à une adresse, le contrat intelligent envoie cette information via un système de gestion de données sortantes à un mécanisme qui déverrouille la serrure intelligente.

❖ **Les données spécifiques aux contrats**

Les données spécifiques à un contrat intelligent sont conçues pour être utilisés par un seul contrat intelligent. Cela signifie que si l'on veut déployer plusieurs contrats intelligents, il faut développer un nombre proportionnel de données spécifique aux contrats. Ce type de données est considéré comme très chronophages et coûteux à maintenir. Les entreprises qui veulent extraire des données de diverses sources peuvent trouver cette approche très peu pratique. En revanche, étant donné que les données spécifiques aux contrats peuvent être conçues à partir de zéro pour servir un cas d'utilisation spécifique, les développeurs disposent d'une grande flexibilité pour les adapter à des exigences particulières [108].

3.7.3 . Exemple de projets Blockchain-Big Data

Grace à l'association Blockchain-Big Data, plusieurs projets ont vu le jour. Nous allons essayer d'en citer quelques-uns :

❖ **Storj**

C'est un projet de stockage décentralisé de bout en bout qui utilise des matériels excédentaire et une capacité de bande passante permettant l'authentification paire à paire des contrats de stockage entre les fournisseurs et les utilisateurs. Le processus implique le cryptage des fichiers coté client, qui sont divisés en morceaux appelés « shards ». La cryptomonnaie Storj permet aux locataires de vérifier les fichiers des agriculteurs et également de payer la maintenance de ce système de stockage.

❖ **Omnilytics**

C'est une plateforme Blockchain pour l'analyse de données volumineuse qui fournit des informations pour l'industrie de vente, de marketing et du marchandisage. Elle utilise diverses technologies pour intégrer les données de différentes industries. La plateforme fournit des analyses de données et des services connexes afin de comparaitre les concurrents, les tendances

et les prix pour les clients. Y'a l'usage des contrats intelligents pour les échanges de données et d'autres services.

❖ **Rubix**

Elle utilise le concept de décentralisation pour intégrer les traders de cryptomonnaies dans une plateforme de trading commune afin d'authentifier leur crédibilité et leur prédiction. Le protocole est basé sur l'attribut de transparence et d'immuabilité de la Blockchain en combinaison avec l'analyse des données d'investissements pour générer des prévisions de trading plus précises.

❖ **Provenance**

C'est une plateforme Blockchain principalement utilisée dans la gestion de la chaine d'approvisionnement qui permet de collecter des informations importantes sur les produits et de les partager de manière fiable, sécurisée et accessible.

❖ **Datum**

C'est une plateforme décentralisée, distribuée, de haute performance et NOSQL, prise en charge par Ethereum, Bigchain DB et IPFS. Il permet essentiellement aux utilisateurs de stocker des données de manière anonyme et sécurisée à partir des réseaux sociaux, des appareils IOT et des technologies portables.

❖ **Filecoin**

Filecoin a l'intention de créer un réseau de stockage décentralisé qui permettrait aux commerçants d'acheter et de vendre du stockage sur un marché ouvert. Le filecoin permet aux utilisateurs de louer du stockage sur des appareils disposant d'espaces de stockage excédentaires à l'aide de la crypto-monnaie filecoin. Les clients dépensent des crypto-monnaies pour partager ou récupérer les données et les mineurs gagnent les pièces de monnaie grâce au stockage et aux services de données. Lorsque les mineurs exploitent un bloc particulier, ils doivent soumettre une preuve d'espace-temps (PoST) au réseau, qui valide si un fournisseur de stockage s'acquitte des responsabilités requises pour stocker les données externalisées pendant la période stipulée. Le filecoin se compose d'une blockchain, de nœuds de récupération, de nœuds de stockage et d'un jeton filecoin natif. Les nœuds de stockage stockent les copies scellées des données et les transactions sont enregistrées par la blockchain. Les nœuds de récupérations récupèrent et livrent les fichiers aux utilisateurs tout en respectant les Postes [109].

❖ **ASTRAEA**

C'est un oracle décentralisé, basé sur un jeu de vote qui décide de la vérité ou de la fausseté des propositions. Elle commence par un aperçu de haut niveau des rôles des utilisateurs et du fonctionnement du jeu et se termine par une description détaillée du jeu [110].

3.8 . La relation IOT-Big data

Selon plusieurs études, l'utilisation d'IOT devrait générer 4,4 billions de GO en 2020, et ce chiffre devrait augmenter les années suivantes. De plus, ces données doivent être lues, exploitées et retransmises dans des temps impartis, ainsi, comme vous l'aurez deviné, l'enjeu majeur dans le domaine de l'Internet des objets est de pouvoir exploiter un nombre de données gigantesque, d'où l'usage du Big Data. L'IOT et le Big Data sont deux technologies indépendantes mais indissociables l'une de l'autre, pour permettre des avancées technologiques notoires. Si l'IOT permettrait en majeure partie de collecter les données d'objets physiques via différents capteurs, le Big Data lui, permettrait un stockage et un traitement de ces données plus rapide et plus efficace. Grace à l'intégration de ces deux technologies, on peut le big data peut combler certaines lacunes de l'IOT comme le stockage limité et les applications sur internet. De même l'IOT peut aider le big data à résoudre le problème principal de la portée limitée. La question de la sécurité de cette intégration pose un sérieux problème. Lorsque les applications IOT se trouve vers le big data, les inquiétudes surgissent en raison du manque de confiance dans le fournisseur de service ou de la connaissance des accords de niveau de service et de la connaissance de l'emplacement physique des données.

La combinaison entre big data et IOT consiste d'abords à gérer les sources de données de l'IOT, où les dispositifs de capteurs connectés utilisent des applications pour interagir les uns avec les autres. Par exemple, l'interaction d'appareils tels que les caméras de vidéosurveillances, les feux de circulation intelligents et les appareils domestiques intelligents, génère de grande quantité de sources de données avec différents formats. Ces données peuvent être stockées dans un stockage de base à faible coût sur le cloud. Les données générées sont appelées « big data ». Ces énormes quantités de données sont stockées dans des fichiers volumineux de base de données distribuée, partagée et tolérante aux pannes.

L'application des technologies du big data dans l'internet des objets, accélère les avancées de la recherche et les modèles commerciaux de l'IoT [111], [112].

3.8.1 . Les exemples de projets IoT-Big Data

On note l'existence de plusieurs projets d'intégration de l'internet des objets et du big data dans des macrostructures. Ci-dessous nous allons essayer d'en citer quelques-uns [113], [114].

- **Le mobile world congress à Barcelone**

Le Mobile World Congress est le plus grand salon mondial de la téléphonie et de la haute technologie. Il grandit chaque année et se tient à Barcelone, l'une des villes les plus classées d'Europe en tant que ville intelligente**.** La ville dispose de zones Wi-Fi dans toute la ville, la 3G est disponible dans les transports en commun et les places de parking sont mises à jour en temps réel. Des capteurs indiquent la température, le niveau de bruit et la qualité de l'air**.** La ville utilise la plate-forme cloud Azure de Microsoft pour agréger les données. Avec toutes les données générées par les nombreux petits capteurs répartis dans toute la ville**,** Barcelone peut gérer au mieux l'afflux massif de visiteurs. Pendant le salon, une application spéciale développée par l'association GSMA (la plus grande association mondiale de 850 opérateurs) permet aux visiteurs de créer des réseaux**,** de parcourir des programmes et de partager des informations professionnelles.

- **TempuTech**

L'industrie agricole représente une grande partie du Big Data et de l'Internet des objets. TempuTech propose plusieurs systèmes connectés de stockage des données agricoles et de gestion des risques à partir de différents paramètres agricoles. Ces systèmes sont soutenus par une série de petits capteurs qui collectent de grandes quantités de données qui sont ensuite analysées pour soutenir la prise de décision et optimiser l'efficacité des cultures. On peut notamment calculer le débit d'eau nécessaire par parcelle ou la quantité de semence nécessaire.

- **Disneyland**

Le meilleur exemple de cette interaction se trouve dans le parc à thème Disneyland Resort aux États-Unis. La société a investi plus d'un milliard de dollars pour lancer un smart band appelé MagicBand. Un bracelet a gagné les faveurs des voyageurs puisque 90% d'entre eux se disent satisfaits des bienfaits du port de ce bracelet, selon un sondage. Le bracelet permet aux parents de géolocaliser leurs enfants, de payer dans les boutiques et restaurants, ou encore de prendre des photos prises dans les attractions. Disney House collecte ces données et les utilise pour améliorer l'expérience client.

- **British Columbia Hydro**

BC Hydro est une compagnie d'électricité qui distribue de l'électricité à plus de 2 millions de personnes au Canada. En 2011, l'entreprise a mis à niveau tous les compteurs d'électricité de ses clients vers un système plus intelligent que les compteurs existants. Ces compteurs permettent aux utilisateurs de suivre facilement leur consommation d'énergie. Il est même possible de savoir si une alimentation inappropriée a été utilisée en cas de vol de la montre. Le système est basé sur la collecte d'une grande quantité de données de consommation qui peuvent

aider à prévoir la demande d'énergie sur une période de temps et ainsi permettre à l'entreprise de prendre les mesures appropriées.

3.9 . La relation IA-Big Data

Pour mieux comprendre à quel point ces deux technologies sont complémentaires, il faut revenir à la définition de l'IA. Au sens large, l'intelligence artificielle fait référence à toute technique capable de reproduire les capacités analytiques humaines. Pour cela, la machine a besoin d'intégrer une grande quantité de données afin d'apprendre à se modifier et d'intérioriser le modèle algorithmique adapté à la situation qu'elle rencontre. Ce processus d'apprentissage est appelé apprentissage automatique (ML). Les mégadonnées ont un grand impact ici. Plus une machine absorbe une grande quantité de données croisées, plus elle peut améliorer les connaissances et le raisonnement, mimant ainsi la fonction cognitive de l'intelligence humaine. C'est pourquoi le big data et l'IA sont destinés à travailler ensemble de manière inévitable. On parle même de "big data intelligence"[115]. L'intelligence artificielle est utilisée pour faciliter la capture et la structuration des mégadonnées, afin d'obtenir des informations clés. Elle consiste à augmenter les volumes, les vitesses et la variété des données. Dans des situations de gros volume de données, l'intelligence artificielle permet de déléguer la reconnaissance de formes difficiles, l'apprentissage et d'autres taches aux approches informatisées. Par exemple plus de la moitié des transactions boursières dans le monde sont effectuées à l'aide de systèmes basées sur l'IA. De surcroit l'IA contribue à la vélocité des données, en facilitant des décisions informatiques rapides qui mènent à d'autres décisions. Par exemple, étant donné que de nombreuses transactions boursières sont effectuées par de systèmes basés sur l'IA plutôt que des personnes, la vitesse des transactions peut augmenter et une transaction peut en entrainer d'autres. Les problèmes de variété ne sont pas résolus simplement en parallélisant et en distribuant le problème. Au lieu de cela, la variété est atténuée en capturant, structurant et comprenant les données non structurées à l'aide de l'intelligence artificielle et d'autres analyse [116], [117].

3.9.1 . Les exemples de projets IA-Big Data

On note l'existence de plusieurs plateformes d'intégration du big data et de l'intelligence artificielle. Ci-dessous nous allons essayer d'en énumérer quelques-unes.

Il faut noter aussi que les plateformes que nous allons citer, proposent des APIs afin de s'intégrer à d'autres applications informatiques. Ces intégrations permettent par exemple de se connecter à une base de données, d'échanger des données, ou bien encore de synchroniser des

fichiers entre plusieurs programmes informatiques via une extension, un plugin, ou une API (application programming interface / interface de programmation). Elles sont compatibles avec la plupart des systèmes d'informations d'entreprises ainsi qu'avec la plupart des systèmes d'exploitation (OS) comme Windows, Mac OS, et Linux car elles sont accessibles depuis un navigateur web (Chrome, Firefox …) [118], [119], [120].

- **CognitiveScale**

C'est un fournisseur de logiciels d'entreprise cognitive cloud, une nouvelle classe de systèmes d'interprétation Big Data et d'apprentissage automatique. Il est disponible en version d'essai.

- **Infrrd**

Infrrd est un service disponible en version d'essai. Une plate-forme d'IA d'entreprise moins chère, plus légère et plus rapide qui donne un sens aux données d'image, de texte et de comportement pour automatiser la décision de réduction des coûts / main-d'œuvre ou d'augmentation des revenus.

- **AForge.Neuro**

AForge.Neuro est un service disponible en version d'essai. AForge.NET est un Framework C # open source, conçu pour les développeurs et les chercheurs dans les domaines de la vision artificielle et de l'intelligence artificielle, du traitement d'images, etc.

- **BPN-NeuralNetwork**

BPN-NeuralNetwork est un service disponible en version d'essai. BPN-NeuralNetwork est un système d'apprentissage automatique implémentant un réseau de neurones à trois couches et un réseau de neurones à propagation arrière (BPN), la théorie de QuickProp et la théorie de Kecman (EDBD).

- **Brainstrom**

Brainstrom est un service disponible en version d'essai. Brainstorm permet de travailler avec des réseaux de neurones rapide, flexible et amusant, ce qui permet de travailler sur plusieurs plates-formes avec plusieurs serveurs informatiques.

- **Botworx**

Botworx est un service disponible en version d'essai. Botworx est une plate-forme de commerce conversationnel reposant sur l'IA qui aide les marques à acquérir et à dialoguer avec les consommateurs qui utilisent une application de messagerie sociale.

- **AIDA**

AIDA est un service disponible en version d'essai. AIDA est un outil d'intelligence artificielle qui personnalise le contact avec le client, il mappe les utilisateurs et les actions / produits pour mieux impliquer les clients.

3.10 . Motivation de l'intégration des quatre (4) technologies

Les gouvernements et les organisations privées commencent à faire beaucoup d'investissements dans les technologies comme la blockchain, l'intelligence artificielle, le big data et l'internet des objets, afin de résoudre de nombreux problèmes du monde réel.

Aujourd'hui, l'IOT représente plus de 20 milliards d'appareils connectés. Chaque appareil produit et échange des données sur internet. En effet une quantité croissante de données est générée tous les jours. Cette croissance exponentielle des données numériques générées crée de nouvelles opportunités et poussent les chercheurs à essayer de comprendre les besoins des clients. Cette production extensive et continue du Big Data, présente ses propres défis. Certains des principaux défis du big data sont les problèmes de sécurité, de confidentialité et de la fiabilité des sources de données. Ces défis auxquels sont confrontés par le big data peuvent être résolus par les propriétés uniques de la Blockchain comme le stockage décentralisé, l'immuabilité, la transparence et les mécanismes de consensus. L'IA peut analyser les quantités astronomiques de données dans des intervalles de temps restreints. Et cela peut augmenter les performances du traitement de données. L'intelligence artificielle permet aussi une automatisation de la prise de décision sur les données. En effet nous obtiendrons de nouvelles données qualitatives menant à des modèles entièrement nouveaux. L'immuabilité inhérente conduit à une plus grande confiance dans les données de formation, de test et les modèles qu'ils produisent. Ces technologies robustes et très puissantes évoluent dans presque tous les domaines. Cependant elles ne sont pas infaillibles et chacune peut avoir un impact particulier sur l'autre. Lorsqu'elles sont intégrées, cela pourra ouvrir de nouvelles opportunités de recherche pour des applications intelligentes et efficaces, avec un niveau de sécurité très élevés [121] [122].

3.11 . Problématique de recherche

L'IOT, le Big Data, et l'IA ont suscité de vifs intérêts dans divers domaines scientifiques et d'ingénierie au cours des dernières années. Malgré leurs nombreux avantages et applications,

il y'a de nombreux défis à relever pour une meilleure qualité de service, par exemple dans l'analyse, la gestion, la confidentialité et la sécurité des données. La Blockchain, avec sa nature décentralisée et sécurisée a de grand potentiel d'améliorer les services et applications des technologies citées ci-dessous.

Nonobstant nos nombreux efforts de recherche, nous n'avons connaissance d'aucune enquête qui étudie de manière approfondie l'intégration de ces 4 technologies et leurs applications dans un domaine spécifique. Bien que dans l'article [109] les chercheurs ont proposés une architecture reliant ces 4 technologies sans pour autant spécifié le domaine d'application. Cet article examine principalement les services de la blockchain pour le big data. Leur architecture est très bien conçue et suit un processus bien déterminé où l'IOT avec ses appareils connectés se charge de l'acquisition des données, le Big Data collecte et stocke les données, ensuite la Blockchain va se charger de récupérer, d'explorer mais aussi sécuriser les données avant de les passer à l'IA pour des apprentissages et des analyses prédictives. Il faut noter aussi dans leur architecture les données sont spécifiquement tirées des villes intelligentes, des maisons intelligentes, des hôpitaux intelligents et / ou des réseaux électriques intelligents.

Nous allons à partir de cette architecture, essayer de sortir la quintessence de cette intégration pour le bénéfice des services de santé. En d'autres termes, y ajouter un système de santé intelligent et bien sécurisé, où le médecin aura la possibilité de suivre son patient à distance. Cette application aura un impact importantissime, car de nos jours on note un déficit criant de médecin ici au Sénégal. Suivant le rapport de l'OMS, il faut un médecin pour 10000 habitants. Le Sénégal n'atteint pas ces normes, ce qui montre que le système sanitaire sénégalais est malade. Et ce déficit, ce sont les régions qui en souffrent le plus. D'après l'article [123], il y'a un déficit de 102 médecins au Diourbel. Ce qui fait qu'un patient peut patienter plus de 4h dans les salles d'attente avant d'être diagnostiquer par un spécialiste.

Pour essayer de combler ce gap, nous avons pensé à un système de santé intelligent où les patients auront dans leurs maisons des objets connectés pour l'acquisition des données en rapport avec leur santé par exemple leur rythme cardiaque, tension… Les médecins profiteront de leur temps libre pour consulter et examiner les données. En effet les patients n'auront besoin d'aller à l'hôpital qu'en cas d'urgence ou demande du médecin. Ceci pourra résoudre les problèmes de longue attente et d'accessibilité géographique. De surcroît la préservation de la confidentialité et la sécurité des données seront au rendez-vous grâce notamment aux différentes technologies que nous allons utiliser.

3.12 . Conclusion

En somme ce chapitre nous a permis de montrer la complémentarité des différentes technologies, la motivation et l'impact que pourrait avoir leur intégration. Ce qui nous pousse à proposer une architecture dans le chapitre suivant.

Chapitre 4 : Proposition d'une architecture dans le domaine de la santé

4 . Introduction

Dans cette partie nous avons comme objectif de proposer une architecture dans le domaine de la santé, reliant quatre technologies (IOT, IA, Big Data, Blockchain). Ces technologies sont complémentaires et chacune d'elle aura un rôle bien déterminé et apportera sa quintessence dans la perfection de notre architecture.

4.1 . Le diagramme en flux de l'architecture

La figure 26 ci-dessous montre les différents flux existants entre les technologies et l'utilisateur final. Le processus de communication se fera comme suit :

Dans 1), après collection des données par les appareils IOT, elles seront récupérées par la partie Edge représentée par une super machine très réactive, à travers des passerelles IOT. La super machine va à son tour analyser les données, garder les plus pertinentes qui sont en rapport avec l'état de santé du patient avant d'envoyer les autres dans le service local.

Dans 2), L'intelligence artificielle interagit directement avec la maison intelligente et va se charger de récupérer les données.

Dans 3), L'IA transmet les données vers la blockchain pour qu'elle les sécurise.

Dans 4), Le médecin grâce à son compte utilisateur au niveau de la Blockchain, récupère les données grâce notamment à sa clé privée et aux politiques d'accès.

Dans 5), L'IA va aider le médecin sur la prise de décision, par rapport aux données du patient, grâce à l'intelligence artificielle, le médecin peut évaluer l'état de santé du patient.

Dans 6), l'IA intervient sur les données qui sont dans le serveur local, avec des algorithmes d'apprentissages pour le réveil automatique. L'IA met aussi en place des algorithmes de détecteurs d'anomalies pour régulariser les appareils IOT.

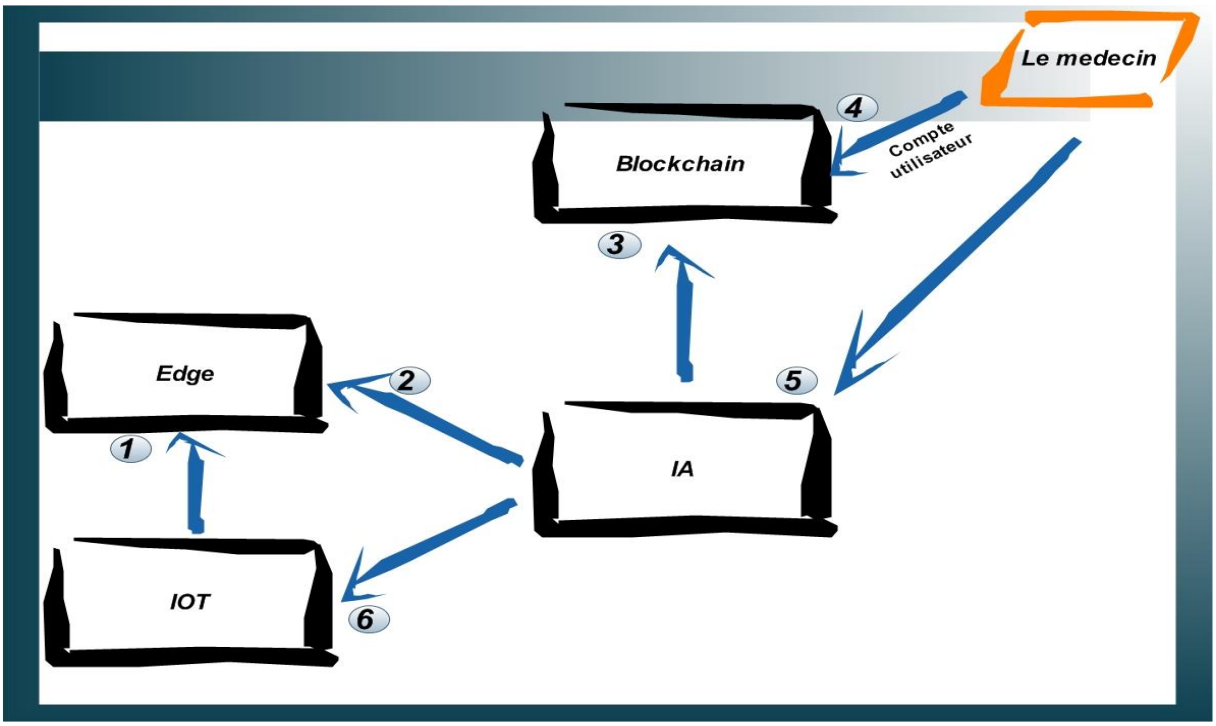


Figure 25: Diagramme en flux de l'architecture.

4.2 . Présentation de l'architecture

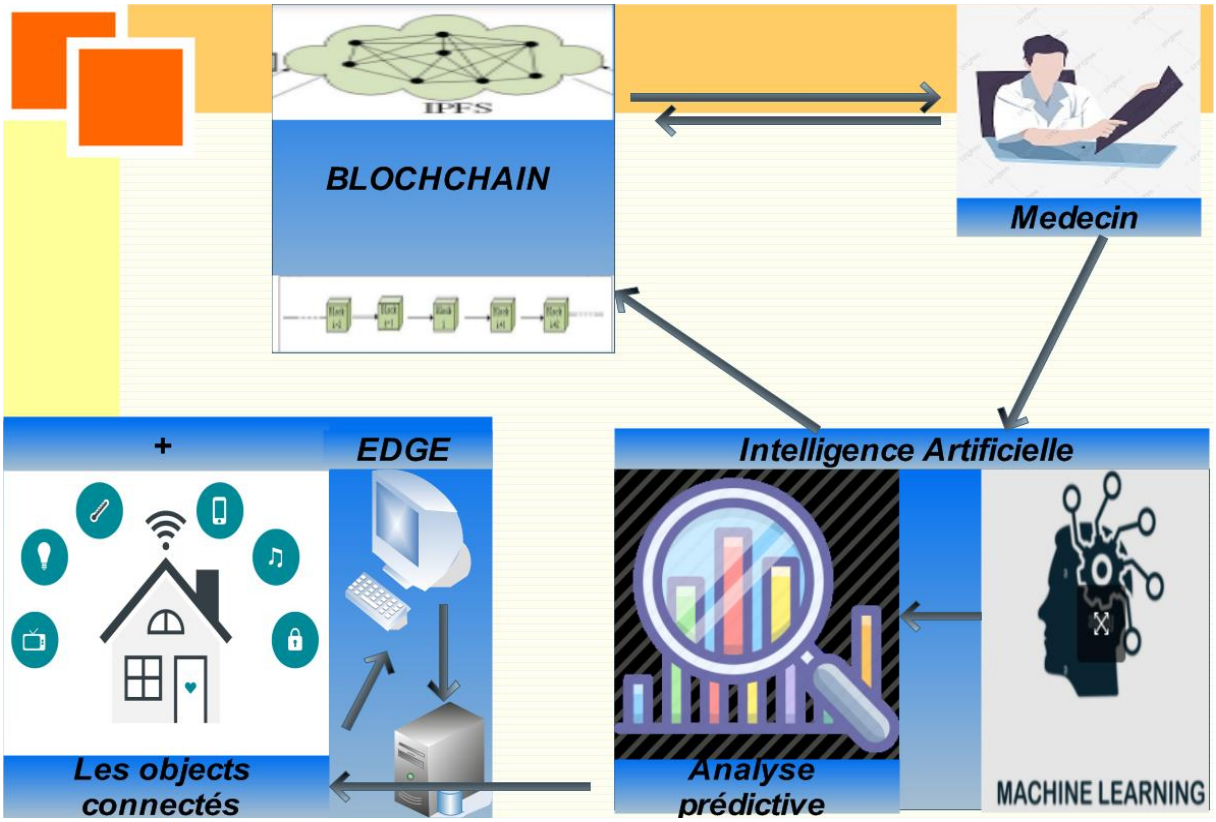


Figure 26: L'architecture proposée.

L'objectif de cette architecture est de montrer la complémentarité des technologies que nous allons utiliser. L'intégration de ces technologies permettra par exemple à un médecin de diagnostiquer à distance son patient. Pour le rôle du big data on a choisi l'Edge Computing car étant plus réactif.

4.2.1 . Edge computing

L'edge computing est un nouveau paradigme informatique dans lequel le stockage et le traitement sont effectués sur des appareils de périphérie afin d'effectuer des tâches gourmandes en ressources de calcul ainsi que des tâches sensibles aux délais. Son système réside à proximité de l'utilisateur final ou des appareils IOT, permettant de réduire le temps de réponse et optimiser la bande passante.

Dans l'edge computing, les données n'ont pas besoin d'être envoyé dans leur intégralité au data center, seules certaines informations seront remontées au data center. Les données seront collectées et stockées dans le dispositif périphérique, et traitées immédiatement en fonction du contexte au niveau du dispositif. L'hétérogénéité des appareils est hautement prise en charge. L'edge communique avec un cloud plus grand, mais lointain, un cloud centralisé.

Les différentes tâches de l'edge computing sont les suivantes :

- Gérer les appareils IOT et collecter les données ;
- Assurer une haute sécurité pour les données de capteurs à passerelle ;
- Exécuter les mains libres à l'embarquement des appareils ;
- Ingérer, collecter, stocker et analyser des données à la périphérie.

L'edge computing fournit des services limités, mais peut être utilisé pour des applications en temps réel [124].

4.3 . Le fonctionnement de l'architecture

Dans notre architecture chaque acteur, aura un rôle spécifique à jouer. Comme énumérer en haut, le but de cette architecture est de permettre à un médecin de pouvoir diagnostiquer son patient à distance mais aussi de faire des prédictions grâce à l'intelligence artificielle. Ci-dessous nous allons essayer d'expliquer de manière explicite les différentes étapes de l'architecture.

- 1ère étape : IOT

Nous avons une maison intelligente, où vit un individu avec un état de santé instable. Dans la maison nous avons des appareils IOT (capteurs, caméra de surveillance, alarme, un Hotler etc.,). Le rôle des appareils IOT est de :

- Générer des données ;
- Prétraiter des données ;
- Compresser des données ;
- Envoyer les données dans la partie Edge (voir figure 27).

- 2ème étape : Edge Comupting

Cette partie est représentée par la super machine et le serveur local qui sont dans la maison intelligente (voir figure 27). Après réception des données générées par les appareils IOT, la super machine va analyser et garder les données pertinentes qui ont besoin d'une grande réactivité et exigeant un traitement local, et envoyer les autres dans le serveur local intermédiaire au niveau Edge. Puisque y'aura beaucoup de données, nous avons spécifiquement besoin des données de la caméra de surveillance (pour l'enregistrement les mouvements de l'individu), celles de l'alarme (pour le réveil de l'individu) et enfin les données de l'Hotler (pour vérifier la fréquence cardiaque du patient). Le rôle de la super machine est de :

- Analyser et traiter les données à temps réel ;

Le serveur local quant à lui va se charger de stocker tout autres données non stockées par la super machine

- 3ème étape : L'IA

L'analyse des données va consister à faire le tri sur des données du Edge et celles du serveur local. Les informations sur le Edge seront analysées globalement pour un modèle prédictif, améliorant l'intelligence de la maison. L'intelligence artificielle se chargera par la suite de transférer les données vers la blockchain pour une meilleure sécurisation.

- 4ème étape : Blockchain

C'est l'une des étapes la plus importante de notre architecture car permettant de répondre aux problèmes et défis de sécurité des autres niveaux. De plus si les données du patient sont utilisées à mauvaise escient, la confidentialité du patient est compromise.

La blockchain, avec sa nature décentralisée et immuable, est capable de fournir des transmissions sécurisées de données et prendre également en charge le partage des données, dans le but de résoudre les problèmes de sécurité et de confidentialité qui subsistent dans les protocoles de transmission de données traditionnels.

Seules données médicales enregistrées dans le cloud seront transmises dans la blockchain pour leurs sécurisations.

Dans notre architecture nous allons utiliser la blockchain publique IPFS (InterPlanétary File System), qui est une plateforme de stockage décentralisée, développée pour résoudre le problème de la redondance des fichiers. C'est un système basé sur le cryptage des attributs, de la politique de texte chiffré, permettant de :

- Stocker les données médicales électroniques cryptées ;
- Contrôler efficacement l'accès aux données médicales électroniques, sans affecter l'efficacité de la récupération ;
- Allouer un hachage unique pour chaque fichier.

Dans IPFS, chaque nœud du réseau ne stocke que le contenu qui l'intéresse, plus quelques informations d'indexation, qui aident à déterminer où les fichiers sont stockés.

La blockchain IPFS utilise un algorithme de consensus appelé IPNS, c'est un système de dénomination décentralisé, permettant de faire le lien entre les empreintes et les noms des différents fichiers présents sur le réseau. Le client entre dans le réseau et indique au système le contenu qu'il veut rechercher, le système prend sa demande et l'envoie dans le réseau où les nœuds commenceront à répondre, en indiquant les versions du contenu disponible sur tout le réseau.

Pour empêcher d'autres utilisateur à consulter les antécédents médicaux du patient (les données), IPFS lors du chiffrage des données médicales attribue différents droits d'accès en fonction de l'attribut de l'utilisateur. La clé privée de l'utilisateur est liée à ses attributs, tandis que le texte chiffré est lié à la politique d'accès. L'utilisateur peut déchiffrer le texte chiffré si et seulement si sa clé privée correspond aux politiques d'accès du texte.

Le chiffrement basé sur les attributs (ABE) peut être divisé en chiffrement basé sur les attributs de la politique de clé (KP-ABE) et en chiffrement basé sur les attributs de la politique de texte chiffré (CP-ABE). Ce dernier est principalement utilisé pour les systèmes de stockage chiffrés,

tandis que le KP-ABE est principalement utilisé dans les systèmes d'identification biométrique. Le chiffrement se fait grâce à la fonction de hachage SHA-256.

Dans le système IPFS, l'utilisateur peut trouver rapidement le dossier médicale correspondant selon les modalités spécifiées des mots clés [125].

En outre, la blockchain est utilisée pour enregistrer le processus de stockage et de récupération des données. La valeur de hachage des données de stockage médical est stockée dans la blockchain afin d'avoir la preuve de l'authenticité de la vérification de l'utilisateur. Le cadre de blockchain décentralisé aide à assurer la sécurité du stockage des fichiers et évite le point de défaillance unique.

- 5ème étape : Le médecin

Il est l'utilisateur final de notre architecture. Son rôle est de :

- Rechercher et récupérer les données du patient dans la blockchain ;
- Faire des diagnostics sur l'état de santé du patient.

Pour récupérer les données, le médecin indique au système le contenu qu'il recherche. Le système prend sa demande et l'envoie au réseau, où des nœuds du système commenceront à répondre. Le médecin recevra la réponse des nœuds, lui indiquant les versions du contenu disponible sur tout le réseau. Grâce à sa clé privée, il déchiffre le texte chiffré qui satisfait à sa politique d'accès.

- 6ème étape : L'IA

Le rôle de l'intelligence artificielle est de :

- Faire des prédictions sur les données ;
- L'IA doit régulariser les appareils connectés qui sont dans la maison, en mettant un système de mise à jour très fréquent ou un détecteur d'anomalie, afin d'éviter le risque de contenir des failles de sécurité.

Dans notre architecture, les prédictions de l'IA seront axées spécifiquement sur les données de la caméra de surveillance et de l'alarme. Car le but est d'avoir un système d'alarme très intelligent. Par exemple l'alarme doit réveiller le patient tous les jours à 8h du matin afin qu'il puisse prendre ses médicaments. Au 1er jour l'alarme sonne et automatiquement le patient se lève de son lit, grâce à la caméra qui est capable de détecter tout mouvement du patient, la machine learning saura si le patient s'est levé ou pas et note l'information quelque part. Au 2ème

jour le même scénario se répète. Au 3ème l'alarme sonne et le patient se lève 30 minutes après, l'IA note l'information comme quoi le patient s'est levé 30 minutes après l'alarme. Au 4ème jour le même scénario que le 3ème se produit, l'IA note toujours l'information. Au 5ème, toujours le même scénario. L'IA change automatiquement l'heure de l'alarme du patient et le décale vers 8h 30 minutes. Grâce à ses modèles prédictifs, l'intelligence artificielle va améliorer l'intelligence de la maison. L'IA aidera aussi le médecin sur la prise de décision lors des diagnostics des données du patient.

4.4 . Conclusion

En définitive, cette architecture permettra de résoudre certains problèmes dans le domaine de la santé. Son application sera bénéfique pour les médecins et évitera aux patients de faire des heures dans les salles d'attentes. Grâce à la blockchain, les problèmes de confidentialité et de sécurité des données seront résolus.

5 . Perspectives

Dans nos travaux futurs, nous pensons à :

- Mettre en place une application décentralisée, permettant de matérialiser notre architecture.
- Etudier et mettre en place un système de stockage externe pour les blockchains, afin de résoudre le problème de stockage.

6 . Conclusion Générale

Pour terminer, cette étude nous a permis de voir la constante évolution de la blockchain. Initialement conçue pour permettre les transactions en bitcoin, la blockchain est maintenant décrite par certains comme la plus grande invention depuis internet ou comme une réelle révolution qui va changer notre mode de vie. Son utilisation a largement dépassé le cadre des cryptomonnaies, elle peut s'appliquer dans différents domaines (finance, santé, gouvernance etc.,). Elle peut aussi être associée à d'autres technologies, permettant de mettre en place des applications prometteuses et innovatrices.

Cependant les gouvernements se penchent également sur la blockchain et les crypto-monnaies. Ils tentent de saisir leur fonctionnement, leurs opportunités mais aussi leurs risques. Ils essayent de cadrer leurs développements, notamment en essayant de leur appliquer un cadre juridique. En France, le Bitcoin est ainsi inscrit dans la loi [126].

Néanmoins, On a vu le Salvador investir des millions de dollars dans le bitcoin et en a fait aussi une monnaie légale, encourageant les gens à l'utiliser pour des transactions quotidiennes.

Malgré qu'elle soit trop à l'aise côté sécurité, la blockchain n'est pas infaillible. Récemment elle a subi des attaques dans les finances décentralisées, où l'attaquent a remporté plus de 600 millions de dollar et le pire y'avait aucune possibilité de tracer l'opération, heureusement que l'attaquant a volontairement rendu l'argent 3 jours après. Sur ce elle doit renforcer son niveau de sécurité dans ses autres domaines d'applications.

REFERENCES

[1] « Les Blockchains - De la théorie à la pratique, de l'idée à l'implémentation (2e édition) - Origines de la technologie | Editions ENI ». https://www.editions-eni.fr/open/mediabook.aspx?idR=ea31114c253daecb43042e10af4f7637 (consulté le 7 mars 2022).

[2] O. Ayadi, « CHAPITRE III : État de l'art de la Blockchain », 2019.

[3] « Blockchain : définition, bitcoin... Tout ce qu'il faut savoir ». https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1195520-blockchain-definition-bitcoin-tout-ce-qu-il-faut-savoir/ (consulté le 7 mars 2022).

[4] H. T. M. Gamage, H. D. Weerasinghe, et N. G. J. Dias, « A Survey on Blockchain Technology Concepts, Applications, and Issues », *SN COMPUT. SCI.*, vol. 1, nº 2, p. 114, avr. 2020, doi: 10.1007/s42979-020-00123-0.

[5] « Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies ». https://www.senat.fr/rap/r17-584/r17-584_mono.html (consulté le 7 mars 2022).

[6] « Que signifie Registres distribués (DLT)? - Definition IT de Whatis.fr », *LeMagIT*. https://www.lemagit.fr/definition/Registres-distribues-DLT (consulté le 7 mars 2022).

[7] « La signature numérique - Fonctionnement ». http://igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html (consulté le 8 mars 2022).

[8] Ailleurs, « Les mathématiques de Bitcoin : SHA-256 », *bitcoin.fr*, 26 octobre 2020. https://bitcoin.fr/les-mathematiques-de-bitcoin-sha-256/ (consulté le 9 mars 2022).

[9] M. Platt *et al.*, « Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work », *arXiv:2109.03667 [cs]*, sept. 2021, Consulté le: 9 mars 2022. [En ligne]. Disponible sur: http://arxiv.org/abs/2109.03667

[10] « Le réseau de mineurs », *OpenClassrooms*. https://openclassrooms.com/fr/courses/3925766-comprendre-le-bitcoin-et-la-blockchain/4160996-le-reseau-de-mineurs (consulté le 25 février 2022).

[11] J. Yang, A. Paudel, H. B. Gooi, et H. D. Nguyen, « A Proof-of-Stake public blockchain based pricing scheme for peer-to-peer energy trading », *Applied Energy*, vol. 298, p. 117154, sept. 2021, doi: 10.1016/j.apenergy.2021.117154.

[12] « Qu'est-ce que l'horodatage sur Blockchain ? - Académie Bit2Me ». https://academy.bit2me.com/fr/timestamp-blockchain/ (consulté le 13 juin 2022).

[13] A. Bit2Me, « Qu'est-ce qu'un NONCE », *Bit2Me Academy*, 9 juillet 2018. https://academy.bit2me.com/fr/qu%27est-ce-que-le-nonce/ (consulté le 13 juin 2022).

[14] A. Bit2Me, « Qu'est-ce qu'un arbre Merkle? », *Bit2Me Academy*, 11 novembre 2019. https://academy.bit2me.com/fr/qu%27est-ce-qu%27un-arbre-merkle/ (consulté le 13 juin 2022).

[15] « Fonctionnement d'une blockchain ». https://blog.ippon.fr/2018/01/08/fonctionnement-dune-blockchain/ (consulté le 24 novembre 2021).

[16] « Blockchain Architecture | SpringerLink ». https://link.springer.com/chapter/10.1007/978-981-13-8775-3_8 (consulté le 16 juin 2022).

[17] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, et F.-Y. Wang, « Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends », *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, nº 11, p. 2266-2277, nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[18] « Journal of Medical Internet Research - Generalizable Layered Blockchain Architecture for Health Care Applications: Development, Case Studies, and Evaluation ». https://www.jmir.org/2020/7/e19029/ (consulté le 16 juin 2022).

[19] « blockchain_1.pdf ». Consulté le: 29 juin 2021. [En ligne]. Disponible sur: https://www.asprom.com/application/blockchain_1.pdf

[20] « blockchain-a-catalyst.pdf ». Consulté le: 2 mars 2022. [En ligne]. Disponible sur: https://www.pwc.com/gx/en/insurance/assets/blockchain-a-catalyst.pdf

[21] « Public and private blockchain in construction business process and information integration - ScienceDirect ». https://www.sciencedirect.com/science/article/abs/pii/S0926580520301886 (consulté le 21 juin 2022).
[22] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, et E. Hamida, « Consortium Blockchains: Overview, Applications and Challenges », sept. 2018.
[23] J. Y. Lee, « A decentralized token economy: How blockchain and cryptocurrency can revolutionize business », *Business Horizons*, vol. 62, n° 6, p. 773-784, nov. 2019, doi: 10.1016/j.bushor.2019.08.003.
[24] « Tout ce qu'il faut savoir sur la cryptomonnaie et la blockchain ». https://www.heidi.news/innovation-solutions/tout-ce-qu-il-faut-savoir-sur-la-cryptomonnaie-et-la-blockchain (consulté le 7 mars 2022).
[25] « Qu'est ce qu'une Altcoin ? | Echange de cryptomonnaies| bitFlyer Europe ». https://bitflyer.com/fr-eu/faq/55-7 (consulté le 22 juin 2022).
[26] « Token : définition et explication ». https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1207715-token-definition/ (consulté le 22 juin 2022).
[27] « Pourquoi les cryptomonnaies sont-elles si volatiles? | GOLD AVENUE ». https://www.goldavenue.com/fr/blog/newsletter-metaux-precieux-spotlight/pourquoi-les-cryptomonnaies-sont-elles-si-volatiles (consulté le 22 juin 2022).
[28] « Le stablecoin, la crypto-monnaie anti-volatilité ». https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1210122-le-stablecoin-la-crypto-monnaie-anti-volatilite-juin-2021/ (consulté le 14 mai 2022).
[29] « Définition | Stablecoin - Stable coin | Futura Tech ». https://www.futura-sciences.com/tech/definitions/cryptomonnaies-stablecoin-19671/ (consulté le 14 mai 2022).
[30] F. Aliu, A. Nuhiu, P. Pálka, et M. Blahova, « Portfolio performance analysis: a case study of cryptocurrencies », *International Journal of Blockchains and Cryptocurrencies*, vol. 1, p. 286-301, déc. 2020, doi: 10.1504/IJBC.2020.111571.
[31] « Les meilleures crypto-monnaies par capitalisation boursière », *ADVFN*. https://fr.advfn.com/cryptomonnaies (consulté le 22 juin 2022).
[32] « Le Bitcoin plonge, le Salvador perd la moitié de ses investissements ». https://www.presse-citron.net/le-bitcoin-plonge-le-salvador-perd-la-moitie-de-ses-investissements/ (consulté le 22 juin 2022).
[33] M. Crosby, « BlockChain Technology: Beyond Bitcoin », n° 2, p. 16, 2016.
[34] M. Möser, « Anonymity of Bitcoin Transactions », p. 10.
[35] « Qu’est-ce qu’Ethereum ? », *MediaSorare*, 29 septembre 2021. https://www.mediasorare.com/cryptomonnaies/quest-ce-que-ethereum/ (consulté le 22 juin 2022).
[36] S. Tikhomirov, « Ethereum: State of Knowledge and Research Perspectives », in *Foundations and Practice of Security*, vol. 10723, A. Imine, J. M. Fernandez, J.-Y. Marion, L. Logrippo, et J. Garcia-Alfaro, Éd. Cham: Springer International Publishing, 2018, p. 206-221. doi: 10.1007/978-3-319-75650-9_14.
[37] V. Buterin, « Ethereum: Platform Review », p. 45.
[38] X. F. Liu, X.-J. Jiang, S.-H. Liu, et C. K. Tse, « Knowledge Discovery in Cryptocurrency Transactions: A Survey », *IEEE Access*, vol. 9, p. 37229-37254, 2021, doi: 10.1109/ACCESS.2021.3062652.
[39] « Comment créer son nœud Ethereum avec Geth ? », *Cryptoast*, 15 mai 2019. https://cryptoast.fr/creer-son-noeud-ethereum-geth/ (consulté le 22 juin 2022).
[40] « Go Ethereum ». https://geth.ethereum.org/ (consulté le 22 juin 2022).
[41] « Meilleure plateforme crypto (2022) : comparatif des exchanges fiables », *Journal du Geek*. https://www.journaldugeek.com/crypto/ (consulté le 6 juin 2022).
[42] « A propos de nous | IZICHANGE ». https://izichange.com/client/pu_propos (consulté le 22 juin 2022).

[43] « Comprendre les Smart Contracts – Camarablock ». https://camarablock.com/comprendre-les-smart-contracts (consulté le 24 novembre 2021).
[44] F. Ashari, « Smart Contract and Blockchain for Crowdfunding Platform », *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, p. 3036-3041, juin 2020, doi: 10.30534/ijatcse/2020/83932020.
[45] T. Kerikmäe, *The Future of Law and Technologies*. 2017.
[46] « NFT et crypto monnaie : le guide ultime pour tout savoir sur cette nouvelle forme de crypto », *Web Trade Immo*, 6 octobre 2021. https://web-trade-immo.com/nft-crypto-monnaie-non-fungible-tokens/ (consulté le 13 novembre 2021).
[47] Q. Wang, R. Li, Q. Wang, et S. Chen, « Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges ». arXiv, 24 octobre 2021. Consulté le: 23 juin 2022. [En ligne]. Disponible sur: http://arxiv.org/abs/2105.07447
[48] « Cryptopunks NFT - La Collection NFT Révolutionnaire ». https://cryptonaute.fr/cryptopunks/ (consulté le 23 juin 2022).
[49] J. R. Jensen, V. von Wachter, et O. Ross, « An Introduction to Decentralized Finance (DeFi) », *Complex Systems Informatics and Modeling Quarterly*, n° 26, Art. n° 26, avr. 2021, doi: 10.7250/csimq.2021-26.03.
[50] « Finance Décentralisée : 4 Plateformes offrant des Dividendes en crypto », *Cointribune*, 21 juillet 2020. https://www.cointribune.com/tribunes/tribune-de-la-defi/finance-decentralisee-4-plateformes-offrant-des-dividendes-en-crypto/ (consulté le 16 novembre 2021).
[51] S. T. Alvi, M. N. Uddin, et L. Islam, « Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract », in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, août 2020, p. 228-233. doi: 10.1109/ICSSIT48917.2020.9214250.
[52] T. D. Smith, « The blockchain litmus test », in *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, déc. 2017, p. 2299-2308. doi: 10.1109/BigData.2017.8258183.
[53] « Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities - ScienceDirect ». https://www.sciencedirect.com/science/article/abs/pii/S026840121931792X (consulté le 23 juin 2022).
[54] S. J. Alsunaidi et F. A. Alhaidari, « A Survey of Consensus Algorithms for Blockchain Technology », in *2019 International Conference on Computer and Information Sciences (ICCIS)*, avr. 2019, p. 1-6. doi: 10.1109/ICCISci.2019.8716424.
[55] A. Kiayias et D. Zindros, « Proof-of-Work Sidechains », in *Financial Cryptography and Data Security*, vol. 11599, A. Bracciali, J. Clark, F. Pintore, P. B. Rønne, et M. Sala, Éd. Cham: Springer International Publishing, 2020, p. 21-34. doi: 10.1007/978-3-030-43725-1_3.
[56] « On the Security and Performance of Proof of Work Blockchains | Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security ». https://dl.acm.org/doi/abs/10.1145/2976749.2978341 (consulté le 25 juin 2022).
[57] G.-T. Nguyen et K. Kim, « A Survey about Consensus Algorithms Used in Blockchain », *Journal of Information Processing Systems*, vol. 14, n° 1, p. 101-128, févr. 2018, doi: 10.3745/JIPS.01.0024.
[58] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, et E. Dutkiewicz, « Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities », *IEEE Access*, vol. 7, p. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.
[59] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, et M. Zhou, « Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism », *IEEE Access*, vol. 7, p. 118541-118555, 2019, doi: 10.1109/ACCESS.2019.2935149.
[60] D. Wang, C. Jin, H. Li, et M. Perkowski, « Proof of Activity Consensus Algorithm Based on Credit Reward Mechanism », in *Web Information Systems and Applications*, Cham, 2020, p. 618-628. doi: 10.1007/978-3-030-60029-7_55.
[61] I. Bentov, C. Lee, A. Mizrahi, et M. Rosenfeld, « Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake », p. 19.

[62] S. S. Hazari et Q. H. Mahmoud, « Comparative evaluation of consensus mechanisms in cryptocurrencies », *Internet Technology Letters*, vol. 2, n° 3, p. e100, 2019, doi: 10.1002/itl2.100.
[63] A. Pal et K. Kant, « DC-PoET: Proof-of-Elapsed-Time Consensus with Distributed Coordination for Blockchain Networks », in *2021 IFIP Networking Conference (IFIP Networking)*, Espoo and Helsinki, Finland, juin 2021, p. 1-9. doi: 10.23919/IFIPNetworking52078.2021.9472787.
[64] « Srivastav et al. - 2020 - A Survey on Vulnerabilities and Performance Evalua.pdf ». Consulté le: 25 juin 2022. [En ligne]. Disponible sur: https://gredos.usal.es/bitstream/handle/10366/146094/A_Survey_on_Vulnerabilities_and_Performa.pdf?sequence=1
[65] K. Karantias, A. Kiayias, et D. Zindros, « Proof-of-Burn », in *Financial Cryptography and Data Security*, 2020, p. 523-540. doi: 10.1007/978-3-030-51280-4_28.
[66] S. Aggarwal et N. Kumar, « Chapter Eleven - Cryptographic consensus mechanisms☆☆Introduction to blockchain. », in *Advances in Computers*, vol. 121, S. Aggarwal, N. Kumar, et P. Raj, Éd. Elsevier, 2021, p. 211-226. doi: 10.1016/bs.adcom.2020.08.011.
[67] S. M. H. Bamakan, A. Motavali, et A. Babaei Bondarti, « A survey of blockchain consensus algorithms performance evaluation criteria », *Expert Systems with Applications*, vol. 154, p. 113385, sept. 2020, doi: 10.1016/j.eswa.2020.113385.
[68] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, et V. Sassone, « PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain », présenté à Italian Conference on Cyber Security (06/02/18), janv. 2018. Consulté le: 25 juin 2022. [En ligne]. Disponible sur: https://eprints.soton.ac.uk/415083/
[69] B. Lashkari et P. Musilek, « A Comprehensive Review of Blockchain Consensus Mechanisms », *IEEE Access*, vol. 9, p. 43620-43652, 2021, doi: 10.1109/ACCESS.2021.3065880.
[70] N. Chaudhry et M. Yousaf, *Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities*. 2018, p. 63. doi: 10.1109/ICOSST.2018.8632190.
[71] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, et M. A. Imran, « A Scalable Multi-Layer PBFT Consensus for Blockchain », *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, n° 5, p. 1146-1160, mai 2021, doi: 10.1109/TPDS.2020.3042392.
[72] T. Crain, V. Gramoli, M. Larrea, et M. Raynal, *DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains*. 2018, p. 8. doi: 10.1109/NCA.2018.8548057.
[73] S. Pahlajani, A. Kshirsagar, et V. Pachghare, *Survey on Private Blockchain Consensus Algorithms*. 2019, p. 6. doi: 10.1109/ICIICT1.2019.8741353.
[74] D. Mazières, « The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus ». 2015.
[75] « L'algorithme de consensus du protocole Ripple · Écarts raisonnables ». https://reasonabledeviations.com/notes/papers/ripple_consensus_protocol/ (consulté le 5 juillet 2021).
[76] « Que penser de Ripple ? », *Journal du Coin*. https://journalducoin.com/guide/avis-ripple/ (consulté le 5 juillet 2021).
[77] P. à l'origine par V. S. le, « ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms | Hacker Noon ». https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f (consulté le 1 juillet 2021).
[78] A. Yadav, « Comprehensive Study on Incorporation of Blockchain Technology With IoT Enterprises », 2021, p. 22-33. doi: 10.4018/978-1-7998-3295-9.ch002.
[79] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, et L. He, « A Comparative Study of Blockchain Consensus Algorithms », *J. Phys.: Conf. Ser.*, vol. 1437, n° 1, p. 012007, janv. 2020, doi: 10.1088/1742-6596/1437/1/012007.
[80] S. Hattab et I. F. T. Alyaseen, « Consensus Algorithms Blockchain: A comparative study », *International Journal on Perceptive and Cognitive Computing*, vol. 5, n° 2, Art. n° 2, déc. 2019, doi: 10.31436/ijpcc.v5i2.103.

[81] P. Gokhale, O. Bhat, et S. Bhat, « Introduction to IOT », vol. 5, p. 41-44, janv. 2018, doi: 10.17148/IARJSET.2018.517.
[82] « The Next Step in Internet Evolution: The Internet of Things », *CMSWire.com*. https://www.cmswire.com/cms/internet-of-things/the-next-step-in-internet-evolution-the-internet-of-things-023902.php (consulté le 18 mars 2022).
[83] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, et T. Kamal, « A review on internet of things (IoT) », *International journal of computer applications*, vol. 113, n° 1, p. 1-7, 2015.
[84] S. Madakam, R. Ramaswamy, et S. Tripathi, « Internet of Things (IoT): A Literature Review », *JCC*, vol. 03, n° 05, p. 164-173, 2015, doi: 10.4236/jcc.2015.35021.
[85] M. A. Iqbal, O. G. Olaleye, et M. A. Bayoumi, « A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches », *Global Journal of Computer Science and Technology*, janv. 2017, Consulté le: 28 juin 2022. [En ligne]. Disponible sur: https://computerresearch.org/index.php/computer/article/view/1483
[86] J. McCarthy, « WHAT IS ARTIFICIAL INTELLIGENCE? », p. 15.
[87] « Intelligence Artificielle, Machine Learning, Deep Learning », *Oracle France*. https://www.oracle.com/fr/cloud/deep-learning-intelligence-artificielle.html (consulté le 4 décembre 2021).
[88] « Les domaines de l'intelligence artificielle ». http://www.intelligenceartificielle.fr/domaines_IA.php (consulté le 28 juin 2022).
[89] M. A. Waller et S. E. Fawcett, « Click Here for a Data Scientist: Big Data, Predictive Analytics, and Theory Development in the Era of a Maker Movement Supply Chain », *Journal of Business Logistics*, vol. 34, n° 4, p. 249-252, 2013, doi: 10.1111/jbl.12024.
[90] « Qu'est-ce que le Big Data ? | Oracle France ». https://www.oracle.com/fr/big-data/what-is-big-data/ (consulté le 23 février 2022).
[91] « Les 5V qui définissent le big data - MBA DMB ». https://blog.mbadmb.com/big-data-agriculture-la-donnee-est-dans-le-pre/les-5v-qui-definissent-le-big-data/ (consulté le 28 juin 2022).
[92] Y. Demchenko, C. Ngo, et P. Membrey, « Architecture Framework and Components for the Big Data Ecosystem », p. 31.
[93] U. G. Gupta et A. Gupta, « Vision: A Missing Key Dimension in the 5V Big Data Framework », *Journal of International Business Research and Marketing*, vol. 1, n° 3, p. 50-56, 2016.
[94] M. A. Khan et K. Salah, « IoT security: Review, blockchain solutions, and open challenges », *Future Generation Computer Systems*, vol. 82, p. 395-411, mai 2018, doi: 10.1016/j.future.2017.11.022.
[95] O. Alphand *et al.*, « IoTChain: A Blockchain Security Architecture for the Internet of Things », Barcelona, Spain, avr. 2018. Consulté le: 28 juin 2022. [En ligne]. Disponible sur: https://hal.archives-ouvertes.fr/hal-01705455
[96] « IoT and Blockchain Convergence: Benefits and Challenges - IEEE Internet of Things ». https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html (consulté le 24 mai 2022).
[97] C.-C. Lin et A. Vinel, « Recent Internet of Things Applications in Smart Grid and Various Industries », *Mobile Networks and Applications*, p. 1-2, 2020.
[98] E. T. Bradlow, M. Gangwar, P. Kopalle, et S. Voleti, « The Role of Big Data and Predictive Analytics in Retailing », *Journal of Retailing*, vol. 93, n° 1, p. 79-95, mars 2017, doi: 10.1016/j.jretai.2016.12.004.
[99] F. Corea, « The Convergence of AI and Blockchain », in *Applied Artificial Intelligence: Where AI Can Be Used In Business*, F. Corea, Éd. Cham: Springer International Publishing, 2019, p. 19-26. doi: 10.1007/978-3-319-77252-3_4.
[100] A. A. Hussain et F. Al-Turjman, « Artificial intelligence and blockchain: A review », *Transactions on Emerging Telecommunications Technologies*, vol. 32, n° 9, p. e4268, 2021, doi: 10.1002/ett.4268.

[101] K. Salah, M. H. U. Rehman, N. Nizamuddin, et A. Al-Fuqaha, « Blockchain for AI: Review and Open Research Challenges », *IEEE Access*, vol. 7, p. 10127-10149, 2019, doi: 10.1109/ACCESS.2018.2890507.
[102] K. Rabah et M. Research, « Convergence of AI, IoT, Big Data and Blockchain: A Review », vol. 1, n° 1, p. 18, 2018.
[103] « The Convergence of AI and Blockchain: What's the deal? », *KDnuggets*. https://www.kdnuggets.com/the-convergence-of-ai-and-blockchain-whats-the-deal.html/2/ (consulté le 1 juillet 2022).
[104] F. Corea, « AI and Blockchain », in *An Introduction to Data*, vol. 50, Cham: Springer International Publishing, 2019, p. 69-76. doi: 10.1007/978-3-030-04468-8_11.
[105] N. Abdullah, A. håkansson, et E. Moradian, *Blockchain based approach to enhance big data authentication in distributed environment*. 2017, p. 892. doi: 10.1109/ICUFN.2017.7993927.
[106] « Improving security of medical big data by using Blockchain technology - ScienceDirect ». https://www.sciencedirect.com/science/article/abs/pii/S0045790621004742 (consulté le 1 juillet 2022).
[107] E. Karafiloski et A. Mishev, « Blockchain solutions for big data challenges: A literature review », in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, 2017, p. 763-768.
[108] « Qu'est-ce qu'un Oracle Blockchain ? », *Binance Academy*. https://academy.binance.com/fr/articles/blockchain-oracles-explained (consulté le 1 juillet 2022).
[109] N. Deepa *et al.*, « A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions », *arXiv:2009.00858 [cs]*, févr. 2021, Consulté le: 25 février 2022. [En ligne]. Disponible sur: http://arxiv.org/abs/2009.00858
[110] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, et A. Kastania, « Astraea: A Decentralized Blockchain Oracle », in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, juill. 2018, p. 1145-1152. doi: 10.1109/Cybermatics_2018.2018.00207.
[111] E. Ahmed *et al.*, « The role of big data analytics in Internet of Things », *Computer Networks*, vol. 129, p. 459-471, déc. 2017, doi: 10.1016/j.comnet.2017.06.013.
[112] « IoT et Big Data : comprendre la relation entre ces deux technologies - Ryax Technologies ». https://ryax.tech/fr/iot-et-big-data-comprendre-la-relation-entre-ces-deux-technologies/ (consulté le 13 juillet 2022).
[113] « Dix exemples de collaboration entre l'Internet des objets et le Big Data ». https://fr.jsspu.com/data/Ten-examples-of-IoT-and-big-data-working-well-together/ (consulté le 13 juillet 2022).
[114] Renaud, « 4 bons exemples de l'intégration de l'IoT et du Big Data dans des macrostructures », *Objetconnecte.com*, 23 juin 2015. https://www.objetconnecte.com/4-organisations-combinaison-bigdata-iot-2306/ (consulté le 13 juillet 2022).
[115] « Big Data et Intelligence artificielle : enjeux business », *Talend - A Leader in Data Integration & Data Integrity*. https://www.talend.com/fr/resources/big-data-ia/ (consulté le 15 juillet 2022).
[116] A. Kulakli et V. Osmanaj, « Global research on big data in relation with artificial intelligence (A bibliometric study: 2008-2019) », 2020.
[117] D. E. O'Leary, « Artificial Intelligence and Big Data », p. 4, 2013.
[118] « Comparatif Plateformes d'intelligence artificielle: Avis Prix Alternatives | Comparateur Logiciels.Pro ». Consulté le: 16 juillet 2022. [En ligne]. Disponible sur: https://www.logiciels.pro/comparatif-logiciels-saas/comparatif-services-it-big-data-donnees/comparatif-science-des-donnees/comparatif-plateformes-dintelligence-artificielle/
[119] « CognitiveScale Avis Prix & Alternatives | Comparateur Logiciels.Pro ». https://www.logiciels.pro/logiciel-saas/cognitivescale/ (consulté le 16 juillet 2022).
[120] « AIDA Avis Prix & Alternatives | Comparateur Logiciels.Pro ». https://www.logiciels.pro/logiciel-saas/aida/ (consulté le 16 juillet 2022).

[121] S. M. H. Bamakan, N. Faregh, et A. ZareRavasan, « Di-ANFIS: an integrated blockchain–IoT–big data-enabled framework for evaluating service supply chain performance », *Journal of Computational Design and Engineering*, vol. 8, n° 2, p. 676-690, avr. 2021, doi: 10.1093/jcde/qwab007.
[122] D. Gohil et S. V. Thakker, « Blockchain-integrated technologies for solving supply chain challenges », *Modern Supply Chain Research and Applications*, vol. 3, n° 2, p. 78-97, janv. 2021, doi: 10.1108/MSCRA-10-2020-0028.
[123] « Kolda, Sédhiou, Ziguinchor… : un déficit de 102 médecins et des mois sans soins », *Infomed*, 5 mai 2021. https://infomed.sn/kolda-sedhiou-ziguinchor-un-deficit-de-102-medecins-et-des-mois-sans-soins/ (consulté le 30 septembre 2022).
[124] « Edge computing: A survey - ScienceDirect ». https://www.sciencedirect.com/science/article/abs/pii/S0167739X18319903 (consulté le 28 septembre 2022).
[125] J. Sun, X. Yao, S. Wang, et Y. Wu, « Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS », *IEEE Access*, vol. 8, p. 59389-59401, 2020, doi: 10.1109/ACCESS.2020.2982964.
[126] « Blockchain : introduction et applications | Etopia ». https://etopia.be/blockchain-introduction-et-applications/ (consulté le 21 juillet 2022).